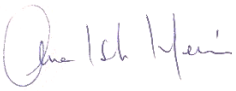
Deusto
Universidad de Deusto

LA RESPUESTA NORMATIVA AL TRATAMIENTO DE DATOS PERSONALES DEL MENOR POR PROVEEDORES DE REDES SOCIALES. DE LA PRESTACIÓN DEL CONSENTIMIENTO AL OLVIDO DIGITAL EN LA ERA DEL *BIG DATA* Y LA INTELIGENCIA ARTIFICIAL

-Tesis doctoral-



ESTELA BRIÓN BERDOTE

Dirigida por: Ana Isabel Herrán Ortiz

y Francisco Lledó Yagüe

Programa de Doctorado en Derecho Económico y de la Empresa

Universidad de Deusto

Donostia-San Sebastián, 2023

A mis padres,

por el sacrificio de poner ante mí un mundo repleto de posibilidades

A mi hermana,

por ser la fuente que me motiva a continuar siendo un ejemplo a seguir

A mi marido,

por recordarme que hay esfuerzos que merecen la pena

“Los críticos son los que consiguen mejoras”

-Jaron Lanier-

“Oscuros y difíciles tiempos nos aguardan. Pronto todos tendremos que decidir entre lo que es correcto y lo que es fácil”

-Albus Dumbledore-

AGRADECIMIENTOS

Esta tesis doctoral ha sido fruto de la confianza y el apoyo mostrados por la Universidad de Deusto, y en especial, de la Facultad de Derecho. Tanto es así, que sin sus recursos no hubiera sido posible presentar esta tesis doctoral. Sin embargo, en este reconocimiento merece un especial agradicimiento el campus de Donostia, pues es el lugar en el que se ha desarrollado la presente investigación.

Asimismo, quiero mostrar mi gratitud a todas las personas de la Universidad que han contribuido a que esta tesis doctoral que se presenta llegue a buen término; desde aquellas que me animaron a embarcarme en este proyecto, hasta las que han intervenido en el día a día de su elaboración, brindándome los ánimos y el afecto que de tanta ayuda me han servido.

Nuevamente, muchas gracias a todos.

RESUMEN

En plena era digital, los más jóvenes pueden considerarse los principales usuarios de redes sociales desde edades verdaderamente tempranas. Sin embargo, estos nuevos hábitos en línea erosionan la privacidad de los más jóvenes de un modo sin precedentes, en especial, desde la irrupción de técnicas de tratamiento que emplean *big data* e inteligencia artificial. En consecuencia, el presente estudio se centra, por una parte, en analizar si la normativa otorga especial protección a la información personal del menor cuando maneja estas plataformas; por otra parte, se plantean nuevas garantías normativas en orden a proteger de manera reforzada los datos personales del menor como usuario especialmente vulnerable de estos servicios.

ÍNDICE

CAPÍTULO I:

LA PROTECCIÓN JURÍDICA DEL MENOR EN LA ERA DE LA TRANSFORMACIÓN DIGITAL

LISTADO DE ABREVIATURAS..... IX

INTRODUCCIÓN..... 1

1. LOS ANTECEDENTES HISTÓRICOS DE LA PROTECCIÓN JURÍDICA DEL MENOR..... 13

2. LA PROTECCIÓN DE LA INFANCIA EN EL ÁMBITO JURÍDICO INTERNACIONAL 14

2.1. Aproximación a la normativa internacional sobre protección jurídica del menor 15

2.2. El alcance de la Convención de los Derechos del Niño de 1989 respecto a los derechos fundamentales relacionados con la privacidad de los menores de edad. ¿Un texto jurídico adaptado al contexto tecnológico actual? 17

3. LA CONFIGURACIÓN DEL MARCO NORMATIVO EUROPEO DE PROTECCIÓN JURÍDICA DE LOS MENORES..... 23

3.1. Primeros pasos de la Unión Europea en la regulación de derechos fundamentales del menor..... 24

3.2. La privacidad de los menores en la Carta Europea de los Derechos del Niño, de 8 de julio de 1992. Su escaso valor como texto jurídico para la protección jurídica de la infancia en un entorno digital 26

4. LA NECESARIA INCORPORACIÓN DEL MODELO INTERNACIONAL DE PROTECCIÓN JURÍDICA DE LA INFANCIA A LA LEGISLACIÓN ESPAÑOLA 29

4.1. La protección de los derechos fundamentales del menor en la Constitución Española 29

4.2. La Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del menor. Primera iniciativa en la protección específica de derechos fundamentales del menor en España 31

4.2.1. El menor como titular de derechos fundamentales y la capacidad progresiva para su ejercicio de manera autónoma 35

4.2.2. El interés superior del menor como principio fundamental de su protección en la legislación y jurisprudencia españolas 43

4.2.3. El desarrollo normativo de los derechos fundamentales adaptado a la minoría de edad en la LOPJM. Especial atención a la protección del derecho a la intimidad 52

5. TRANSFORMACIÓN DIGITAL Y LOS DERECHOS FUNDAMENTALES DEL MENOR..... 55

5.1. Los derechos de la personalidad del menor y su vulneración en el entorno digital 56

5.2. De la necesidad de proteger específicamente el derecho a la protección de datos personales cuya titularidad recaiga en menores de edad..... 64

5.3. Una nueva configuración legal de los derechos fundamentales del menor en la LOPJM: de la necesaria revisión legislativa ante la irrupción de la sociedad de la información 67

CAPÍTULO II:

LA CONSTRUCCIÓN NORMATIVA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES. SU CONFIGURACIÓN A LA LUZ DEL INTERÉS SUPERIOR DEL MENOR

1. ANTECEDENTES NORMATIVOS DE LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO INTERNACIONAL . 77

1.1. Las valiosas aportaciones de la ONU y la OCDE en torno al tratamiento de datos personales 78

1.2. La contribución del Consejo de Europa a la protección de datos personales: El Convenio nº 108 y sus posteriores modificaciones 82

1.3. La proyección internacional del derecho a la protección de datos en el siglo XXI. Una tímida visibilización de la protección del menor 87

2. LA UE ANTE EL RETO NORMATIVO DE DESARROLLAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES 94

2.1. La compleja configuración de los derechos fundamentales en la UE: el marcado carácter económico de la normativa europea hasta la aprobación de la Carta Europea de Derechos Humanos, de 7 de diciembre de 2000 95

2.2. El fundamento jurídico del derecho a la protección de datos personales en el Derecho originario de la UE 97

2.3. La Directiva 95/46/CE de protección de las personas frente al tratamiento de sus datos personales y de la libre circulación de estos datos. Un modelo normativo superado 100

2.3.1. La Directiva 95/46/CE: una respuesta fallida a la necesidad de armonización legislativa en el seno de la UE 100

2.3.2. La protección de datos personales de los menores: el silencio de la Directiva 95/46/CE 103

2.3.3. La obsolescencia de la Directiva 95/46/CE ante el avance de la sociedad de la información y su incidencia sobre la protección de los datos de menores de edad 106

2.4 Hacia un marco normativo europeo homogéneo de protección de datos personales: el Reglamento 2016/679 110

2.4.1. Las claves de un nuevo sistema normativo de protección de datos personales adaptado al actual contexto digital 113

2.4.2. La esperada positivización de la protección de datos personales de menores 121

3. UNA APROXIMACIÓN A LA EVOLUCIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA JURÍDICO ESPAÑOL 124

3.1 De la limitación del uso de la informática a la configuración de un derecho fundamental autónomo de protección de datos de carácter personal 125

3.1.1. El fundamento constitucional del derecho a la protección de datos personales: el debatido artículo 18.4 CE 126

3.1.2. La intensa labor interpretativa del Tribunal Constitucional en la proclamación de un nuevo derecho fundamental: el contenido esencial del derecho a la protección de datos personales 129

3.2 El desarrollo legislativo del derecho fundamental a la protección de datos personales: la salvaguarda de los datos personales del menor en la normativa española de protección de datos de carácter personal 136

CAPÍTULO III:

EL TRATAMIENTO DE DATOS PERSONALES DEL MENOR COMO USUARIO DE REDES SOCIALES. DIFICULTADES LEGALES EN LA CONFIGURACIÓN EN LÍNEA DEL CONSENTIMIENTO AL TRATAMIENTO OTORGADO POR MENORES DE EDAD

1. DE LA WEB 1.0 A LA WEB 4.0: LA IRRUPCIÓN DE LA WEB 2.0 COMO UN NUEVO MODO DE RELACIONARSE 149

2. EL IMPACTO DE LAS REDES SOCIALES *ONLINE* EN LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL DEL MENOR 154

2.1. Concepto, tipología y funcionamiento de redes sociales *online* 154

2.1.1. A vueltas con el concepto de red social 154

2.1.2. La experiencia del usuario de redes sociales y el tratamiento de sus datos personales. Un reto para el ordenamiento jurídico. 158

2.2. Hábitos del usuario menor de edad en redes sociales. De las dificultades para la protección de su información personal 165

2.3. Aproximación a los riesgos y amenazas para el menor derivados del acceso a redes sociales. Especial referencia a su privacidad 171

3. LA NORMATIVA APLICABLE A LAS REDES SOCIALES *ONLINE:* LA AUSENCIA DE UN MARCO JURÍDICO ESPECÍFICO DE REFERENCIA 180

3.1. A propósito de los responsables del tratamiento en redes sociales *online*. Sobre los problemas que plantean los hábitos del usuario (su participación activa) en redes sociales 182

3.2. La determinación jurídica de la legislación aplicable ante la ubicuidad de las redes sociales: un debate superado 190

4. LA PRESTACIÓN DEL CONSENTIMIENTO DEL MENOR DE EDAD COMO BASE LEGAL DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES EN REDES SOCIALES 196

4.1. Luces y sombras en torno al consentimiento *online* del tratamiento de datos personales 199

4.1.1 Los principios de licitud y transparencia en los tratamientos de datos de menores de edad: las confusas y complejas políticas de privacidad de las redes sociales 202

4.1.2. La configuración online de la prestación del consentimiento vs. la normativa sobre protección de datos personales 220

4.2. La prestación del consentimiento por el menor de edad al tratamiento de datos personales en redes sociales. Problemas para verificar la edad de los internautas..... 230

CAPÍTULO IV:

HACIA UNA EXPERIENCIA PERSONALIZADA DEL USUARIO EN REDES SOCIALES COMO FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES. LA INTELIGENCIA ARTIFICIAL APLICADA AL PROCESO DE RECOPILACIÓN MASIVA DE INFORMACIÓN PERSONAL DEL MENOR CON FINES DE PUBLICIDAD Y MERCADOTECNIA DIRECTA

1. LA ERA DE LOS MACRODATOS 247

2. TÉCNICAS DE ANÁLISIS MASIVOS DE DATOS PERSONALES EN REDES SOCIALES: UN NUEVO DESAFÍO PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL MENOR 251

2.1. La inevitable relación entre los datos de carácter personal y el desarrollo de las técnicas de análisis masivos de datos 252

2.2. Sobre el empleo de técnicas de *big data* e inteligencia artificial por proveedores redes sociales como instrumento para rentabilizar sus servicios 258

2.3. *Big data* e inteligencia artificial: su impacto sobre los derechos fundamentales de personas en tránsito hacia su madurez 265

3. RESPUESTA NORMATIVA A LAS TÉCNICAS DE ANÁLISIS MASIVO DE DATOS EN EL MARCO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES 274

3.1. La cuestionada eficacia del consentimiento del interesado como condición de licitud para el tratamiento de datos personales mediante tecnologías *big data* e inteligencia artificial 275

3.2. De la recopilación a gran escala de datos personales del menor internauta y las tensiones que esta genera con el principio de minimización de los datos 281

3.3. El RGPD ante la elaboración de perfiles de personalidad del menor y la toma de decisiones automatizadas en redes sociales 291

4. MONITORIZACIÓN DEL COMPORTAMIENTO DEL MENOR EN REDES SOCIALES A TRAVÉS DE LAS *COOKIES* CON FINES DE PUBLICIDAD COMPORTAMENTAL. LA INSUFICIENCIA DE LA NORMATIVA EUROPEA 304

4.1. La personalización de la publicidad basada en el análisis del comportamiento de los usuarios de redes sociales. Nuevas técnicas para la recopilación de datos personales 304

4.2. La transparencia y el consentimiento previo como garantías jurídicas fundamentales para la instalación de *cookies* con fines de publicidad comportamental 307

4.3. A propósito de una nueva regulación en el empleo de *cookies*: la propuesta del Reglamento comunitario sobre privacidad y las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (e-privacy)..... 319

5. EL TRATAMIENTO DE DATOS PERSONALES EN REDES SOCIALES A PARTIR DE LA INTELIGENCIA ARTIFICIAL. UN NUEVO DESAFÍO LEGISLATIVO..... 323

5.1. Los principios y valores que deben inspirar el desarrollo de la IA..... 324

5.2. La explicabilidad y auditabilidad como presupuestos indispensables para una IA lícita 327

CAPÍTULO V:

LA DELIMITACIÓN NORMATIVA DE LOS DERECHOS DEL MENOR EN LA SALVAGUARDA DE SU INFORMACIÓN PERSONAL. ESPECIAL REFERENCIA AL DERECHO AL OLVIDO DIGITAL EN REDES SOCIALES, ¿UTOPÍA O REALIDAD?

1. DILEMAS EN EL EJERCICIO DE LOS DERECHOS ARCO-POL QUE ASISTEN AL MENOR DE EDAD PARA LA PROTECCIÓN DE SU INFORMACIÓN PERSONAL EN REDES SOCIALES 345

1.1. Sobre la revisión de los tradicionales derechos para la protección de la información personal en la era del *big data* y las redes sociales..... 346

1.2. Nuevas facultades para garantizar al interesado el control sobre sus datos personales en el marco de la inteligencia artificial ante el avance de las redes sociales 351

2. DEL "RIGHT TO PRIVACY" DE WARREN Y BRANDEIS AL DERECHO AL OLVIDO DIGITAL..... 360

3. ANTECEDENTES NORMATIVOS DEL DERECHO AL OLVIDO DIGITAL... 365

3.1. Las autoridades nacionales de control de datos personales en la construcción de un derecho al olvido: especial referencia a la intervención de la AEPD en el reconocimiento del derecho al olvido digital..... 367

3.2. La configuración jurisprudencial del derecho al olvido digital en el ámbito europeo y nacional 371

4. LA CONSAGRACIÓN JURÍDICA DEL DERECHO AL OLVIDO DIGITAL EN LA NORMATIVA EUROPEA Y ESPAÑOLA 381

4.1. La UE como fiel partidaria del reconocimiento del derecho al olvido digital. En especial, de las personas menores en tránsito hacia su madurez 382

4.2. El diferente camino normativo seguido por el legislador español en la regulación del derecho al olvido digital en la LOPDGDD 387

5. DIFICULTADES EN LA SUPRESIÓN U OLVIDO DIGITAL DE DATOS PERSONALES DE MENORES EN REDES SOCIALES 391

5.1. ¿El olvido digital se identifica con el desindexado en el contexto de redes sociales? 391

5.2. Los hábitos del usuario en redes sociales: un impedimento para la eficaz supresión de datos personales..... 396

5.3. El derecho de supresión (olvido digital) en tiempos de *big data* e inteligencia artificial..... 401

CONCLUSIONES 409

BIBLIOGRAFÍA 449

LISTADO DE ABREVIATURAS

AEPD *Agencia Española de Protección de Datos*

CE *Constitución Española*

Convención de 1989 *Convención de los Derechos del Niño, de 20 de noviembre*

CEPD *Comité Europeo Protección de Datos*

Directiva 95/46/CE *Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 24 de octubre de 1995*

ENISA *European Network and Information Security Agency*

Garante Italiano *Garante per la Protezione del Dati Personali*

IA *Inteligencia Artificial*

INE *Instituto Nacional de Estadística*

Carta Europea de los Derechos del Niño *Carta europea de los Derechos del Niño, de 8 de junio de 1992*

LOPJM *Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del Menor*

LOPD *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal*

LOPDGDD *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos de carácter personal y garantías digitales*

LORTAD *Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*

LSSIE *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*

OCDE *Organización para la Cooperación y Desarrollo Económico*

OIT *Organización Internacional del Trabajo*

ONU *Organización de las Naciones Unidas*

RGPD *Reglamento General de Protección de Datos Personales, de 27 de abril de 2016*

TIC *Tecnologías de la Información y de la Comunicación*

TEDH *Tribunal Europeo de Derechos Humanos*

TJCE *Tribunal de Justicia de las Comunidades Europeas*

TJUE *Tribunal de Justicia de la Unión Europea*

TFUE *Tratado de Funcionamiento de la Unión Europea*

TUE *Tratado de la Unión Europea*

UE *Unión Europea*

INTRODUCCIÓN

El deseo de proteger jurídicamente la infancia como colectivo especialmente vulnerable de aquellos riesgos que inciden en su desarrollo personal y vulneran sus derechos fundamentales, se presenta como una tarea cada vez más presente en la agenda del legislador. Desde el reconocimiento del menor como sujeto titular de derechos y con capacidad progresiva para su ejercicio autónomo, los ordenamientos jurídicos han aunado esfuerzos para procurar garantizar su autonomía como sujetos, pero sin olvidar que, en ocasiones, su especial situación de tránsito hacia la madurez aparejará la necesidad de protegerlos especialmente. En esta dicotomía, la irrupción de la era digital ha supuesto un nuevo reto para la protección jurídica de la minoría de edad.

En escasos cuarenta años, la rápida evolución de Internet ha desembocado en que la sociedad del siglo XXI traslade prácticamente todos sus hábitos al ámbito digital de un modo que puede considerarse irreversible. En efecto, desde el arranque de la web 1.0 a la actual web 4.0, la sociedad ha protagonizado un éxodo masivo de sus comportamientos diarios al entorno *online*. En ese sentido, destaca que entre otras funcionalidades que Internet ofrece, las personas se han acostumbrado a saciar sus necesidades de comunicación y entretenimiento por medio de la herramienta por la que se caracteriza la web 2.0: las redes sociales. Así las cosas, personas de todas las edades acceden a estos espacios a diario con el fin de relacionarse.

Sentado cuanto antecede, desde la misma irrupción de las redes sociales y persuadidos por el entorno relacional que estas predisponen, los menores de edad han protagonizado un acceso masivo a estos espacios desde edades verdaderamente tempranas. Alentados por el diseño de estas plataformas, se han aventurado a compartir infinidad de informaciones propias y de terceros. Ahora bien, la metamorfosis sufrida en los servicios que estos proveedores prestan-centrándose ahora en personalizar la experiencia del usuario ofreciéndole publicidad adaptada a sus gustos y preferencias-, ha generado un riesgo mayor para la privacidad de los más jóvenes, si cabe. Efectivamente, los proveedores de redes sociales han implementado, paulatinamente, sistemas de recogida y tratamiento de datos personales más intrusivos en orden a rentabilizar sus negocios.

En consecuencia, estos espacios generan un entorno hostil para los derechos fundamentales relacionados con la privacidad del menor. En concreto, el acceso y manejo de redes sociales puede vulnerar derechos como el honor, la intimidad personal y familiar,

así como la propia imagen, pero también el derecho a la protección de datos personales, pues la esencia de estos servicios reside en incitar al usuario de los mismos al desvelo de información personal constante. En virtud de lo expuesto, a pesar de que el concepto de privacidad comprenda los mentados derechos fundamentales, el presente trabajo centrará su estudio en el derecho a la protección de datos personales. Sentado que la actividad principal de estos servicios precisa del tratamiento de datos personales de los usuarios, el derecho fundamental a la protección de datos personales consagrado en el art. 18.4 CE adquiere una posición central ante el implacable avance de la sociedad de la información. Ciertamente, este derecho fundamental de más de veinte años de recorrido, se convierte en la principal herramienta al servicio de las personas para controlar y proteger los datos concernientes a su persona en este nuevo escenario digital.

Por todo lo expuesto, el objetivo general de este trabajo se identifica con evaluar minuciosamente la existencia y suficiencia de aquellas medidas que buscan una protección jurídica específica del menor como usuario de redes sociales. Concretamente, el reto se halla en conceder una salvaguarda íntegra al menor frente a cualquier riesgo que pueda vulnerar su derecho a la protección de datos personales, especialmente, en el entorno digital actual.

Asimismo, se identifican seis objetivos específicos. El primero se corresponde con analizar la suficiencia de la normativa sobre protección jurídica de los menores en los ámbitos internacional, europeo y nacional en plena era de la sociedad de la información. Con especial atención desde el final del siglo xx, el legislador ha acometido la tarea de construir un marco jurídico de referencia en torno a la protección jurídica de la infancia; por tanto, deviene indispensable analizar si el mismo ampara y protege los derechos fundamentales de los menores internautas en un siglo caracterizado por la revolución tecnológica.

El segundo objetivo, por su parte, se identifica con el estudio de la normativa sobre protección de datos personales con el fin de determinar si la misma protege la información personal los menores de edad como usuarios de redes sociales especialmente vulnerables. Efectivamente, el derecho a la protección de datos personales se configura como la principal herramienta al servicio de las personas para controlar su información personal; por tanto, cabe estudiar si la misma prevé garantías suficientes para la protección específica de los datos personales de los más jóvenes como sujetos necesitados de especial protección.

El tercer objetivo, se centra en identificar y analizar los riesgos tanto jurídicos, como psicológicos que entraña el manejo de redes sociales por menores de edad, pues solamente identificando estas amenazas puede construirse una respuesta normativa garantista que salvaguarde eficazmente la información del menor en este ámbito. Particularmente, son múltiples los peligros que puede traer consigo el manejo de estas plataformas; no obstante, el presente trabajo desea poner el foco en aquellos que inciden sobre la privacidad de los menores cuando manejan redes sociales.

El cuarto objetivo, estudia el derecho al olvido digital como posible respuesta al rastro tecnológico permanente que los datos dejan en la red, especialmente en el caso de menores, pues los jóvenes no son conscientes de que el gran volumen de datos que comparten, dejará una huella indefinida en la red a la que los proveedores de redes sociales extraerán un provechoso rendimiento económico. Así, nos preguntamos si esta facultad que mana del contenido esencial del derecho fundamental a la protección de datos personales garantiza un eficaz olvido digital de la información en redes sociales.

El sexto y último objetivo, culmina con la formulación de propuestas legales concretas de mejora para la protección de la información personal concerniente a menores de edad cuando manejan estos espacios. Sin ánimo de anticiparnos en exceso, la respuesta del ordenamiento jurídico en torno a la protección jurídica del menor como usuario de redes sociales no es la deseada; por tanto, es tarea reservada del presente trabajo proponer medidas jurídicas concretas cuyo fin se identifica con la protección integral del menor como principal usuario de estos espacios.

En consecuencia, dado que el ordenamiento jurídico debe procurar la protección integral de los menores de edad frente a nuevos riesgos que el avance tecnológico predispone, la presente investigación se propone conceder una respuesta a la siguiente hipótesis:

¿Se encuentra el derecho fundamental a la protección de datos personales del menor, como sujeto especialmente vulnerable, suficientemente protegido por el ordenamiento jurídico cuando es usuario de redes sociales?

Con la finalidad de responder a la pregunta de investigación que se plantea, la metodología empleada en la presente investigación se corresponde con la propia de las ciencias jurídicas. Así, el estudio ha combinado diversos métodos de investigación, entre los que destaca el método dogmático. Sin embargo, también se han empleado métodos

como el histórico-evolutivo, especialmente, en los dos primeros capítulos. Por último, en menor medida, también ha resultado de utilidad el método comparativo en determinadas cuestiones referentes al tratamiento de datos personales como, por ejemplo, en lo concerniente a sistemas de verificación de la edad del usuario internauta para la prestación del consentimiento al tratamiento o en lo referente a la explicabilidad de los algoritmos que se emplean para el tratamiento de datos personales.

Respecto a las fuentes empleadas, la investigación se ha centrado en el estudio y análisis pormenorizado de la legislación al efecto, la doctrina especializada en la materia, así como en el análisis de la jurisprudencia y documentos de organismos oficiales.

En primer lugar, se ha acometido un análisis riguroso de la normativa desde una doble dimensión. Por una parte, la legislación analizada en una primera dimensión se corresponde con la normativa sobre protección jurídica de la infancia, tanto en el ámbito internacional, como en el europeo y nacional. En concreto, desde una perspectiva internacional, la normativa en vigor destaca por considerarse precursora en el reconocimiento de derechos a favor de los más jóvenes; a nivel europeo, la Carta de los derechos del niño, de 8 de julio de 1992, aunque sin valor jurídico, se configura como el documento de referencia; por último, en el ámbito nacional, se han analizado el Código Civil, así como las Leyes orgánicas sobre protección jurídica del menor. Por otra parte, en una segunda dimensión se somete a examen la normativa internacional, europea y nacional que regula el derecho a la protección de datos personales. Comenzando por el ámbito internacional, se aborda el análisis del Convenio 108 del Consejo de Europa como único texto jurídicamente vinculante sobre la materia. En el ámbito europeo, se desarrolla un estudio detenido de la normativa, pues en torno al derecho a la protección de datos personales, la Unión Europea (en adelante, UE) alcanza una posición central en su regulación. Así, se estudian las diversas normas que han otorgado amparo a la información personal en el espacio europeo. Por último, en el ámbito nacional, las tres Leyes orgánicas de protección de datos personales que han estado vigentes en diferentes momentos, se han visto condicionadas por los compromisos internacionales y europeos adquiridos por el legislador español; sin embargo, dado que la normativa europea concede la posibilidad a los Estados de desarrollar de diverso modo determinados aspectos normativos del tratamiento de datos, su estudio se antoja indispensable. Además, cabe señalar que el trabajo se ha encontrado inevitablemente ligado al Derecho constitucional, debido al carácter de derecho fundamental que el derecho a la protección de datos

recogido en el art. 18.4 CE posee. Con todo, el presente trabajo se ha centrado en identificar y analizar, fundamentalmente, la suficiencia del amparo concedido por estos instrumentos normativos a la información personal del menor.

Por otra parte, el estudio y análisis de la doctrina especializada en relación a la materia que nos ocupa se erige como uno de los recursos fundamentales del trabajo. Definitivamente, la doctrina se configura como un recurso indispensable, en especial, para las siguientes materias: para la construcción del derecho a la protección de datos personales en el Estado español; para conceptualizar fenómenos como las redes sociales, el *big data* y la inteligencia artificial (en adelante, IA); así como para el estudio sobre la consagración del derecho al olvido digital en el ámbito europeo y español, entre otros.

Por otra parte, la rápida evolución de estas tecnologías, ha dificultado en ocasiones hallar disponible doctrina para someterla a estudio. Por ello, resultan realmente destacables los valiosos trabajos de organismos oficiales internacionales, europeos y nacionales cuya actividad principal radica en interpretar la normativa sobre protección de datos personales. Puede afirmarse, incluso, que su labor deviene indispensable para la configuración de determinados apartados del presente trabajo. Comenzando por aquellos documentos de ámbito internacional, destacan los trabajos, tanto de la Organización para la Cooperación y Desarrollo Económico (en adelante, OCDE), como de la Organización de las Naciones Unidas (en adelante, ONU); siguiendo con el ámbito europeo, aquellas formuladas por el Grupo de Trabajo del Artículo 29, posteriormente, Comité Europeo de Protección de Datos (en adelante, CEPD); y por último, de carácter nacional, se concede un estudio a los trabajos de las Agencias de protección de datos como la española o francesa e incluso autonómicas como la catalana o vasca.

Finalmente, determinadas materias han precisado del estudio de jurisprudencia tanto europea, encabezada por aquella que mana del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), como nacional, presidida especialmente por la jurisprudencia del Tribunal Supremo (en adelante, TS) y del Tribunal Constitucional (en adelante, TC). Especialmente en relación al derecho al olvido digital, el análisis jurisprudencial ha sido esencial, pues sin ánimo de anticiparnos en exceso, se configura como un derecho cuyo nacimiento se atribuye expresamente al TJUE.

Con el fin de otorgar una respuesta a la hipótesis planteada, el trabajo se estructura como sigue:

En un primer capítulo, se analiza la evolución de la normativa sobre protección jurídica de la infancia y su adaptación al nuevo escenario digital. Sentado que el menor se concibe como un sujeto que ha de recibir una protección especial dada su particular situación en tránsito hacia su madurez, la normativa cuya protección jurídica procura debe otorgarle amparo frente aquellos riesgos más presentes en sus hábitos diarios. Así, considerando al menor titular del derecho fundamental a la protección de datos personales, el presente capítulo centra su estudio en dilucidar si la normativa responsable de proteger los derechos del menor, ampara con suficientes garantías el derecho fundamental a la protección de datos personales tan íntimamente relacionado con el mundo digital y las redes sociales.

El segundo capítulo, por su parte, se centra en analizar la evolución del derecho fundamental a la protección de datos personales en la normativa internacional, europea y nacional, para después estudiar las medidas tendentes a garantizar la protección jurídica de la infancia en su contexto. Ciertamente, habida cuenta que el derecho a la protección de datos personales, se configura como un derecho fundamental de tercera generación de reciente creación, deviene crucial conceder un espacio al análisis de su evolución en orden a evaluar su adaptación a los nuevos contextos en los que debe procurar la protección de la información personal de los interesados; y en particular, frente a los servicios prestados por los proveedores de redes sociales. Lamentablemente, como quedará de manifiesto, las menciones a la minoría de edad en la normativa de referencia, han arribado con manifiesto retraso, lo que ha derivado en unas terribles consecuencias jurídicas para la protección de la información personal de los más jóvenes.

En tercer lugar, puesto que, entre los objetivos del presente trabajo se encuentra analizar la protección de la información personal de los más jóvenes en un contexto en línea concreto, como es el de las redes sociales, el tercer capítulo comienza un examen centrado exclusivamente en estos espacios.

Tras analizar el concepto de red social, así como las principales cuestiones sobre su funcionamiento y los riesgos que su manejo trae consigo- especialmente para la privacidad del menor- el estudio que mediante este trabajo de investigación se proporciona se ha inspirado en conceder un examen a las diferentes fases a las que se enfrenta la información personal del usuario de redes sociales o interesado cuando decide convertirse en partícipe de estas plataformas. Concretamente, nos referimos a las siguientes: un primer momento en el que el usuario se da de alta y consiente el tratamiento

de datos personales; un segundo momento relativo al manejo del servicio, esto es, durante la vigencia de la relación entre el usuario y el proveedor de la red social; por último, cuando el usuario desea, que se supriman determinados datos personales, o bien cancelar la cuenta y abandonar el manejo del servicio.

Con las fases del ciclo de tratamiento como guía, el tercer capítulo profundiza en las vulnerabilidades a las que se enfrentan los datos personales de los usuarios en la primera fase caracterizada por el proceso de darse de alta en el que el usuario deberá consentir el tratamiento de datos personales. Particularmente, se valorará la adecuación y suficiencia de la normativa vigente en lo relativo a la prestación del consentimiento al tratamiento de datos personales cuando este se concede *online* por usuarios menores de edad.

El cuarto capítulo, por su parte, se centra en los tratamientos de datos que se practican en la segunda fase, correspondiente al manejo del servicio por parte del usuario; en nuestro caso, con especial atención cuando este no alcanza la mayoría de edad. Sin intención de desmerecer los riesgos más tradicionales a los que se enfrenta la protección de la información personal cuando un usuario maneja estos servicios, la presente investigación se propone estudiar la suficiencia de la normativa sobre protección de datos personales frente a los nuevos paradigmas de tratamiento de datos personales, encabezados por el empleo de técnicas como el *big data* o la IA.

Concretamente, el presente y el futuro del tratamiento de datos personales viene de la mano del empleo de algoritmos, cada vez más complejos, con distintas aplicaciones prácticas. Efectivamente, los proveedores de redes sociales han diseñado potentes algoritmos en orden a ofrecer una experiencia personalizada en sus espacios, así como para la práctica de publicidad y mercadotecnia directa. Antes bien, las consecuencias del empleo de estas técnicas para el desarrollo del menor, así como para sus derechos fundamentales pueden resultar devastadoras si no se prevén sólidas garantías normativas.

Por último, el quinto capítulo, aborda con especial detalle el análisis de los derechos que se configuran como facultades del contenido esencial del derecho a la protección de datos personales con el fin de asegurar un control de la información personal a su titular. Sin embargo, la rápida evolución de las Tecnologías de la Información y Comunicación (en adelante, TIC), unida a las dificultades que plantea el ejercicio de los mismos por personas que no alcanzan la mayoría de edad, erosiona la eficacia de estas herramientas.

Por otra parte, constituye tarea reservada del presente capítulo, conceder un estudio minucioso del derecho al olvido digital como pieza angular de la última fase del ciclo del tratamiento: el fin de la relación entre el usuario y el proveedor de la red social o el deseo de que se abandone el tratamiento de informaciones compartidas. En efecto, el tráfico desinhibido y constante de información personal, ha alumbrado nuevos retos para el logro de un olvido digital eficaz de la información personal. Así las cosas, se concede un capítulo al estudio, tanto de la evolución del mentado derecho, como de un alcance satisfactorio del mismo en el actual contexto de tratamientos de datos en redes sociales. En particular, se analiza con especial atención la posibilidad de que los más jóvenes ejerciten con éxito este derecho debido al alud de datos personales que de manera constante vuelcan en estos espacios. Cabe esperar así, que el derecho al olvido digital se configure de tal modo que asegure la eficaz supresión de datos personales que, siendo todavía menor se compartieron en la red, pero que ya no se corresponden con la realidad, y por tanto, devienen obsoletos.

En último lugar, se formulan y exponen las principales conclusiones alcanzadas en el trabajo. A través de las mismas, además de responder a la hipótesis que ha servido como guía en la investigación, se articulan una serie de propuestas normativas e inspiradoras para las políticas públicas en orden a asegurar que los tratamientos de datos que los proveedores de redes sociales practican respetan el interés superior del menor como sujeto especialmente necesitado de protección.

CAPÍTULO I:

LA PROTECCIÓN JURÍDICA DEL MENOR ANTE LA ERA DE LA TRANSFORMACIÓN DIGITAL

La consideración de los menores de edad como titulares del derecho fundamental a la protección de datos personales, se configura como una afirmación que no siempre ha gozado de la rotundidad que posee actualmente. Así las cosas, exponer en la presente investigación la evolución experimentada por la normativa de protección jurídica del menor en los últimos años, se presenta como una necesidad de primer orden a efectos de comprender los postulados de la normativa actual sobre protección jurídica de la infancia respecto a los derechos fundamentales. Ya que, a pesar de que en la actualidad no resulte cuestionable que el menor es titular del derecho a la protección de datos personales, no es menos cierto que este derecho fundamental especialmente presente en el siglo XXI, no ha experimentado el desarrollo normativo deseado con el fin de proporcionar una protección específica al menor cuando interactúa con las TIC.

1. LOS ANTECEDENTES HISTÓRICOS DE LA PROTECCIÓN JURÍDICA DEL MENOR

La lucha por la promoción y protección de los derechos de la infancia puede considerarse, desafortunadamente, un acontecimiento relativamente reciente en los ordenamientos jurídicos modernos. Hasta el siglo XX y como consecuencia, principalmente, de las Guerras Mundiales no se visibiliza la necesidad de reconocer y proteger los derechos de los niños y niñas por parte de la Sociedad de Naciones, precedente de la ONU. Tanto es así, que las referencias a los mismos en los instrumentos normativos han resultado escasas o incluso inexistentes a lo largo de la historia jurídico-política[1].

Huelga apuntar que a los menores, como personas y ciudadanos, siempre les han resultado de aplicación las normativas protectoras de derechos íntimamente relacionados con la personalidad en los Estados modernos (aunque tal consideración no se ha sostenido por todas las voces doctrinales[2]). Pero lo verdaderamente destacable reside en que, hasta

[1] En palabras de OCÓN DOMINGO, J. "Normativa internacional de protección e la infancia", *Cuadernos de Trabajo Social,* 2006, vol. 19, p. 114, hasta el siglo XX, denominado «del Niño» y a causa de los estragos sobre millones de niños causados por las guerras mundiales, no se entra en una nueva etapa jurídico política que, paulatinamente, produce una mayor dosis de esperanza en torno a la lucha por la protección y promoción de los derechos de la infancia.

[2] Autores como Hart han sostenido que, plantearse cuestiones sobre derechos de los niños o de los animales resulta una aplicación innecesaria de la palabra "derecho". HART, H.L., "¿Hay Derechos naturales?", *Derecho y Moral. contribución a su análisis,* Buenos Aires, Depalma, 1962, pp. 74-75.

fechas muy recientes nunca había adoptado ninguna normativa cuyo objeto radicara de manera específica en la protección de la infancia.

En este devenir, a principios del siglo XX, el entorno jurídico-político sufre un cambio de paradigma como consecuencia de los sucesivos conflictos bélicos. La devastación ocasionada por las guerras en diversos ámbitos potencia la necesidad de cambio en los Estados modernos. A raíz del señalado momento, el menor adquiere visibilidad y, en consecuencia, organismos internacionales como la Sociedad de Naciones trasladan a los Estados la necesidad de atender a la protección de dicho colectivo por medio de textos normativos. No obstante, la protección de la minoría de edad no se articula, en ese momento, mediante textos específicos cuyo ámbito subjetivo se circunscribe únicamente a menores de edad, sino que cabe destacar las menciones a la minoría de edad en textos como la Declaración de los Derechos Humanos de 10 de diciembre de 1948[3] o el Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966, aprobado por la Asamblea General de las Naciones Unidas[4], sobre los que volveremos posteriormente.

En adición a lo expuesto, el siglo XX impulsa a la ONU a la creación de organizaciones especializadas relacionadas con la protección de la infancia, entre las que destaca la conocida *United Nations Children´s Fund,* UNICEF (Fondo de las Naciones Unidas para la Infancia en español) creada en Nueva York el 18 de agosto de 1946. El objetivo principal de esta organización se identifica con lograr una mayor seguridad y protección de la infancia a través de la defensa de los derechos de los niños y niñas. En ese sentido, desde sus comienzos, UNICEF impulsa la mejora de políticas y servicios dirigidos a proteger a todos los niños y niñas del mundo para que crezcan en un mundo seguro.

2. LA PROTECCIÓN DE LA INFANCIA EN EL ÁMBITO JURÍDICO INTERNACIONAL

Tal y como se ha expuesto en el apartado anterior, los Organismos Internacionales fomentaron la articulación de mecanismos de protección de menores que posteriormente

[3] Resolución 217 A (III) de la Asamblea General de las Naciones Unidas, por la que se adopta la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948.
[4] Pacto Internacional de Derechos Civiles y Políticos de la Organización de las Naciones Unidas, de 19 de diciembre de 1966, Instrumento de adhesión de España de 28 de septiembre de 1976, Boletín Oficial del Estado, 30 de abril de 1977, núm. 103, pp. 9337-9343.

servirían a los Estados para desarrollar sus normativas protectoras de la infancia. No obstante, hasta épocas muy recientes, no han comenzado a aprobarse textos normativos cuyo ámbito subjetivo se circunscriba, exclusivamente, a los menores de edad. Como quedará de manifiesto, ello ha influido de manera decisiva en la construcción de un sistema jurídico protector de la infancia.

2.1. Aproximación a la normativa internacional sobre protección jurídica del menor

En el año 1919, la Sociedad de Naciones, de manera pionera, muestra interés en mejorar la situación de los niños y niñas, creando a tal fin el Comité de Protección de la Infancia[5]. Así las cosas, la Sociedad de Naciones se posiciona como la primera institución encargada de aprobar la primera Declaración de Derechos del Niño, firmada en Ginebra el 24 de septiembre de 1924 en su V Asamblea[6], en respuesta principalmente, al desamparo causado por la Primera Guerra Mundial en millones de menores. Por ese motivo, el objeto principal de la Declaración se identifica con la concesión de una protección especial a cualquier menor abandonado. En la aprobación de dicha Declaración, influyó decisivamente la organización internacional *Save the Children* encabezada por la activista Engantyne Jebb-fiel defensora en la articulación de una visión particular de la niñez y las formas de tratarla-abogando por la necesidad de garantizar los derechos de los niños independientemente del contexto en el que se encuentren[7].

Años más tarde, después de la Segunda Guerra Mundial, ONU advirtió la necesidad de proteger los derechos fundamentales de todos los miembros de la familia a través de la Declaración de los Derechos Humanos de 10 de diciembre de 1948. Sin embargo, no se configura este como un texto dirigido única y exclusivamente a menores, sino que su articulado acoge todos aquellos derechos de los que cualquier individuo posee la titularidad. A pesar de ello, el art. 25.2 de la Declaración de Derechos Humanos de 1948, concretamente, dispone que la maternidad y la infancia merecen derecho a cuidados y

[5] TIANA FERRER, A., "Declaración de los Derechos del Niño y Convención sobre los Derechos del Niño", *Transatlántica de educación*, 2008, vol. 5, p. 96.

[6] Declaración de los derechos del niño firmada en Ginebra el 24 de septiembre de 1924 aprobada por la Sociedad de Naciones. Obtenido de: https://www.ciprodeni.org/wp-content/uploads/2018/08/Declaracion-de-Ginebra-1924.pdf (última consulta el 4 de julio de 2022).

[7] Para mayor detalle, véase el documento sobre "La primera carta de los derechos del niño" de *Save the Children*. Obtenido de: https://www.savethechildren.es/sites/default/files/imce/docs/primera_carta_derechos_del_nino-.pdf (última consulta el 27 de noviembre de 2022).

asistencia especiales, y que todos los niños, nacidos dentro o fuera de matrimonio, se encuentran provistos del derecho a una igual protección social. Como se ha afirmado anteriormente, el presente texto no circunscribe su aplicación de manera exclusiva y específica a menores, pero la diferencia con los anteriores se halla en que en su articulado se advierte la necesidad de protección de dicho colectivo.

Tras un dilatado debate sobre si los derechos de los menores se encontraban amparados en la Declaración de Derechos Humanos de 1948, como ampliación de este texto, la Resolución 1386 (XIV) de la Asamblea General de las Naciones Unidas aprueba la Declaración de los Derechos del niño el 20 de noviembre de 1959[8], texto que, adquirirá gran influencia en la posterior legislación sobre protección jurídica de la infancia. El objetivo de la Declaración de 1959, en palabras de PALOMAR OLMEDA reside en que los niños puedan tener una infancia feliz, instando a los progenitores, personas, organizaciones particulares, autoridades locales y gobiernos nacionales al reconocimiento de esos derechos, así como a la lucha por su observancia[9].

Así, la Declaración de 1959, reconoce un amplio catálogo de derechos que los niños habrán de disfrutar sin discriminación, ahora bien, la proclamación de derechos resulta sumamente abstracta y generalista, pues no incide suficientemente en políticas específicas de protección de la infancia que lleven a los Estados a cumplir tales consideraciones[10]. Antes bien, la Declaración de los Derechos del Niño de 1959, no gozó de la aplicabilidad deseada, debiéndose ello principalmente a que el texto no presentaba carácter vinculante para los Estados.

El Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966, aprobado por la Asamblea General de las Naciones Unidas, por su parte, también refleja en su articulado la preocupación por la protección de los menores a pesar de no considerarse como una normativa destinada específicamente a la protección de los mismos. En concreto, el art. 24 expresa dicha preocupación por la protección de la minoría de edad cuando establece que todo menor posee derecho a las medidas de

[8] Resolución 1386 (XIV), de la Asamblea General de las Naciones Unidas sobre la Declaración de los Derechos del Niño, de 20 de noviembre de 1959.
[9] PALOMAR OLMEDA, A., "La protección del menor ¿avanzamos o retrocedemos?", *Revista Aranzadi de Derecho de deporte y Entretenimiento,* 2019, núm. 62, p. 4.
[10] *Ibid*, p 5.

protección que por su condición de menor requiera, no importando a tal efecto su raza, color, sexo, origen, posición económica o nacimiento[11].

Sentado cuanto antecede, los mencionados textos internacionales y en especial, la Declaración de los Derechos del niño de 1959, influyeron decisivamente en la aprobación de la Convención de las Naciones Unidas sobre los Derechos del niño, de 20 de noviembre de 1989 (en adelante, Convención de 1989)[12]. Dicho cuerpo normativo se convierte en el Convenio de Derechos Humanos con mayor número de Estados rafiticantes de la historia, afectando al 96% de niños del mundo[13]. Si bien la Convención de Derechos del niño se proclama como uno de los instrumentos más relevantes en materia de derechos de los menores, no cabe considerarlo como el último cuerpo normativo regulador de los mismos. A medida que discurre el siglo XX, la regulación de la protección de los derechos fundamentales de los más jóvenes evoluciona de manera paulatina. Como responsables de dicho progreso destacan, entre otras, las Reglas mínimas de las Naciones Unidas para la Administración de Justicia de Menores, de 28 de noviembre de 1985[14], sobre las que volveremos más adelante y el Convenio relativo a la Protección del niño y a la cooperación en materia de Adopción Internacional , de 29 de mayo de 1993[15].

2.2. El alcance de la Convención de los Derechos del Niño de 1989 respecto a los derechos fundamentales relacionados con la privacidad de los menores de edad. ¿Un texto jurídico adaptado al contexto tecnológico actual?

La falta de obligatoriedad en el cumplimiento de la Convención de 1959, motivó que, entre otras cuestiones, en 1978 el gobierno de Polonia impulsara la aprobación de la Convención de los Derechos del Niño de 1989. En la víspera del "Año internacional del

[11] Véase el art. 24 del Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966 de las Naciones Unidas.

[12] Convención de 20 de noviembre de 1989 de las Naciones Unidas sobre los Derechos del Niño. Instrumento de ratificación de España, de 26 de enero de 1990, Boletín Oficial del Estado, 31 de diciembre de 1990, núm. 313, p. 38897.

[13] OCÓN DOMINGO, J. "Normativa internacional de protección de la infancia", *op. cit.*, p. 117.

[14] Resolución 40/33 adoptada por la Asamblea General de las Naciones Unidas sobre Reglas mínimas de las Naciones Unidas para la administración de la justicia de menores (Reglas de Beijing), de 28 de noviembre de 1985. Obtenido de: https://www.bienestaryproteccioninfantil.es/imagenes/tablaContenidos03SubSec/Reglas_minimas_NU_Beijing.pdf (última consulta el 28 de septiembre de 2022).

[15] Convenio, sobre protección del niño y cooperación en materia de adopción internacional, hecho en La Haya, de 29 de mayo de 1993, Instrumento de ratificación de España, de 27 de marzo de 1995, Boletín Oficial del Estado, 1 de agosto de 1995, núm. 182, p. 23447.

niño" celebrado en 1979, este gobierno propone transformar la Declaración de 1959 en un texto jurídicamente vinculante. A pesar de que, dicha propuesta no prosperó, el gobierno polaco continuó trabajando sobre la propuesta efectuada, presentando el *Second Polish Draft*, documento que albergaba en su seno cuestiones como los derechos individuales de los niños, así como un mayor protagonismo de la familia; cuestión que, sin duda sentaría las bases para el posterior desarrollo de la Convención de 1989[16].

Ante el fracaso del gobierno de Polonia en el intento por instaurar una obligatoriedad jurídica de la Convención de 1959, se procedió a la conformación de un Grupo de Trabajo en el marco de la Comisión de Derechos Humanos de la ONU, principal responsable de la redacción de la Convención de 1989. En este período de elaboración del texto, también debemos destacar la participación activa de treinta Estados, dos organizaciones internacionales intergubernamentales como UNICEF y la Organización Internacional del Trabajo (en adelante, OIT) y, por último, las quince organizaciones internacionales no gubernamentales.

La relevancia de la Convención de los Derechos del niño, de 20 de noviembre de 1989 no radica únicamente en la gran amplitud de ratificación lograda. Jurídicamente, cabe destacar que se considera el primer instrumento internacional que reconoce las prerrogativas que se exponen a continuación.

En primer lugar, reconoce a los niños y niñas como titulares de sus propios derechos. Hasta la fecha, ningún cuerpo normativo consideraba al menor como titular de derechos de la personalidad. En segundo lugar, manifiesta la necesidad de proteger especialmente a los menores de edad como sujetos particularmente vulnerables por encontrarse en pleno tránsito hacia la madurez. Por último, señala la condición jurídica y social del niño, afirmando que, si bien carece de plena autonomía, es sujeto de derechos. Esta última afirmación supone un gran hito en el reconocimiento de la capacidad del menor, ya que se abandona el esquema tradicional que considera a este como una persona incapacitada en el plano jurídico, para conferirle determinada capacidad a medida que adquiere paulatinamente determinada madurez.

Desde luego, el cambio de paradigma resulta destacable en el sentido que, tal y como explica HIERRO SÁNCHEZ-PESCADOR, antiguamente quedaba entendido que,

[16] BARNA, A., "Convención Internacional de los Derechos del Niño. Hacia un abordaje desacralizador", *Revista de Temas Sociales*, 2012, núm. 29, pp. 10-12.

los menores de edad carecían de la autonomía necesaria a efectos de considerarlos titulares de derechos como la libertad de expresión, la libertad de asociación o reunión, el derecho de sufragio, etc., reservando la titularidad de derechos humanos únicamente a individuos adultos[17]. La situación hoy en día , en cambio, ha evolucionado ya que, puede afirmarse que, si bien la capacidad del menor quedará sujeta a las condiciones de madurez que este presente en determinado momento de su vida como menor, ello no afectará a la titularidad de derechos fundamentales que se reconocerá independientemente de dicha capacidad[18].

El punto de inflexión generado por la Convención de 1989 resulta más que destacable. A partir de ese momento, toda la normativa posterior dirigida a menores, tanto internacional como de los Estados ratificantes, girará en torno a las mencionadas premisas: el menor se considera ahora titular de sus derechos de la personalidad, pero al mismo tiempo, un sujeto vulnerable y digno de especial protección por el ordenamiento jurídico. Por último, su capacidad no es plena para el ejercicio de derechos de manera autónoma, pero existe y, además, evolucionará a medida que el menor cumpla progresivamente determinada edad.

A lo expuesto cabe añadir cinco principios normativos básicos que la Convención dispone: el primero de ellos se identifica con la protección universal de menores por parte de los Estados que han ratificado la Convención. En segundo lugar, la prevalencia del interés superior de los niños y niñas, concepto que como se verá posteriormente adquiere carácter de principio inspirador de la normativa nacional. En tercer lugar, la subsidiariedad de los Estados; y, por último, los principios de vigilancia, evaluación y exigencia de responsabilidades con el fin de garantizar el cumplimiento de la Convención.

En cumplimiento de esta última premisa, en virtud del art. 19 de la Convención, los Estados deberán adoptar las medidas legislativas, administrativas, sociales y culturales apropiadas para articular la protección de los menores[19]. Esta obligación reviste

[17] HIERRO SÁNCHEZ-PESCADOR, L., "¿Tienen los niños Derechos? Comentario a la Convención sobre los Derechos del niño", *Revista de Educación,* 1991, núm. 294, pp. 225-226.

[18] El art. 12 de la Convención de 20 de noviembre de 1989 de la Organización de las Naciones Unidas sobre los Derechos del Niño, dispone que «Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio, el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño». Véase en ese sentido también MARCOS MARÍN, T., "Los derechos de la personalidad de las personas-menores en el contexto internacional y su aplicación en el ordenamiento español*", Menores e Internet,* 1ª edición, Pamplona, Editorial Aranzadi, 2013, p. 5.

[19] OCÓN DOMINGO, J. "Normativa internacional de protección de la infancia", *op. cit.*, p. 118.

especial importancia, dado que los Estados ratificantes de la presente Convención, entre los que se encuentra España desde 1990, implementarán sus propias normativas protectoras de los derechos que en la Convención se contienen, articulando para ello normativas propias de protección jurídica de la infancia. Sobre ello volveremos posteriormente.

Con todo, si bien es cierto que la Convención de 1989 logra un mayor reconocimiento internacional de los derechos de la infancia a causa de su carácter vinculante, a nuestro juicio, dos son los recelos que nos suscita el texto. En primer lugar, la Convención de 1989, no garantiza suficientemente los mecanismos concretos a través de los cuales los Estados deberán proteger realmente estos derechos. En segundo lugar, la convención de 20 de noviembre de 1989, continúa considerándose el texto internacional de referencia en torno a los derechos de la infancia.

Sobre el primero de los recelos, sirva como ejemplo que, en octubre de 1994, la Delegación española manifestó su preocupación en torno a las políticas de protección y promoción de los derechos de los niños españoles entre las que merecen especial atención, por una parte, la preocupación del Gobierno Español por la posible incompatibilidad entre el art. 19 de la Convención y el art. 154 del Código Civil que brindaba entonces la posibilidad a los progenitores de castigar moderadamente a los hijos; por otra parte, la necesidad de programas y servicios especiales de protección y cuidados necesarios en familias monoparentales[20].

Sin embargo, el mecanismo de garantía que prevé la Convención de 1989 en pos de alcanzar un cumplimiento efectivo de su articulado en lo que a la lucha por los derechos y protección de la infancia se refiere, se identifica con la remisión por parte de los Estados de informes periódicos. En estos, los Estados deberán notificar al Comité de las medidas adoptadas, así como el progreso en el reconocimiento y protección de los derechos de la infancia. Así, queda en evidencia que, la Convención de 1989, con el fin de guiar a los Estados en este nuevo quehacer, debía precisar con mayor rigor los mecanismos que coadyuvaran a garantizar de manera efectiva estos derechos.

En efecto, si bien se debe destacar la labor protagonizada por la ONU en el reconocimiento de derechos fundamentales de la minoría de edad, dicha circunstancia debe garantizarse mediante mecanismos que salvaguarden el cumplimiento de los

[20] *Ibid*, p.119.

mismos. De lo contrario, las diferencias entre la Declaración de los Derechos del Niño de 1959, en la que, no se prevén mecanismos que garanticen la protección real de los derechos y la Convención de 20 de noviembre de 1989 no es tal. Esto es, los mecanismos dirigidos a garantizar los derechos de la minoría de edad deben proporcionar una alta efectividad de cumplimiento y respeto de los mismos en los ordenamientos nacionales. Sin dicha efectividad, el reconocimiento de dichos derechos queda relegado a una declaración no garantista y generalista de derechos, que puede conducir a vulneraciones y una aplicación no efectiva de la Convención.

Respecto al segundo recelo expresado anteriormente, la Convención de 20 de noviembre de 1989, continúa recibiendo la consideración de texto internacional de mayor referencia en lo que a derechos de la infancia se refiere. Tras 34 años de vigencia del cuerpo normativo, la sociedad ha sufrido una vertiginosa evolución en la que se han visto implicados los derechos de los menores; sin embargo, dichos cambios no se reflejan en la Convención de 20 de noviembre de 1989. Sin lugar a dudas, la protección de los derechos de los menores de edad en entornos digitales se presenta como uno de los ámbitos que carecen tanto de reconocimiento, como protección suficiente en la normativa internacional de referencia a pesar de encontrarnos inmersos en plena era digital.

Expuesto cuanto antecede, la Convención de Derechos del niño contiene un único precepto que incide en el ámbito de la privacidad del menor. El art. 16 de la Convención de derechos del niño señala que, ningún menor sufrirá injerencias arbitrarias o ilegales en su vida privada, familia, domicilio o correspondencia.

Como puede apreciarse, la Convención refleja el derecho a la privacidad del menor como un derecho de la personalidad del mismo, digno de tutela y especial protección dada la condición del titular en el que se reconoce. No obstante, en el momento en el que se procedió a la redacción de dicho precepto, no se alcanzaba a imaginar la crucial relevancia que los derechos de la privacidad del menor adquirirían con el cambio de siglo. Por ello, indispensablemente, estos derechos propios del siglo XXI tan presentes en el día a día de los menores e íntimamente relacionados con la era digital, se han de acoger de manera actualizada en la normativa de referencia internacional de protección de derechos del menor. Véase que el precepto de la Convención de 1989 que alude a injerencias arbitrarias o ilegales en la vida privada de los menores, la de sus familias, correspondencia o domicilio, puede considerarse una garantía de protección de una esfera

íntima amplia en el siglo XX. En cambio, no puede considerarse suficiente en la actualidad, ya que las intromisiones en la vida privada de los menores de edad pueden ocurrir en el entorno *online* sobre el que la normativa guarda silencio, pues esta no se ha modificado tras más tres décadas de vigencia de la misma.

Es cierto que, en épocas recientes el Comité de los Derechos del Niño, aprueba el 2 de marzo de 2021 la Observación general número 25, relativa a los derechos de los niños en relación con el entorno digital[21]. La misma, sienta como objetivo principal orientar a los Estados partes en la aplicación de la Convención de 1989 en relación con el entorno digital, para lo que ofrece apoyo sobre las medidas legislativas, normativas y de otra índole destinadas a garantizar el cumplimiento de la Convención. En ese sentido, el apartado 23 de la citada Observación general invita a los Estados partes a aprobar legislación nacional, y a revisar y actualizar la existente, a fin de garantizar un entorno digital compatible con los derechos previstos en la Convención de 1989. Sin embargo, sobre este particular, recordemos que la privacidad se regula en este texto desde un prisma tradicional en este texto.

Sin perjuicio de lo expuesto, esta Observación general constituye un avance, pues la misma, a diferencia del Informe del Secretario General de la ONU, de 24 de agosto de 2017, sobre la Situación de la Convención sobre los Derechos del Niño a solicitud de la Asamblea General[22], sí que prevé un apartado expreso sobre la privacidad del menor en el entorno en línea. Sin embargo, lamentamos que los riesgos que este entorno digital genera para el menor, no hayan impulsado al organismo internacional a auspiciar la actualización del texto jurídico de referencia en torno a la protección jurídica de la infancia: la Convención de 1989. Antes bien, la Observación general visibiliza al fin, riesgos que el entorno digital presenta para el desarrollo del menor en la actualidad. Sobre este texto volveremos en apartados posteriores.

En otro orden de cosas, sobre el derecho a la intimidad resultan de obligada mención, por su carácter posterior a la Convención de 1989, las Reglas Mínimas para la

[21] Observación general número 25, del Comité de los Derechos del Niño, de 2 de marzo de 2021, relativa a los derechos de los niños en relación con el entorno digital. Obtenido de: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12 (última consulta el 2 de febrero de 2023)

[22] Informe del Secretario General de las Naciones Unidas, sobre la Situación de la Convención sobre los Derechos del niño, presentado en el septuagésimo segundo periodo de sesiones en relación a la Promoción y protección de los derechos del niño, de 24 de agosto de 2017.

Administración de Justicia a Menores mencionadas anteriormente, en concreto la regla número 8, puesto que, el texto se detiene, junto con otros derechos, en el de la protección de la intimidad del menor[23]. Sin embargo, el derecho a la intimidad de los menores de edad que en estas líneas se reconoce, presenta una aplicabilidad concreta en el ámbito de la Administración de Justicia, motivo por el que no constituirá objeto de estudio de la presente investigación.

En los textos expuestos se sitúa el origen, aunque tímido, del reconocimiento legislativo al derecho a la intimidad personal y familiar de los menores como titulares de dicho derecho. Ahora bien, actualmente la protección del derecho a la intimidad de los menores de edad que la Convención de 1989 trata de garantizar no preserva este derecho de los menores de edad de manera suficiente ni acomodada a los nuevos modos en los puede verse especialmente vulnerado, cuestión que, abordaremos más adelante por encontrarse en íntima relación con el derecho a la protección de datos personales.

3. LA CONFIGURACIÓN DEL MARCO NORMATIVO EUROPEO DE PROTECCIÓN JURÍDICA DE LOS MENORES

Las instituciones europeas también han desarrollado una gran labor en la construcción de un marco de desarrollo de los derechos fundamentales en el ámbito comunitario. Especialmente en los últimos años, los menores resultan objeto de preocupación de las instituciones europeas como colectivo necesitado de protección, motivo por el que la UE ha regulado los derechos de la personalidad de los menores con especial cuidado y atención.

En ese sentido, señalar que, al igual que sucede en los textos de ámbito internacional en relación a los derechos fundamentales, no todos los textos comunitarios que recogen los derechos de la personalidad circunscriben su ámbito de aplicación de manera exclusiva a menores. En consecuencia, tal y como se ha abordado en el apartado anterior, proponemos en este estudio un recorrido, en primer lugar, por los cuerpos normativos que no se circunscriben específicamente a menores, pero en los que se disponen derechos de estos, para posteriormente, incidir en aquellos textos que regulan

[23] SÁNCHEZ GÓMEZ, A., "El marco normativo tradicional para la protección de los derechos de la personalidad del menor. ¿Alguna asignatura pendiente en el siglo XXI?", *Revista Doctrinal Aranzadi Civil-Mercantil,* 2016, núm. 11/2016 parte Doctrina, p. 2.

de manera específica derechos de menores como sujetos necesitados de protección añadida.

3.1. Primeros pasos de la Unión Europea en la regulación de derechos fundamentales del menor

El Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, cuya entrada en vigor data del 3 de septiembre de 1953, y ratificado por España el 24 de noviembre de 1977 se posiciona como el primer texto en procurar protección y desarrollo a los derechos humanos y libertades fundamentales en el ámbito europeo[24]. Para esta labor, las instituciones europeas tomaron como referencia los contenidos de la Declaración de los Derechos Humanos de 1948 mencionada anteriormente.

Como cabía esperar, el citado texto se caracteriza por su aplicabilidad general a los individuos, sin considerarse un texto destinado específicamente a menores[25]. En lo que a derechos de los niños se refiere, cuenta en su articulado con diversos preceptos que aluden de forma directa a la minoría de edad. Entre ellos, destacaremos aquellos que guardan relación con el presente estudio: por una parte, el art. 8 referente a la vida privada y familiar; y, por otra parte, el art. 9.2 regulador de la libertad de pensamiento, conciencia y de religión. Además, para su efectivo cumplimiento, el Convenio se dota de dos órganos: una Comisión Europea y un Tribunal Europeo de Derechos Humanos (en adelante, TEDH) con el fin de que cualquier persona u organización cuyos derechos sufran un menoscabo puedan exigir su cumplimiento ante las mentadas instancias. Es de apreciar que, el art. 8 propugna la protección de la vida privada y familiar, en la que podemos considerar incluidos a los menores como integrantes de la unidad familiar[26].

Pocos años más tarde, el 18 de octubre de 1961, se firma en Turín la Carta Social Europea. A pesar de que su entrada en vigor a nivel comunitario data del 26 de febrero de 1956, el Estado español no ratifica el señalado texto hasta el 27 de abril de 1980[27]. Su

[24] Convenio sobre la Protección de los derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950, hecho en Roma. Instrumento de adhesión de España de 24 de noviembre de 1977, Boletín Oficial del Estado, de 10 de octubre de 1979, núm. 243.
[25] Véase FERNÁNDEZ PÉREZ, A., "La protección de los derechos fundamentales de los menores en internet desde la perspectiva europea". *Revista Ius et Praxis,* 2016, núm. 1, pp. 383-384.
[26] Véase el art. 8 del Convenio de 4 de noviembre de 1950, sobre la Protección de los derechos Humanos y las Libertades Fundamentales, hecho en Roma citado anteriormente.
[27] Carta Social Europea, de 18 de octubre de 1961, hecha en Turín. Instrumento de Ratificación de 29 de abril de 1980, Boletín Oficial del Estado, de 26 de junio de 1980, núm. 153.

articulado regula la minoría de edad en diversos apartados, destacando a tal efecto el art.7, que recoge los derechos de los niños y niñas y adolescentes a una protección especial contra los peligros físicos y morales a los que pueden verse expuestos cuando desarrollan una actividad laboral. De modo similar, el art. 17, consagra el derecho a la protección social y económica de la madre y los niños, reiterando la necesidad de proteger el entorno del niño mediante la proposición de medidas para la creación o mantenimiento de instituciones o servicios adecuados.

Sin embargo, el devenir de los años, ha conducido a la UE a dotar, todavía de una mayor relevancia la necesidad de protección del menor. Sirvan como ejemplo, sin ánimo de exhaustividad, los textos que se exponen a continuación.

En primer lugar, el apartado segundo del art. 3.3 del Tratado de la Unión Europea firmado en Maastricht el 7 de febrero de 1992[28] (en adelante, TUE), prevé en su articulado dicha protección, disponiendo que la UE combatirá la exclusión social y la discriminación, fomentando la justicia y la protección sociales, la igualdad entre mujeres y hombres, así como la solidaridad entre generaciones y la protección de los derechos del niño[29].

En segundo lugar, la Carta de los Derechos Fundamentales de la UE del año 2000, establece en su art. 24 tres principios básicos sobre los derechos de los niños: el derecho a expresar libremente su opinión en función de su edad y madurez (apartado primero), el derecho a que su interés superior constituya una consideración primordial en todo acto que le concierna (apartado 2) y el derecho a mantener relaciones personales, de manera periódica con sus progenitores (apartado 3)[30].

Por último, merecen especial mención las Directrices de la Unión Europea sobre los derechos del menor aprobadas por el Consejo el 10 de diciembre de 2007 cuyo objetivo reside en reforzar las actividades de la UE para la promoción y protección de los

[28] Tratado de Maastricht, de 7 de febrero de 1992 por el que se modifica el Tratado de la Unión Europea, Diario Oficial de las Comunidades Europeas, C/191/1, de 29 de julio de 1992.
[29] Tratado de Maastricht, de 7 de febrero de 1992, por el que se aprueba el Tratado de la Unión Europea, Diario Oficial de la Unión Europea, C/191, de 29 de julio de 1992.
[30] Manual de legislación europea sobre los derechos del niño de la Agencia de los derechos fundamentales de la UE. Año 2015. Obtenido de: https://www.echr.coe.int/Documents/Handbook_rights_child_SPA.PDF (última consulta el 1 de septiembre de 2022).

derechos del menor, complementando a tal efecto las directrices de la UE relativas a los niños y los conflictos armados y la Agenda de la UE en pro de los derechos del niño[31].

Sin embargo, ninguno de los cuerpos legales se refiere específicamente al derecho a la intimidad o privacidad de los menores de edad. Definitivamente, los derechos relacionados con la privacidad del menor han sufrido durante años un notorio abandono en el seno de la UE, pues durante años, la protección conferida a los menores de edad se ha centrado en los derechos fundamentales más tradicionales y no en aquellos derechos que pueden sufrir vulneraciones ante la expansión en el empleo de las TIC.

3.2. La privacidad de los menores en la Carta Europea de los Derechos del Niño, de 8 de julio de 1992. Su escaso valor como texto jurídico para la protección jurídica de la infancia en un entorno digital

La Carta Europea de los Derechos del Niño, de 8 de junio de 1992 (en adelante, la Carta Europea de los Derechos del Niño[32]), se configura como una Resolución del Parlamento Europeo por la que se solicita a los Estados miembros que lleven a cabo determinadas acciones con el fin de permitir un desarrollo equilibrado de los menores. Cabe señalar que el mencionado texto, sufre una marcada influencia de la Convención de Derechos del Niño de 1989 en el ámbito internacional, situándose como el cuerpo normativo regulador de los derechos de los niños por antonomasia en el ámbito comunitario. El propio texto recuerda que, la UE instó a los Estados miembros a que se adhirieran a la Convención de 1989, reservándose la tarea de que la UE procediera igualmente cuando todos los Estados hubieran ratificado el texto. A pesar de ello, el propio texto advierte sobre la necesidad de proteger a los menores en el ámbito comunitario, máxime en el proceso de integración comunitaria, que puede incidir negativamente sobre los menores.

Sentado cuanto antecede, la Carta Europea de los Derechos del Niño recoge cuatro considerandos de necesaria reproducción en las siguientes líneas, a saber: la infancia de

[31] En ese sentido, véanse las Directrices de la UE para la promoción y protección de los derechos del menor, aprobadas por el Consejo el 10 de diciembre de 2007, no publicadas en el Diario Oficial de la Unión Europea. Obtenido de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l33604&from=ES (última consulta el 2 de septiembre de 2022).
[32] Véase la Carta Europea de los Derechos del Niño, aprobada el 8 de julio de 1992, Boletín de las Comunidades Europeas, C 241, de 21 de septiembre de 1992 cuando establece que: «Todo niño tiene derecho a ser protegido contra la utilización de su imagen de forma lesiva para su dignidad».

todo individuo y las circunstancias del entorno familiar de cada uno determinan en gran medida la posterior vida de adulto. En segundo lugar, destaca el papel primordial de la familia y su influencia en el desarrollo de los menores, matizando que los niños constituyen una categoría sensible de la población con necesidades específicas que han de satisfacerse y recibir protección. Por último, destaca los textos internacionales que recogen las necesidades de los niños como fundamento de creación de derechos para estos. Como consecuencia de ello, los derechos de los niños generan obligaciones para los progenitores, el Estado y la sociedad.

Entre el amplio catálogo de derechos que recoge, merecen un análisis riguroso aquellos que guardan relación con la privacidad del menor. En este orden de cosas, la Carta Europea de los Derechos del Niño reconoce el derecho a la protección de la identidad del menor, a la libertad de conciencia, pensamiento y religión, así como el derecho a que su imagen no se emplee de forma lesiva para su dignidad en su art. 7.20.

Al igual que sucede con la Convención de 1989, la normativa comunitaria no repara especialmente en aquellos derechos de la personalidad íntimamente relacionados con la privacidad de los menores. Ciertamente, la Carta Europea de los Derechos del Niño se decanta por una regulación más general que trata con vaguedad las intrusiones injustificadas en la vida privada de los menores de edad. Es decir, mientras que la Convención de 1989 mencionaba el ámbito en el que dichas intrusiones podían acontecer (domicilio, comunicaciones…) la Carta Europea de los Derechos del Niño no especifica ninguno de los ámbitos en los que dichas intromisiones pueden ocurrir. A dicha ausencia de mención, cabe adicionar, que las probabilidades de que la vida privada de los menores de edad sufra injerencias resulta realmente elevada cuando navegan por la red o son usuarios de las redes sociales, cuestión que abordaremos más adelante.

Desde luego, esta ausencia de mención a la privacidad *online* en el año 1992 se debe a que, por aquel entonces, las TIC no se percibían como una amenaza para la privacidad, pues no se podía conocer, ni siquiera imaginar, el posterior impacto que estas poseerían en los derechos de las personas. De modo que, los cuerpos normativos se centraron más en asentar aquellos derechos fundamentales tradicionales básicos para toda la sociedad y en especial para los menores posteriormente. Sin embargo, la vaguedad con la que la Carta Europea de los Derechos del Niño continúa regulando actualmente la privacidad de los menores de edad, no aporta más que inseguridad, pues la Carta Europea

de los Derechos del Niño continúa considerándose como el texto de referencia en la defensa y protección de derechos fundamentales de los menores de edad en la UE. Sobre esta última afirmación, no debemos olvidar que, la Carta Europea de los Derechos del Niño se configura como una Resolución que carece de carácter vinculante. De modo que, la defensa de los derechos de los menores de edad, en el seno europeo, no se configura por medio de un texto específico destinado a menores que garantice dicha protección[33].

En otro orden de consideraciones, la Comisión Europea adoptó la Agenda de la UE en pro de los Derechos del Niño, que contiene los postulados básicos de la legislación sobre los derechos del niño[34]. Concretamente, mediante dicha comunicación, la UE afirma que entre sus objetivos se encuentra el fomento y la protección de los derechos del niño, para cuyo fin dispone que las políticas de la UE que afecten a los niños y niñas deben concebirse, aplicarse y resultar controladas conforme al principio del interés superior del menor. Así, destacar que la UE desea integrar los derechos del niño en la política de la UE en materia de derechos fundamentales. Para ello, la Comisión propone que, cuando proceda, la exposición de motivos de las propuestas legislativas pertinentes, explicarán cómo se han tomado en consideración los derechos del niño en la redacción de las propuestas. Sin embargo, deseamos destacar que, tal y como dispone el texto traído a colación, el 76% de los niños y niñas europeos no conocían que se les reconoce la titularidad de derechos. A lo que el 88% propuso que la UE debía facilitar más información a los menores sobre sus derechos de manera accesible[35].

Ahora bien, la normativa europea tendente a la protección del menor se encuentra dispersa en diversos textos en el marco de iniciativas políticas y económicas de mayor calado[36], lo que lleva a una falta de garantía sólida de los derechos fundamentales de los

[33] Como se verá en apartados posteriores, la defensa de los derechos fundamentales de los menores de edad se aborda mediante la Carta Europea de Derechos Fundamentales a partir del año 2000, pero no se configura como una Carta cuyos únicos destinatarios se consideren los menores de edad, sino todos los individuos.
[34] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre "Una agenda de la UE en Pro de los derechos del Niño, de 15 de febrero de 2011, COM (2011) 60 final.
[35] En ese sentido, la Comisión propuso, durante el año 2011, la creación de un punto único de acceso en Europa para toda la información destinada a los niños en la UE sobre los derechos del niño. Sin embargo, a pesar del transcurso de una década, no se ha procedido a la creación de la señalada web. Véase la página web de la comisión europea donde establece la próxma creación de dicha web: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/rights-child/eu-action-rights-child_es (última consulta 13 de abril de 2021).
[36] Véase el Manual de legislación europea sobre los derechos del niño, de la Agencia de los derechos fundamentales de la Unión Europea. Año 2015. Obtenido de: https://www.echr.coe.int/Documents/Handbook_rights_child_SPA.PDF, pp.20-24 (última consulta el 1 de septiembre de 2022).

menores de edad de conformidad con las particulares circunstancias de estos y a los riesgos que pueden poner en peligro los mismos.

4. LA NECESARIA INCORPORACIÓN DEL MODELO INTERNACIONAL DE PROTECCIÓN JURÍDICA DE LA INFANCIA A LA LEGISLACIÓN ESPAÑOLA

En el ámbito estatal, pese al retraso ocasionado por la dictadura franquista en el desarrollo de la normativa sobre protección de la infancia, paulatinamente se estableció un sistema de protección de menores inspirado principalmente en la Convención de los Derechos del Niño de 1989[37].

4.1. La protección de los derechos fundamentales del menor en la Constitución Española

La Constitución Española de 1978 (en adelante, CE), recoge parcamente en su articulado dos únicos preceptos referentes a la infancia, a saber: el art. 39 CE y el art. 48 CE[38]. A pesar de ello, en aquel entonces los mencionados artículos supusieron un cambio de paradigma en la normativa nacional en relación a la infancia, ya que mediante ellos la Carta Magna dotaba a los menores de edad de la visibilidad jurídica de la carecían hasta entonces en el ordenamiento jurídico español. En efecto, los textos normativos previos a la CE de 1978, no acogieron en su articulado normativa relativa a la minoría de edad[39]. Así, ante el silencio que guardaban los textos legales, la regulación de la minoría de edad se acometía por el Derecho de familia y la capacidad de obrar de las relaciones jurídico-privadas.

De regreso a las menciones explícitas a la minoría de edad en la Constitución actualmente vigente, el art. 39 CE, comprendido en el Capítulo III del Título I bajo la rúbrica "De los principios rectores de la política social y económica" se divide en cuatro apartados, en los que dispone que: en primer lugar, los poderes públicos asegurarán la

[37] En atención a los nuevos postulados de la Convención de 1989, el Gobierno español comenzó a adaptar la normativa nacional al nuevo paradigma de los menores de edad. Dicho cambio legislativo se inicia con la Ley 11/1981, de 13 de mayo, de modificación de la Filiación, Patria Potestad y Régimen Económico del Matrimonio, que suprimió la distinción entre filiación legítima e ilegítima, equiparó al padre y a la madre a efectos del ejercicio de la patria potestad e introdujo la investigación de la paternidad, Boletín Oficial del Estado, de 19 de mayo de 1981, núm. 119.

[38] Véase, Constitución Española de 1978, Boletín Oficial del Estado, de 29 de diciembre de 1978, núm. 311.

[39] ALÁEZ CORRAL, B., *Temas clave de la Constitución Española. Minoría de edad y Derechos Fundamentales*, Madrid, Tecnos, 2003, p. 34.

protección social, económica y jurídica de la familia. En su segundo apartado, el precepto establece que, los poderes públicos asegurarán la protección integral de los hijos, iguales éstos ante la ley con independencia de su filiación, cualquiera que sea su estado civil. De igual modo, la ley posibilitará la investigación de la paternidad. El tercer apartado propugna el deber de los progenitores de asistir en todo orden a los hijos habidos dentro y fuera del matrimonio, durante su minoría de edad y en los demás casos que legalmente proceda. Por último, el cuarto apartado afirma que los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos.

Del análisis de dicho precepto, podemos concluir que el mandato del legislador de aquel entonces se dirige asimismo a los poderes públicos al fin de proteger la familia social, económica y jurídicamente. Hasta ese momento, la protección del menor, por considerarse este como un miembro integrante de la familia, debía ocurrir principalmente en el ámbito familiar eximiendo de dicha responsabilidad a la Administración Pública. Esta afirmación, cobra especial relevancia, como veremos, en el ámbito de las TIC y redes sociales, pues, durante varios años se ha responsabilizado a los representantes legales de los menores de protegerlo de los diversos riesgos que el empleo de las mismas suponen.

Por otra parte, en idéntico Capítulo, se debe mencionar el art. 48 CE, el cual prevé que los poderes públicos promoverán las condiciones para que la juventud participe de manera libre y eficaz en el desarrollo político, social, económico y cultural. Con el fin de materializar las condiciones expuestas en el art. 48 CE, la Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del Menor (en adelante, LOPJM[40]) se propone garantizar que los menores se consideren sujetos más activos y participativos socialmente. Para ello, genera un clima participativo que garantice la autonomía de estos sujetos, procediendo a acomodar el ejercicio de derechos fundamentales a la particular situación en la que la titularidad de los mismos recaiga sobre un menor de edad.

En este orden de cosas, la Constitución de 1978, eleva al plano jurídico nuevos valores ideológicos y ético-sociales. Precisamente, mediante los mencionados artículos y en concreto el art. 39, se propugna una protección integral de los hijos y obliga a los progenitores a prestarles asistencia en todo momento (apartados 2 y 3 del art. 39 CE)[41]; y no solo eso, reconoce la titularidad de derechos fundamentales por parte de los menores

[40] Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, Boletín Oficial del Estado, de 17 de enero de 1996, núm. 15.
[41] RIVERO HERNÁNDEZ, F., *El interés del menor*, Madrid, Dykinson, 2002, p. 38.

de edad (apartado 4 art. 39) además de considerar a estos como sujetos activos y participativos (art. 48).

No obstante, no podemos pasar por alto que, la CE no contiene en su articulado alusión específica a un catálogo de derechos fundamentales específicos de menores. Simplemente, tal y como se desprende del art. 39.4. esta se remite a los derechos reconocidos por los tratados internacionales de los que España forma parte y se han traído a colación en apartados anteriores. Así, solamente los mencionados arts. (39 y 48 CE) brindarán relevancia constitucional a la minoría de edad. A pesar de ello, la conjunción de los mencionados artículos, con la normativa internacional permiten reiterar la siguiente aseveración: los menores son titulares de los derechos fundamentales inherentes a la personalidad. No obstante, a su vez precisan de protección ya que su personalidad se halla todavía en formación, lo que les convierte en personas especialmente vulnerables[42].

Fruto de la afirmación consistente en saber a los menores titulares de derechos fundamentales inherentes a la personalidad, el legislador español aprueba la LOPJM, por la que se proporcionaba un desarrollo legislativo a los arts. 39 y 48 CE.

4.2. La Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del menor. Primera iniciativa en la protección específica de derechos fundamentales del menor en España

El legislador español, años antes de la promulgación de la Ley de Protección jurídica del menor llevó a cabo determinadas modificaciones legislativas con el fin de adaptar el ordenamiento jurídico al nuevo *status* del menor instaurado internacionalmente[43]. A pesar de dichos esfuerzos, advirtió la patente insuficiencia en la normativa de protección de

[42] Sentado lo anterior, y sin ánimo de proceder a su estudio en profundidad, dado que se reserva para líneas posteriores del presente trabajo, también cabe afirmar que los menores son titulares del derecho a la protección de sus datos personales (art 18.4 CE).

[43] Sirvan como ejemplo las modificaciones introducidas en las leyes que citan a continuación. Ley 13/1983, de 24 de octubre, de Reforma del Código Civil en materia de tutela, Boletín Oficial del Estado, de 26 de octubre de 1983, núm. 256; la Ley 21/1987, de 11 de noviembre, por la que se modifican determinados artículos del Código Civil y de la Ley de Enjuiciamiento Civil en materia de adopción, Boletín Oficial del Estado, de 17 de noviembre de 1997, núm. 275; la Ley Orgánica 5/1988, de 9 de junio, sobre exhibicionismo y provocación sexual en relación con los menores, Boletín Oficial del Estado, de 11 de junio de 1988, núm. 140; la Ley Orgánica 4/1992, de 5 de junio, sobre reforma de la Ley reguladora de la competencia y el procedimiento de los Juzgados de Menores, Boletín Oficial del Estado, de 11 de junio de 1992, núm. 140, entre otras.

menores nacional, lo que contribuyó a la aprobación de una nueva normativa protectora de los menores de edad como desarrollo de los arts. 39 y 48 CE[44].

Ciertamente, la normativa española sobre protección de la infancia se encuentra, como resulta lógico, fuertemente influenciada por la Convención de los Derechos del Niño de 1989, tanto que, parte de la doctrina, entre los que destaca RIVERA ÁLAVA critican dicho aspecto en el sentido que, afirman que la LOPJM no aporta ninguna novedad respecto a dicha Convención en lo que a los derechos del menor se refiere[45]. Es cierto que, la LOPJM puede presentar un carácter reiterativo de principios que ya gozaban de vigencia en nuestro ordenamiento jurídico a través de otros textos normativos. A título ejemplificativo, la norma sitúa la minoría de edad hasta los 18 años de edad, afirmación que, ya se encuentra presente en el art. 12 de la CE, así como el art. 1 de la Convención de 1989. Respecto al ejercicio de los derechos del menor y su protección, dispone el art. 3 de la LOPJM que, los menores gozarán de los derechos que la CE y Tratados Internacionales reconocen, y especialmente los previstos en la Convención de los Derechos el Niño de las Naciones Unidas de 1989[46]. Ahora bien, convenimos que debe estimarse que presenta la virtud de recoger estos principios y derechos en un mismo texto de manera armonizada.

Con el fin de aportar un somero análisis de la Ley de protección jurídica del menor, la Exposición de Motivos del propio texto traslada a la normativa nacional la preocupación por dotar al menor de un sólido marco jurídico de protección en la

[44] La Ley Orgánica 1/1996, de protección jurídica del menor, nace como respuesta a la reflexión que alberga su propia exposición de motivos que establece que, las transformaciones sociales y culturales acaecidas en la sociedad, han provocado un cambio en el status social del niño. En consecuencia, se ha proporcionado un nuevo enfoque a la construcción de los derechos humanos concernientes a la infancia.

[45] En ese sentido, RIVERA ÁLAVA, J., "La Ley Orgánica 1/96, de 15 de enero, de protección jurídica del menor: algunas consideraciones relevantes", *Cuadernos de Trabajo Social*, 1997, núm. 10, p. 77.

[46] La inclusión de los derechos del menor vino de la mano de la enmienda a la totalidad del texto presentada por el Grupo Izquierda Unida-Iniciativa per Catalunya en el debate parlamentario del 28 de septiembre de 1995. En dicha sesión, la Señora Urán González trasladaba a la Cámara que, si bien era de destacar el deseo de poner fin a la dispersión de normativa en torno al menor de la que padecía el ordenamiento jurídico, así como proceder a una regulación más protectora con los menores de edad, proponía como indispensable la inclusión de los derechos del menor en el texto. La Señora Urán, en nombre de su partido, apuntaba que, no incluir los derechos de los más jóvenes en esta ley relevaba a los menores de edad a una desprotección más prolongada en el tiempo al no verse recogidos y regulados estos derechos en la normativa nacional al efecto. En contestación a dicha intervención, la Señora Del Campu Casasus, del Grupo Socialista, apuntó con destacado acierto a nuestro parecer que, los menores no quedaban desprotegidos en caso de que los derechos de los mismos no fueran incluidos en la ley de protección del menor pues, la legislación española ya recogía y protegía dichos derechos en virtud de la Convención de los derechos del Niño ratificada por el Parlamento en el año 1990. Ratificación que, procede a incluir dicho texto como normativa nacional en virtud del art. 93 CE. Véase Diario de Sesiones del Congreso de los Diputados, Pleno y Diputación Permanente, Sesión Plenaria, núm. 170, de 28 de septiembre de 1995.

comunidad internacional. Aunque queremos apuntar que dicha necesidad no se advirtió únicamente en el ámbito internacional. En el ámbito europeo, la mencionada Resolución del Parlamento Europeo por la que se aprobaba la Carta Europea de Derechos del Niño respondía a idéntica inquietud: la construcción de un marco jurídico que de forma específica contemple a los menores como sujetos necesitados de especial protección[47].

Siguiendo con el estudio de la LOPJM, la normativa confiere a los menores de edad un cierto grado de autodeterminación respecto de sus progenitores, tutores o educadores siguiendo la estela que la normativa internacional y europea marcaban. En palabras empleadas por la Exposición de Motivos, la mejor forma de garantizar social y jurídicamente la protección de la infancia reside en promover la autonomía del menor como sujetos. De esta manera, esta autonomía permitirá a los menores construir paulatinamente una percepción de control tanto sobre su situación personal como de su proyección de futuro. Una de las manifestaciones jurídicas de dicha expresión, reside en que el menor se constituye como una persona con determinada capacidad, aunque limitada, debido a su estado de tránsito hacia la madurez, pero en ningún caso habrán de considerarse personas civilmente incapaces.

Es destacable, cómo el ordenamiento jurídico, paulatinamente, no acoge fórmulas en las que se fomenta una la relación autoritaria entre los progenitores y sus hijos para acoger una nueva configuración de dicha relación: los menores son sujetos activos, participativos y creativos y los progenitores o tutores deben velar siempre en interés de los hijos, de acuerdo con su personalidad y con respeto a sus derechos y su integridad física y mental (art 154 Código Civil[48]). Además, deberán prestarles cuanta asistencia precisen en ese desarrollo hacia la plena madurez (art 39 CE).

Este ámbito de autodeterminación del menor se garantiza por tres instrumentos que la LOPJM recoge en su articulado.

El primero, la LOPJM establece un estatuto personal de los menores de edad que reconoce la plena titularidad de derechos por parte de estos (cuestión que ya afirmaba la Convención de los derechos del Niño de 1989 y que poseía carácter de normativa interna

[47] Véase como la Exposición de motivos afirma que acorde al mandato constitucional, se ha llevado a cabo un importante proceso de renovación del ordenamiento jurídico en materia de menores.
[48] El tenor literal del art. 154 del Código Civil 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 [...]».

vía art 93 CE) y una capacidad progresiva para ejercitarlos. Superando la fase en la que la minoría de edad resultaba objeto de ignorancia por el legislador como sujetos dignos de tutela por el ordenamiento jurídico, la LOPJM, al igual que la normativa internacional y europea sienta un nuevo *status* para el menor de edad y dota al mismo de la titularidad de derechos fundamentales y la capacidad en evolución para ejercitarlos a medida que este va adquiriendo madurez suficiente para hacerlo.

Huelga decir que, además del reconocimiento de la titularidad de todos derechos fundamentales del menor como individuo, también recoge en su Capítulo II un catálogo de derechos, sobre el que volveremos más adelante, de los que el menor de edad es titular y alberga unas disposiciones específicas para facilitar su ejercicio por parte de este colectivo con el fin de garantizar la protección que estos se merecen[49]. Así las cosas, la eficacia de este reconocimiento residirá en la correcta combinación de la posibilidad del ejercicio de dichos derechos con la protección que los menores precisan.

El segundo ámbito que garantiza la expresión de dicha autodeterminación, se encuentra en la exigencia legal de tener en cuenta siempre el interés superior del menor sobre cualquier otro interés legítimo (art 2 LOPM) que pueda concurrir. Ahora bien, este concepto jurídico indeterminado sobre el que volveremos en apartados posteriores, se convierte en punto álgido de la normativa protectora del menor, ya que dicho interés afecta a todos los derechos fundamentales de los que el menor es titular. Como cabe esperar, no siempre resultará sencillo averiguar dicho interés en cada caso concreto.

En el tercer ámbito en el que la autodeterminación del menor se manifiesta, reside en el derecho a ser oído, tanto en el entorno familiar como en cualquier procedimiento administrativo o judicial en el que se encuentre directamente implicado, de modo que, a los menores se les reconoce una esfera activa en la que sus opiniones deben tomarse en consideración.

Así las cosas, la LOPJM además de regular diversas previsiones inherentes al derecho privado como el acogimiento, la adopción, la tutela, etc., también regula los derechos constitucionales de los menores. Efectivamente, el Capítulo II de la LOPJM

[49] No obstante, coincidimos con SÁNCHEZ GÓMEZ, A., "El marco normativo tradicional para los derechos de la personalidad del menor. ¿Alguna asignatura pendiente del siglo XXI?"; *op. cit.*, p. 9 cuando afirma que las novedades que la LOPM pretendía incorporar no fueron tantas, es más, quizás no deberían considerarse como novedades propiamente. Ello se debe a que los principios y derechos que la LOPJM regula, ya se encontraban regulados en normativas internacionales vigentes previo a su proclamación nacional. En este sentido, recordemos que la Convención de 1989, se constituye como un texto en vigor en el estado español desde el año 1990. Antes bien, si debe valorarse positivamente su armonización en un mismo texto jurídico.

recoge un catálogo de Derechos Fundamentales de los menores, algunos de ellos ya presentes en la Sección 1ª del Capítulo Segundo del Título I de la CE. El fin de la norma en este aspecto se identifica con proveer de desarrollo legislativo a dichos derechos constitucionales, con el fin de adaptar su ejercicio a la minoría de edad, además de garantizar que este se adapta a la protección que el menor precisa[50].

Previo a detallar los derechos que la LOPJM recoge en el Capítulo II de su articulado, dedicaremos los siguientes apartados a profundizar los principios recién mencionados sobre los que la LOPJM se erige, dada la trascendencia de los mismos con el presente estudio.

4.2.1. El menor como titular de derechos fundamentales y la capacidad progresiva para su ejercicio de manera autónoma

Conforme al Derecho civil, el menor es titular de derechos dada la capacidad jurídica que este posee desde su nacimiento. Ahora bien, hasta épocas recientes, se ha afirmado que el menor no adquirirá plena capacidad hasta que cumple 18 años al tenor del art. 12 de la CE[51]. Alcanzada esta edad, el estado civil de las personas se corresponde con la mayoría de edad, y como consecuencia de ello, se adquiere plena capacidad en todas las esferas jurídicas, tanto personales como patrimoniales.

Siguiendo las afirmaciones de la doctrina tradicional, tal y como recuerda LASARTE, la capacidad jurídica se identifica con la aptitud necesaria para considerar a una persona titular de derechos y obligaciones. Ésta se posee por el simple hecho de nacer, no resultando susceptible de graduaciones o matizaciones. Por el contrario, la capacidad de obrar admitía graduaciones en atención al tipo de acto que se pretendiera realizar por el sujeto de derecho[52]. En definitiva, la capacidad de obrar determinaba si un sujeto podía realizar un determinado acto con eficacia jurídica o no. Así, los menores de edad se conocen como sujetos con capacidad jurídica; sin embargo, la afirmación sobre su capacidad de obrar no gozaba de tal rotundidad, pues, no adquirirán plenamente misma hasta que alcancen la mayoría de edad.

[50] Véase en ese sentido la Exposición de Motivos de la LOPJM, p. 3.
[51] La Constitución Española en su art. 12 establece que «los españoles son mayores de edad a los dieciocho años».
[52] LASARTE ÁLVAREZ, C., *Compendio de derecho de la persona y del patrimonio,* Madrid, Dykinson, 2014.

Antes bien, debemos mencionar sobre este punto, que por medio de la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, ya no cabe emplear términos como la capacidad de obrar, pues, el nuevo paradigma sienta que, todas las personas poseen capacidad jurídica plena, salvo aquellas que precisen de apoyo para el ejercicio de derechos con eficacia jurídica[53]. En el contexto del menor de edad, ello se traduce en que, aquel ejercicio de derechos que no pueda realizar por sí mismo dada su falta de madurez, deberá llevarse a cabo por sus representantes legales[54].

Ahora bien, este lapso de tiempo desde que el menor nace y hasta que cumple 18 años, no se trata desde la perspectiva del Derecho como una privación absoluta de la capacidad del menor para concluir actos con eficacia jurídica hasta que se celebre su 18º aniversario[55]. Tal y como afirma LACRUZ BERDEJO, si bien hasta el siglo xx, el menor recibía tal consideración, actualmente al menor se le reconoce como una persona capaz, salvo para aquellas cuestiones que una norma le prohíba expresamente[56].

Así las cosas, se debe tomar conciencia de que la edad del menor conserva una importancia trascendental en lo referente a la capacidad de la persona, ya que se toma en consideración por el Derecho para atribuir una mayor o menor capacidad, o una capacidad especial para ciertos actos[57]. Proponía RAMOS CHAPARRO la superación de un esquema dualista o antitético de la edad, sustituyéndose por uno gradualista, en el cual, la capacidad aumenta progresivamente a medida que la edad del sujeto aumenta hasta llegar a un momento en el que se determina la plenitud de la misma (la mayoría de edad)

---

[53] En definitiva, se desdibuja el esquema tradicional de la capacidad construido por la doctrina del siglo pasado. En efecto, obsoletas quedan las afirmaciones entre las que destacan las de CASTÁN TOBEÑAS cuando dispone que "Esta aptitud o capacidad jurídica se desplegaría en dos manifestaciones: «aptitud del sujeto para la mera tenencia y goce de los derechos, y aptitud para el ejercicio de los mismos y para concluir actos jurídicos. La primera de ellas se acostumbra designar con la simple denominación de personalidad, capacidad de derecho o capacidad de goce. La segunda, se denomina capacidad de obrar o capacidad de ejercicio". CASTÁN TOBEÑAS, J., *Derecho civil español, común y foral*, Tomo 1, Vol. II, Madrid, Reus, 1987, pp. 161-162.

[54] Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, Boletín Oficial del Estado, de 3 de junio de 2012, núm. 132.

[55] En efecto, tal y como afirma DE CASTRO el menor deberá cumplir una suerte de requisitos para la adquisición de la capacidad plena, pues la adquisición limitada de la capacidad del menor acontece con el nacimiento. DE CASTRO, F., *Derecho civil*, Madrid, Instituto de Estudios Políticos, 1952, pp. 174 y ss.

[56] LACRUZ BERDEJO, J.L., *Elementos de Derecho civil I. Parte general*, Vol. II, Madrid, Dykinson, 2010, pp. 119-121.

[57] CARRASCO PERERA, A., *Derecho Civil (Introducción. Derecho de la persona. Derecho subjetivo. Derecho de propiedad)*, Madrid, Tecnos, 1996, p. 100.

[58]. En efecto, este es el criterio seguido por el Código Civil en varios de sus preceptos, entre los que destacan, el art. 162 o el art. 1263. Así, la clave para la determinación de la capacidad del menor de edad en cada momento, reside así en la capacidad natural y madurez que esté presente a medida que cumple años[59].

Afirmada así, la titularidad de los derechos fundamentales por los menores de edad[60], corresponde ahora esclarecer si dicha capacidad evolutiva o progresiva reconocida en el ámbito del Derecho civil resulta de aplicación, asimismo a la capacidad de los menores respecto al ejercicio de los derechos fundamentales.

Si bien las instituciones de Derecho privado han desarrollado ampliamente la capacidad de obrar progresiva durante la minoría de edad, el Derecho público no ha abordado como debiera dicha cuestión[61]. En efecto, la CE no contiene en su articulado ningún precepto dirigido a regular la capacidad de los menores respecto de los derechos fundamentales de los que son titulares. Esta ausencia de mención trae consigo no pocas incógnitas jurídicas a las que intentaremos proporcionar respuesta en el presente epígrafe.

En este contexto, dos son las principales cuestiones a dilucidar en torno a la capacidad del menor en el ámbito de sus derechos fundamentales:

La primera de ellas consiste en responder a partir de qué momento el menor puede ejercitar de manera autónoma los derechos fundamentales de los que es titular y en caso de no poder proceder de manera autónoma, si es posible representar al menor en materia de derechos de la personalidad. Este planteamiento resulta, sin duda el más problemático ya que el carácter personalísimo de los derechos tildados de fundamentales lleva consigo la imposibilidad de separación entre la titularidad y ejercicio [62](a diferencia que los

[58] Véase RAMOS CHAPARRO, E., "Niños jóvenes en el derecho civil y constitución", *Derecho Privado y Constitución*, 1995, núm. 7 septiembre-diciembre, p. 183.

[59] *Ibid*, p. 185: En ese sentido, RAMOS CHAPARRO afirma que, dentro de la minoría de edad deben diferenciarse diferentes fases. Una primera presidida por la absoluta falta de capacidad del menor a razón de la incapacidad natural de este. Una segunda caracterizada por la pubertad o juventud que atribuye a este una capacidad limitada o "semicapacidad", basada en la capacidad natural del sujeto para entender y querer, y generalizada a todos los sectores del Derecho civil.

[60] En ese sentido, resultan de interés las palabras de BERCOVITZ RODRÍGUEZ-CANO, R., en su obra "Menores", *Revista Doctrinal Aranzadi Civil-Mercantil (digital)*, Vol. I parte Tribuna cuando afirma no entender la razón por la que el legislador siente la necesidad de recordar que los derechos y libertades se extienden también a los menores de edad.

[61] PASCUAL MEDRANO, A., "Los Derechos Fundamentales y la Ley de Protección del Menor", *Revista Jurídica de Navarra*, 1996, núm. 22, p. 251.

[62] Por ese motivo, la doctrina tradicionalmente ha negado durante un largo lapso de tiempo la posibilidad de representación en el ejercicio de derechos fundamentales. Así se han manifestado, PANUNZIO, S., *Capacità. II. Diritto Pubblico*, en Enciclopedia Giuridica. Vol. V, Istituto della Enciclopedia Italiana,

derechos subjetivos civiles que no poseen la consideración de derechos fundamentales). De ahí que, lo habitual en estos casos consiste en que, para conceder la titularidad de determinado derecho fundamental, se valoren los requisitos extrínsecos e intrínsecos que el individuo deberá cumplir para garantizar una titularidad y ejercicio indisoluble de estos. La razón de ser de este enfoque se halla en evitar que un tercero que no es titular del derecho fundamental y que afecta a bienes esenciales de la persona (como podrían considerarse los progenitores de un menor), lo ejercite en nombre de aquel, pero en contra de la voluntad y verdadero interés de este[63].

La segunda cuestión, reside en identificar las limitaciones que el ordenamiento jurídico establece a esa capacidad progresiva de los menores a efectos de proteger a los mismos independientemente de su madurez. Ya que no debemos ignorar que, como sujetos en proceso de maduración, la protección de la minoría de edad puede conllevar determinadas restricciones a su capacidad en relación al ejercicio de derechos.

Por consiguiente, con el fin de proporcionar una respuesta a la primera cuestión, resulta de trascendental importancia el art. 162.1 del Código Civil. Este precepto excluye la representación legal de los progenitores en el ámbito del ejercicio de derechos de la personalidad como derechos fundamentales, siempre que el menor sea suficientemente maduro para ejercitarlos por sí mismo[64]. La afirmación no es baladí, ya que los menores de edad podrán ejercitar por sí mismos los derechos fundamentales de los que se les considera titulares (tanto los recogidos en la CE como los desarrollados en la LOPJM) siempre que demuestren madurez suficiente para ello.

El ejercicio autónomo de los derechos fundamentales por parte del menor de edad gira así en torno a la madurez que el sujeto demuestre en tanto en cuanto no cumpla los dieciocho años de edad. En definitiva, los menores de edad poseen capacidad condicionada a su nivel de madurez en el ámbito del ejercicio autónomo de sus derechos

Roma, 1988, p. 3; o HOHM, K.H., Grundrechtsträgerschaft und Grundrechtsmündigkeit Minderjähriger am Beispiel öffentlicher Heimerziehung, *Neue Juristische Wochenschrift*, 1986, núm. 50, p. 3111.

[63] ALÁEZ CORRAL, B., *Temas clave de la Constitución Española. Minoría de edad y Derechos Fundamentales*, *op. cit.*, p. 109.

[64] El tenor literal del art. 162.1ª del Código Civil establece que*:* «Los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. Se exceptúan: 1. Los actos relativos a los derechos de la personalidad que el hijo, de acuerdo con su madurez, pueda ejercitar por sí mismo».

fundamentales. Sin embargo, no existe consenso sobre los criterios que han de regir la determinación del nivel de madurez del menor en el ámbito expuesto[65].

Ahora bien, la siguiente incógnita reside en determinar qué sucede en los casos en los que el menor de edad no cuenta con la madurez suficiente para ejercitar autónomamente los derechos fundamentales de los que es titular. Así, el art. 162.1 CC excluye la representación legal de los progenitores en el ejercicio de derechos inherentes a la personalidad como los derechos fundamentales (art 10.1 CE) pero el segundo párrafo que reza como sigue: *«No obstante, los responsables parentales intervendrán en estos casos en virtud de sus deberes de cuidado y asistencia»* trata de abordar la solución. En ese sentido, la doctrina mayoritaria, con la que nos mostramos de acuerdo, afirma que los progenitores o representantes legales, cuando han de ejercitar derechos fundamentales que el menor de edad no puede ejercitar por sí mismo (dada su falta de madurez) estos asumirán dicho ejercicio en beneficio del menor como consecuencia del deber de asistencia que poseen para con sus hijos (art 39 CE) y no como representantes legales propiamente[66].

En sintonía con dicha consideración se muestran DIEZ PICAZO y GULLÓN cuando disponen que, se exceptúan de la representación de los padres los actos relativos a derechos de la personalidad que el hijo o la hija pueda realizar por sí mismo de acuerdo con las leyes y sus condiciones de madurez. Continúan exponiendo con acierto que, en los casos en los que los progenitores adopten decisiones que afecten a estos derechos, como por ejemplo, autorizar una intervención quirúrgica que el menor no se encuentre en situación de decidir, procederán en cumplimiento del deber de velar por él, no como

[65] En ese sentido, véase la Instrucción 2/2006, de 15 de marzo, de la Fiscalía General del Estado sobre el Fiscal y la protección del derecho al honor, intimidad y propia imagen de los menores, Boletín Oficial del Estado, ref. FIS-I-2006-00002. p 8, cuando afirma que el Código Civil no contiene un precepto específico que defina con carácter general cuándo debe considerarse maduro a un menor. Ahora bien, tanto el CC, como las leyes especiales, contienen preceptos en relación con materias concretas en los que se dota al menor (en unos casos al mayor de doce años, en otros al mayor de catorce y en otros al mayor de dieciséis) de autonomía para la realización de actos con trascendencia jurídica o se exige su audiencia. Esta ausencia de un criterio uniforme, lleva a la necesidad de integrar este concepto jurídico indeterminado valorando todas las circunstancias concurrentes en cada caso, partiendo de que la capacidad general de los menores no emancipados es variable o flexible, en función de la edad, del desarrollo emocional, intelectivo y volitivo del concreto menor y de la complejidad del acto de que se trate.

[66] En ese sentido se posicionan voces doctrinales como, CADENAS OSUNA, D., "El consentimiento informado y el rechazo a la intervención o tratamiento médico por el menor de edad tras la reforma de 2015: estudio comparado con el *common law*", *ADC,* 2018, Tomo LXXI, fasc. III, pp. 802-803 o el ya traído a colación ALÁEZ CORRAL, B., "El ejercicio autónomo de los derechos fundamentales por el menor de edad", *Revista Europea de Derechos Fundamentales,* 2013, núm. 21/1er semestre, p. 45.

representantes legales[67]. LACRUZ BERDEJO por su parte, además de acoger idéntica tesis, matiza que la representación legal no existe en ningún momento en este tipo de actos concernientes a derechos de la personalidad. Esto es, la excepción a la representación no opera únicamente cuando el menor presenta capacidad suficiente para actuar por sí mismo, pues en esos casos puede actuar por sí mismo válidamente sin necesidad de representación legal. Por el contrario, apunta que no se encuentra tampoco en los casos en los que el menor no posee madurez suficiente para decidir por sí mismo[68]. Ahora bien, entendemos que, los progenitores o representantes legales no actuarán en su nombre, pero sí como asistentes ante la falta de madurez del menor.

Por supuesto, dicho ejercicio en nombre de los menores de edad debe, en todo caso, llevarse a cabo en interés superior del menor. Tal y como destaca ALÁEZ CORRAL, la posibilidad de ejercitar un derecho fundamental a través de representante justifica porque este ha de proteger el interés del representado, emitiendo la voluntad que, el propio representado hubiera emitido en caso de poder ejercitar determinado derecho por sí mismo[69].

En definitiva, a pesar de que el ejercicio se practique por persona distinta al titular del derecho fundamental, no se puede considerar que ocurra a través de una representación legal propiamente, sino simplemente por medio de un ejercicio de un derecho fundamental que los progenitores realizan en nombre de sus hijos, respetando siempre el interés de aquellos. No obstante, cuando el ejercicio de dichos derechos fundamentales consiste en la realización de actos naturales, no ha lugar a un ejercicio de dicho derecho por un tercero como pueden considerarse los progenitores o tutores legales. Por actos naturales, debemos entender todas aquellas acciones que realiza una persona y que implican el ejercicio de derechos fundamentales[70].

La razón resulta obvia, hallamos determinados derechos que por su contenido esencial no permiten sustituir al titular del mismo en su ejercicio. Como ejemplo de ello, los derechos de reunión, huelga o libertad de expresión, que fácticamente solo pueden ejercitarse por el titular del derecho en primera persona y, por tanto, un representante no puede ejercitarlos por el menor. La posibilidad de actuar en representación en la esfera

[67] DIEZ PICAZO, L., y GULLÓN, A., *Sistema de Derecho civil,* Volumen IV, Tomo I, Madrid, Tecnos, 2012.
[68] LACRUZ BERDEJO, J.L., *Elementos de Derecho civil I. Parte general, op. cit.,* p. 130.
[69] ALÁEZ CORRAL, B., *Temas clave de la Constitución Española, op. cit.*, p. 113.
[70] ALÁEZ CORRAL, B., "El ejercicio autónomo de los derechos fundamentales por el menor de edad", *op. cit.*, p. 55.

de los derechos fundamentales del menor, bajo las condiciones recientemente expuestas, se presenta como una posibilidad solamente para aquellos negocios jurídicos que afecten el ejercicio de derechos fundamentales. Por ejemplo, los representantes legales pueden consentir el uso de la imagen de uno de sus hijos para una campaña publicitaria cuando el menor no se encuentre dotado de la madurez suficiente para consentir por sí mismo.

Respecto a la segunda cuestión planteada en líneas precedentes, la madurez que el sujeto pueda mostrar en aras de determinar la posibilidad de un ejercicio autónomo de sus derechos queda desvirtuada al concurrir alguna restricción a su capacidad en determinado ámbito o respecto a un concreto derecho fundamental, siempre en observancia del interés superior del menor.

Sobre este aspecto se manifiesta la LOPJM en su art. 2.1 cuando establece que: «*Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva y, en todo caso, siempre en el interés superior del menor*».

De la lectura de dicho precepto se deduce que, la capacidad del menor (incluso aunque presente signos de madurez) puede verse restringida cuando el interés del menor así lo requiera. Esto es, cuando con el fin de proteger determinado derecho fundamental del que se le considera titular, exista una restricción a su capacidad para velar por su interés superior. Esta restricción puede venir impuesta legalmente, cuando el legislador con vistas de proteger el interés superior restrinja su capacidad en el ejercicio autónomo de determinados derechos o cuando la observancia del interés superior del menor en determinada circunstancia, precise de dicha limitación a su capacidad por aquellos que deben velar por su protección (progenitores o representantes legales).

En ese sentido, destacan las palabras de ALÁEZ CORRAL cuando dispone que los progenitores son los destinatarios en primer lugar de las obligaciones y facultades legales, a través de las que se garantiza el proceso evolutivo del menor y solamente corresponde al Estado una función de supervisión de que, los padres cumplan adecuadamente dicha función constitucionalmente recogida. Esas facultades y obligaciones legales, pueden conllevar en ocasiones una delimitación o, incluso, limitación del ejercicio autónomo por parte de los menores de derechos fundamentales que la CE de 1978 les reconoce como personas[71].

[71] ALÁEZ CORRAL, B., *Temas Clave de la Constitución Española; op. cit*., p 68. En idénticos extremos se manifiesta la Fiscalía General del Estado en su Instrucción 2/2006, de 15 de marzo, cuando señala en su

En definitiva, la capacidad de los menores de edad respecto de los derechos de su titularidad puede verse limitada siempre que el interés superior de este lo requiera. No olvidemos que, al tratarse de una persona que precisa de especial protección, en determinadas situaciones deberá excluirse la posibilidad de ejercitar derechos fundamentales autónomamente en caso de que resulte más beneficioso para el menor[72]. En estos casos, sus representantes legales, en asistencia al menor de edad ejercitarán dicho derecho fundamental, del mismo modo que lo hubiera ejercitado el propio menor. Desde luego, una eficaz protección jurídica del menor debe tomar conciencia de esta realidad a la hora de regular las diversas vicisitudes en el ejercicio de derechos fundamentales de menores de edad; ya que, pueden verse vulnerados estos derechos más fácilmente dado su especial *status*, y ello requiere conciliar y mantener un complejo equilibrio entre la autodeterminación del menor y la necesidad de su protección en observancia de su interés superior.

Por todo lo expuesto, y para interpretar correctamente la posible limitación de la capacidad del menor respecto a los derechos fundamentales de los que es titular, y con el

---

Exposición de motivos que: «los arts. 12 y 39.2 y 3 de la Constitución Española contemplan la minoría de edad como una fase de la vida que se caracteriza por la insuficiencia en mayor o menor grado de medios para proporcionarse la persona a sí misma una protección íntegra en el disfrute de sus derechos, precisando por tanto el establecimiento de mecanismos de heteroprotección, en un primer nivel suministrados por los titulares de la patria potestad (art 154 CC) o por sus sustitutos (tutores, guardadores) y en un segundo nivel, en defecto o por insuficiencia del anterior, por las instituciones públicas (en especial, Entidades Públicas de Protección de Menores y Ministerio Fiscal)». Continúa la Instrucción disponiendo que la condición del menor como persona en situación de especial vulnerabilidad se refleja en la regulación de numerosas instituciones en las que el ordenamiento trata de reforzar su protección. Esta idea-fuerza aparece con claridad cuando el Código Penal protege la intimidad, la libertad sexual o cuando la legislación civil protege la intimidad y la propia imagen de menores; en estos casos se les tutela frente a los ataques actuales y simultáneamente se les protege para hacer factible el desarrollo de su personalidad, y, en definitiva, para que puedan ejercer con plenitud sus derechos en el futuro. La necesidad de velar por el desarrollo integral del menor como sujeto en tránsito hacia la plena madurez, hace que el ordenamiento le otorgue una protección de especial intensidad.

[72] A modo de ejemplo, debemos necionar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica, Boletín Oficial del Estado, de 15 de noviembre de 2002, núm. 274. En el sector biosanitario se restringe al menor la aptitud para ejercitar autónomamente su derecho fundamental a la vida e integridad física, al tratarse de un bien jurídico especialmente sensible; la normativa opta por limitar el ejercicio de derechos por el menor con el fin de velar por su interés superior y protegerlo. Así, la normativa reguladora de la materia establece la edad de 16 años para que el menor de edad pueda prestar consentimiento informado por sí mismo a someterse a tratamientos médicos. No obstante, los menores de 16 años con madurez suficiente para entender el alcance de la intervención podrán prestar consentimiento autónomo igualmente. Ahora bien, en casos de gravedad, los menores de edad, aunque tengan más de 16 años y suficiente madurez, no podrán prestar consentimiento válido a las intervenciones médicas. En épocas más recientes, el Anteproyecto de Ley para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI, publicado en Boletín de las Cortes Generales, de 16 de septiembre de 2022, Serie A, núm. 113-1, prevé en su art. 38 la posibilidad de que menores de 16 años soliciten autónomamente ante el Registro civil la rectificación de la mención registral relativa al sexo. En definitiva, solamente cuando no se prevea que el menor pueda ejercitar autónomamente sus derechos fundamentales, los representantes legales de este procederán a su ejercicio a modo de asistentes.

fin de proteger su interés superior, deviene indispensable concretar qué ha de entenderse por interés superior del menor de edad.

4.2.2. El interés superior del menor como principio fundamental de su protección en la legislación y jurisprudencia españolas

A lo largo del presente trabajo se ha podido constatar un crecimiento en el interés sobre el refuerzo de la protección del menor en el ordenamiento jurídico, tanto a nivel nacional como internacionalmente. Fruto de los esfuerzos del legislador y organizaciones internacionales aunados a finales del pasado siglo y comienzos del presente, se ha experimentado el paso de los menores de edad de un estado de invisibilidad jurídica, a una protección de su persona por el ordenamiento jurídico como titulares de sus propios derechos.

En este contexto relativo a la protección del menor, se desenvuelve el concepto de interés superior del menor. No obstante, proporcionar una definición del mismo se presenta como una tarea ardua y complicada ya que la evolución experimentada en el *status* del menor de edad ha influido decisivamente en la interpretación del concepto jurídico indeterminado del mejor interés del menor.

Como no podía tratarse de otro modo, la evolución experimentada por la sociedad, ha ocasionado que el concepto legal de interés superior del menor también haya sufrido análoga evolución acorde a dichos cambios sociales. Entre estos, influye decisivamente la quiebra del modelo jerárquico de la familia; ruptura que favoreció que la posición del menor tanto en la familia como en la sociedad variara por completo, potenciando la participación del menor en su propia maduración, formación y decisiones vitales concernientes a su persona[73].

Entendemos que, esta nueva configuración de principios y valores superan el modelo tradicional patriarcal protagonizado por un total servicio de los miembros de la familia al grupo. Conformes con LAMA AYMÁ, en la actualidad la familia no es un fin en sí misma sino un instrumento para la salvaguarda del verdadero objeto de protección: los miembros de la familia individualmente considerados en la medida en que son personas[74].

[73] RIVERO HERNANDEZ, F., *El interés del menor*, *op. cit.*, p. 39.
[74] Véase a tal efecto LAMA, AYMÁ, A., *La protección de los derechos de la personalidad del menor de edad.* Valencia, Tirant lo Blanch, 2006.

Así las cosas, la familia deja de considerarse como una institución jerárquica y autoritaria al servicio del paterfamilias para convertirse en una asociación en la que cada uno de sus miembros posee importancia individual y en la que se fomenta el libre ejercicio de sus derechos fundamentales. De todos modos, el Derecho no permanece ajeno a la circunstancia por la que el menor de edad se posiciona como la persona más vulnerable del vínculo familiar y es por lo que concede una especial protección a sus derechos fundamentales respecto a los demás individuos que conforman la familia. Principalmente, esta nueva configuración encuentra su razón de ser en la proyección general de los derechos de la personalidad experimentada en el mundo occidental[75].

Desde luego, tal y como se expone a continuación, esta evolución ideológica y social se proyecta también en la normativa tanto internacional como nacional.

En el ámbito nacional, la CE de 1978 acoge en su articulado el reconocimiento de los derechos inherentes de la personalidad. No obstante, el ascenso de principios, termina calando no solo en normativas constitucionales, sino también en preceptos propiamente civiles regulados en el CC. La Carta Magna, por su parte, posee varios preceptos impulsores del cambio. En ese sentido, alcanza una posición central en este cambio el art. 10.1 CE que propugna la dignidad de la persona, los derechos inviolables que le son inherentes, así como el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás. Este nuevo orden influye de manera determinante en nuestro sistema jurídico y, por ende, en las normas reguladoras de la situación jurídica de los menores de edad, que deberán resultar objeto de interpretación bajo el prisma de dicho precepto informador.

Por otra parte, el ya analizado art. 39 CE, se reconoce como otro de los preceptos en los que cristalizó el cambio de paradigma social. El mismo establece que los poderes públicos aseguran la protección social, económica y jurídica de la familia (apartado 1), abogando así por una protección integral de los hijos menores de edad (apartados 2 y 3) al tiempo que apuesta por el reconocimiento de la titularidad de los derechos fundamentales del menor recogidos en tratados internacionales en los que España es parte (apartado 4). Tras este cambio de paradigma, los progenitores y los poderes públicos, se encuentran obligados a la protección de la familia y de los menores, sobrepasando los

[75] Así, RIVERO HERNANDEZ, F., *El interés del menor, op. cit.*, p. 39.

límites del ámbito familiar privado para establecer un marco jurídico de protección que vincula no solo a los progenitores sino a todos los Poderes Públicos[76].

El Derecho civil, por su parte, también experimenta sendas reformas fruto de este cambio social en el orden familiar. Así, la adopción, el acogimiento, la tutela, la guarda y custodia tras la crisis matrimonial…son algunas de las instituciones de Derecho civil que han debido acomodarse a dicho cambio social establecido en la CE. Sin embargo, en relación al presente estudio y como destinatario del cambio social propugnado constitucionalmente, destacamos el art. 154 CC, que aboga por el ejercicio de la patria potestad en beneficio de los hijos y respetando tanto su personalidad, como sus derechos e integridad física y mental[77].

En el ámbito internacional, adquiere especial relevancia el art. 3.1 de la Convención sobre los Derechos del Niño de 1989 ya que el mismo dispone que, en todos los actos concernientes a niños y niñas, el mejor interés del menor deberá anteponerse. Además, tanto el TEDH como el Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE), han tenido ocasión de pronunciarse a favor del interés del menor desde hace más de una década[78]. Actualmente, el TJUE ha sostenido la primacía del interés superior del menor incluso en procedimientos de retorno de menores no acompañados, afirmando que no se podrá ordenar el retorno del menor para los casos en los que no se pueda garantizar una acogida adecuada para este en el país de retorno[79]. Particularmente

[76] NÚÑEZ RIVERO, C., "La protección del menor desde un enfoque del derecho constitucional", *Revista de Derecho UNED*, 2011, núm. 9, p. 274.

[77] Así, el principio general de interés del menor se ha plasmado en la legislación nacional de forma muy notoria. Destacan los arts. 154 CC que dispone que «la patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad…»; y el art. 92.2 de este mismo cuerpo normativo, previsor del interés del menor en los casos de crisis matrimoniales entre progenitores. También cabe señalar el art. 176 CC que establece el interés del adoptado o del art. 172.4 CC que aboga por el interés del menor en los casos de acogimiento.

[78] El Tribunal de Justicia de la UE se ha pronunciado sobre la primacía del interés del menor sobre cualquier otro interés en cuestiones matrimoniales y responsabilidad entre parientes en sentencias como la sentencia del Tribunal de Justicia de la Unión Europea, de 1 de julio de 2010, sobre traslado ilícito de menores, rec C-211/201. El Tribunal Europeo de Derechos Humanos, por su parte, se ha pronunciado sobre el interés superior del menor en sentencias como la sentencia del Tribunal Europeo de Derechos Humanos, de 22 de junio de 2004, sobre secuestro internacional de menores por sus propios progenitores, rec. 78028/2001 y la sentencia del Tribunal Europeo de Derechos Humanos, de 24 de febrero de 2009, sobre el respecto a la vida familiar con la prohibición de discriminación, rec. 29768/2005.

[79] Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de enero de 2022, *TQ/Staatssecretaris van Justitie en Veiligheid*, Asunto C-441/19.

influenciada por el Convenio de Derechos del Niño, la LOPJM propugna idéntico interés en su art. 2.1[80].

Sin ánimo de resultar rigurosos, pues no es objeto de este trabajo, debido al gran protagonismo de este principio en nuestro ordenamiento jurídico, conviene proporcionar ahora una aproximación al concepto de interés superior del menor, ya que dicho precepto condiciona el ejercicio de derechos fundamentales por parte de los menores de edad. Efectivamente, se ha señalado en apartados previos, que el ejercicio de derechos fundamentales por los menores de edad puede verse limitado en observancia de su interés superior, pero ¿cómo debe interpretarse y configurarse jurídicamente dicho interés?

Partiendo de los antecedentes expuestos y siguiendo las afirmaciones de RIVERO HERNÁDEZ coincidimos en que proporcionar una definición del interés superior del menor se antoja una tarea sumamente complicada[81]. En este devenir, su consideración como concepto jurídico indeterminado dificulta considerablemente dicha labor. Antes bien, esta imprecisión en su definición no ha de interpretarse exclusivamente desde un sentido negativo, la ambigüedad del concepto aporta un grado de flexibilidad para adecuar lo que el interés superior del menor ha de entenderse en cada caso concreto[82].

A lo expuesto cabe añadir que el interés superior del menor como principio adopta diferentes dimensiones y funciones en el ordenamiento jurídico, a saber: una primera

[80] Véase art. 2.1 LOPJM que sienta que: «Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado. En la aplicación de la presente ley y demás normas que le afecten, así como en las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos primará el interés superior de los mismos sobre cualquier otro interés legítimo que pudiera concurrir».

[81] En ese sentido, RIVERO HERNÁDEZ, F., *El interés del menor*, *op. cit.*, p 61.

[82] *Ibid*, p. 175 afirma RIVERO HERNÁNDEZ que el interés del menor deberá concretarse a lo que más conviene a un menor determinado. Por otra parte VELA SÁNCHEZ señala que se debe valorar positivamente que este principio permita adaptar el problema en cuestión al supuesto específico que se pretende resolver, de manera que no se imponen al encargado de aplicar la norma jurídica unos parámetros determinados, sino que dicho operador posee un ámbito de actuación flexible que le permite valorar, de acuerdo a las circunstancias concurrentes, la concreción del interés superior del menor en función de las características intrínsecas de cada persona interesada o de los hechos acaecidos VELA SÁNCHEZ, A., "El interés superior del menor como fundamento de la inscripción de la filiación derivada del convenio de gestación por encargo". *Diario La Ley (digital)*, 2013, núm. 8162. De manera más reciente, ha continuado destacando la relevancia cardinal de este principio cuando se trata de dilucidar sobre la inscripción de menores de edad nacidos en el extranjero por medio de la técnica de la gestación subrogada. En efecto, para el autor, los conflictos que suscita la materia llegarían a su fin de aplicarse el interés superior del menor como cláusula general que permita neutralizar la aplicación del precepto que prohíbe dicha técnica en España. Siempre que ello se lleve a término en orden a respetar al interés superior del menor que ya ha nacido a través de la técnica señalada. VELA SÁNCHEZ, A., "La gestación por sustitución en las Salas de lo Social del Tribunal Supremo y de los Tribunales Superiores de Justicia. A propósito de la prestación por maternidad en los casos de nacimientos derivados de convenio gestacional", *Diario la Ley*, 2017, núm. 8927, p. 12.

vendría presidida por la consideración del interés superior del menor como concepto jurídico indeterminado en el que debe existir de manera previa una ponderación de las circunstancias concretas del caso, al fin de aplicar correctamente a cada caso el interés superior del menor. Una segunda se identifica con la idea de que el interés superior del menor se constituye como una cláusula general, que deberá aplicarse de manera prevalente ante un conflicto en el que se vea envuelto un menor. Una tercera y última considera el interés superior del menor como un derecho subjetivo, digno de protección y defensa[83].

En la primera de las vertientes expuestas, esto es, la consideración del interés del menor como concepto jurídico indeterminado, el TS aporta una valiosísima consideración al respecto en la sentencia 1229/2014 de 12 de febrero de 2014[84], en la que estimó que, si bien es cierto que los hechos deben resultar objeto de valoración atendidas las circunstancias del caso junto con otras que pudieran concurrir, la decisión que afecte al menor debe venir justificada por el interés más necesitado de protección, que ha de someterse a juicio de ponderación y valorarse sobre la base de las circunstancias señaladas. Dicha afirmación también se sostiene por CLAVIJO SUNTURA cuando dispone que la indeterminación del interés del menor posee un doble aspecto, por una parte, determinar en qué consiste el interés del menor, para posteriormente precisar lo que más le conviene al menor de acuerdo con una situación concreta[85].

---

[83] Véase en ese sentido la interesantísima reflexión de DOMÍNGUEZ REYES, F.F., "Interés superior del menor en la jurisprudencia del Tribunal Supremo", *Revista Crítica de Derecho Inmobiliario*, 2018, núm. 768, pp. 2213-2214. Dichas dimensiones a las que se refiere la autora se han recogido en la Exposición de Motivos de la Ley 8/2015, de 22 de julio, de modificación del sistema de protección del sistema a la infancia y a la adolescencia, Boletín Oficial del Estado, núm. 175, p. 61871. Textualmente, dicho inciso establece que: «Este concepto se define desde un contenido triple. Por una parte, es un derecho sustantivo en el sentido de que el menor tiene derecho a que, cuando se adopte una medida que le concierna, sus mejores intereses hayan sido evaluados y, en el caso de que haya otros intereses en presencia, se hayan ponderado a la hora de llegar a una solución. Por otra, es un principio general de carácter interpretativo, de manera que si una disposición jurídica puede resultar interpretada en más de una forma se debe optar por la interpretación que mejor responda a los intereses del menor. Pero, además, en último lugar, este principio es una norma de procedimiento. En estas tres dimensiones, el interés superior del menor tiene una misma finalidad: asegurar el respeto completo y efectivo de todos los derechos del menor, así como su desarrollo integral».

[84] Así, el FD 2º de la Sentencia del Tribunal Supremo 1229/2014, Sala 1ª de lo Civil, de 12 de febrero de 2014 (rec. 383/2012), FD 2º dispone que el mantenimiento de uso de la vivienda por uno de los cónyuges debe venir justificado por el interés más necesitado de protección, concepto jurídico indeterminado que deberá constituir objeto de juicio de ponderación en el que, sobre las circunstancias señaladas, se contrasten directamente las circunstancias e interés dignos de protección o consideración que presente la situación de cada cónyuge.

[85] CLAVIJO SUNTURA, H., "El interés del menor como concepto jurídico indeterminado y las técnicas de su determinación en situaciones de crisis familiares", *Pórtico Legal*. Obtenido de: *https://www.porticolegal.com/pa_articulo.php?ref=306* (Consultado el 10 de julio de 2020).

Por otra parte, el TS también ha incidido especialmente en la consideración de cláusula general del interés superior del menor, en el sentido que, este principio se materializa una preponderación del interés de los hijos, que deberá anteponerse frente al resto de intereses. De este modo, esta técnica permite concretar las actuaciones y decisiones que resulten más beneficiosas al menor en cada situación concreta. Sobre este aspecto, es de destacar la Sentencia del TS 83/2014, de 6 de febrero de 2014[86], en la que se reconoce que el interés superior del menor se configura como una cláusula general que el legislador introduce para ampliar los márgenes de la ponderación judicial en cada caso concreto. Siguiendo a MIQUEL GONZÁLEZ afirma que, la función principal de las cláusulas generales reside en completar el Derecho, además de desarrollarlo y adoptarlo[87]. Por lo que, efectivamente el juez deberá ponderar minuciosamente las circunstancias concretas de cada caso, con el fin de adoptar la decisión que más acorde al interés del menor resulte.

Por último, respecto a la consideración del interés del menor como derecho fundamental subjetivo podríamos decir que consiste en definir este concepto como aquella conducta tendente a procurar la protección de los derechos fundamentales de los niños, de forma prioritaria y preferente a los demás derechos implicados. En ese sentido se manifiesta la Sentencia del TS 4281/2016, de 28 de septiembre de 2016 cuando el Alto Tribunal sienta que la protección de los derechos fundamentales de los niños debe realizarse de manera prioritaria al resto de derechos implicados[88].

Sin embargo, en épocas más recientes, el TS ha continuado perfilando este criterio en relación al reconocimiento de la filiación de menores nacidos por medio de la técnica

[86] Véase la Sentencia del Tribunal Supremo 835/2013, Sala 1ª de lo Civil, de 6 de febrero de 2014, (rec. 245/2012). La Sentencia se dicta con motivo de la solicitud de inscripción en el Registro Civil de dos menores nacidos en California por medio de la técnica de gestación subrogada prohibida en España. Tras varios recursos, la cuestión llega al TS, que afirma que en ocasiones las cláusulas expresan un criterio normativo sobre el que no existe unanimidad social. Esa circunstancia en ocasiones puede llevar a que el interés superior del menor se corresponda con aquel sobre el que no existe consenso social como es la inscripción de menores en el Registro Civil nacidos por medio de una Técnica de Reproducción Humana Asistida no permitida en España, y sobre la que la normativa no permite inscripción de dichos menores en el Registro Civil. El Fundamento Jurídico 5º de la Sentencia dispone que: «la cláusula general de la consideración primordial del interés superior del menor, contenida en la legislación no permite al juez alcanzar un resultado cualquiera en la aplicación de la misma. La concreción de dicho interés del menor no debe hacerse conforme a sus personales puntos de vista, sino tomando en consideración los valores asumidos por la sociedad como propios, contenidos tanto en las reglas legales como en los principios que inspiran la legislación nacional y convenios internacionales».

[87] MIQUEL GONZÁLEZ, J.M., "Cláusulas generales y desarrollo judicial del Derecho", *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 1997, núm.1, p. 305.

[88] Sentencia del Tribunal Supremo 4281/2016, Sala 1ª de lo Civil, de 28 de septiembre de 2016, (rec. 3682/2015), Fundamento jurídico 2º.

de gestación subrogada. Concretamente, en la Sentencia 277/2022, de 31 de marzo de 2022 afirma que, para la toma de la concreta decisión se ha valorado *in concreto* la satisfacción del interés superior del menor[89]; no obstante, también sostiene que a su vez ha procurado salvaguardar los derechos fundamentales de las madres gestantes y niños en general susceptibles de vulneración en caso de fomentar comercialmente el empleo de estos medios de reproducción.

Así las cosas, todas las perspectivas abordadas convergen en un punto común: el interés superior del menor deberá valorarse en cada caso concreto atendiendo a las circunstancias que se presentan.

En relación a lo expuesto, la definición del concepto de interés del menor que mejor se acomoda al objeto la presente investigación, por encontrarse estrechamente relacionada con la titularidad de derechos fundamentales, consiste en proteger y garantizar los derechos fundamentales del menor de edad como persona y fomentar el libre desarrollo de su personalidad[90]. Ahora bien, la norma no alumbra el modo en el que se debe alcanzar dicha protección en cada caso y precisamente en esa indeterminación, se encuentra la clave para la aplicación del principio ya que, el hecho de que la ley no proporcione la respuesta directamente, nos conduce a su búsqueda en cada caso acudiendo a juicios de experiencia o de valor. De manera específica, quien desee concretar el interés del menor (juez, organismo, institución, progenitores…) habrá, en aplicación de la ley, dotar de contenido el concepto jurídico indeterminado, pues es quien poseerá los datos y circunstancias para valorar el supuesto de hecho concreto y así determinar cuál es dicho interés concurrente.

A efectos de concretar ese interés específico del menor de edad, resultan de gran utilidad los criterios contenidos en la Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema de protección de la infancia y la adolescencia[91], que fueron incorporados a la LOPJM con el objetivo de incluir la jurisprudencia del TS, mencionada

[89] Véase así la Sentencia del Tribunal Supremo 277/2022, de 31 de marzo de 2022, (rec. 1153/2022). En este pronunciamiento, el TS no acepta reconocer automáticamente la filiación de un menor nacido por medio de la técnica de gestación subrogada en el extranjero, sosteniendo que la madre comitente deberá adoptar al menor en cuestión y que el padre podrá determinarla mediante la práctica de la correspondiente prueba de paternidad.

[90] Véase LAMA AYMÁ, A., *La protección de los derechos de la personalidad del menor de edad, op. cit*., p. 97.

[91] Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema a la infancia y a la adolescencia, Boletín Oficial del Estado, de 23 de julio de 2015, núm. 175.

hace escasas líneas en relación a la materia[92]. Ciertamente, como afirma DOMINGUEZ REYES, hasta la reforma efectuada en el año 2015, el Código Civil no ofrecía una lista de criterios que permitiera al juzgador de instancia ponderar el interés del menor[93].

Esa circunstancia ha acarreado la dispersión de decisiones adoptadas por Jueces y Tribunales y que las Audiencias Provinciales, TS y TC han tratado de paliar dictando sentencias con criterios de concreción[94]. Sin embargo, dichos criterios atienden a dos ámbitos muy concretos: por una parte, criterios relacionados con el derecho de familia, y, por otra parte, relacionados con los derechos fundamentales del menor. Respecto al primero de los ámbitos, los criterios a destacar que las resoluciones establecen, giran principalmente en torno a la atribución de la guarda y custodia, así como la determinación de la filiación e inscripción de menores nacidos a través de la técnica de gestación subrogada. El segundo de los ámbitos, relacionado con los derechos fundamentales del menor, ha sentado jurisprudencia, principalmente en relación a la protección del derecho a la propia imagen de los menores de edad, cuando este entra en colisión con el derecho de información, disponiendo a tal efecto una serie de criterios que deberán emplearse en el momento de ponderar los intereses en conflicto[95].

Mediante el art. 2.2 de la LOPJM se positivizan, por primera vez cuatro criterios que pretenden servir de ayuda en la búsqueda del interés del menor y que deberán resultar objeto de aplicación tomando en consideración los elementos generales del apartado tercero del mismo precepto. Podemos resumir estos en los siguientes: la protección del derecho a la vida, supervivencia y desarrollo del menor, así como la satisfacción de sus necesidades básicas, tanto materiales, físicas y educativas como emocionales y afectivas; la consideración de los deseos, sentimientos y opiniones del menor, así como su derecho a participar de manera progresiva en función de su edad, madurez, desarrollo y evolución personal, en el proceso de determinación de su interés superior; la conveniencia de que su vida y desarrollo ocurra en un entorno familiar adecuado y libre de violencia; por

[92] Los mencionados criterios se incluyeron con el fin de incorporar la jurisprudencia del Tribunal Supremo en relación a la materia, así como los criterios de la Observación general número 14 del Comité de las Naciones Unidas de Derechos del Niño, de 29 de mayo de 2013.
[93] DOMÍNGUEZ REYES, F.F., "Interés superior del menor en la jurisprudencia del Tribunal Supremo", *op. cit.*, p. 2221.
[94] BELLOSO MARTÍN, N., "La concreción del interés (superior) del menor", *Anuario Facultad de Derecho-Universidad de Alcalá X*, 2017, núm. 10, pp. 23-28.
[95] Véanse en ese sentido las siguientes sentencias del TC: Sentencia del Tribunal Constitucional 54/2004, de 15 de abril, Boletín Oficial del Estado, de 18 de mayo de 2004, núm. 120, pp. 31 a 40 y la Sentencia del Tribunal Constitucional 61/2004, de 19 de abril, Boletín Oficial del Estado, de 18 de mayo de 2004, núm. 120, pp. 92 a 97.

último, la preservación de la identidad, cultura, religión, convicciones, orientación e identidad sexual o idioma del menor, así como la no discriminación del mismo por estas o cualesquiera otras condiciones, incluida la discapacidad, garantizando el desarrollo armónico de su personalidad.

No obstante, los criterios expuestos se aplicarán bajo la observancia de una suerte de elementos entre los que destacan la edad y madurez que presenta el menor; la necesidad de garantizar su igualdad y no discriminación por su especial vulnerabilidad; el irreversible efecto del transcurso del tiempo en su desarrollo; la necesidad de estabilidad de las soluciones adoptadas al fin de promover la efectiva integración y desarrollo del menor en la sociedad, así como minimizar los riesgos de cualquier cambio de situación material o emocional que pueda ocasionar en su personalidad y desarrollo futuro; la preparación del tránsito a la edad adulta e independiente, de acuerdo con sus capacidades y circunstancias personales; y aquellos otros elementos de ponderación que, en el supuesto concreto, se consideren pertinentes y respeten los derechos de los menores. Así mismo, los elementos señalados deberán valorarse conjuntamente conforme a los principios de necesidad y proporcionalidad de tal modo que la medida adoptada en interés superior del menor no restrinja en mayor medida los derechos de este.

Como puede apreciarse, la determinación del interés del menor en cada supuesto variará en función de las circunstancias de cada menor de edad. Antes bien, la razón de ser de los criterios radica en procurar evitar decisiones marcadamente subjetivas por quien ha de delimitar interés superior del menor en cada caso concreto.

En este contexto, creemos conveniente analizar la articulación del interés del menor con el ejercicio de derechos fundamentales por parte del menor de edad que hemos apuntado en el apartado anterior. Desde luego, el ejercicio de los derechos fundamentales por parte del menor de edad debe inspirarse por el interés superior de este, de modo que, si el interés del menor lo requiere, la observancia del mismo se traduce en la limitación de dicho ejercicio autónomo. Dicha limitación puede acometerse legislativamente, cuestión sobre la que volveremos más adelante o, puede ocurrir que, el interés superior del menor radique en la intromisión de un derecho fundamental del que éste es titular. En estos casos, alcanza especial relevancia la correcta aplicación de este principio, puesto que, si bien es cierto que determinados derechos fundamentales no se configuran de modo absoluto, una intromisión en los mismos debe venir precedida por una causa que lo

justifique (como puede tratarse el interés superior del menor). Devendrá totalmente legítimo que una correcta ponderación del interés en atención a los criterios expuestos conlleve la vulneración de dichos derechos si las circunstancias lo requieren, así se ha manifestado incluso el TS[96].

Además, el art. 154 CC traído a colación en varias ocasiones, puede legitimar a los progenitores a llevar a cabo dicha intromisión siempre que la misma se efectúe en beneficio de los hijos. Los menores de edad como personas que se encuentran en un estado de evolución constante, pueden resultar especialmente vulnerables, lo que puede propiciar una intromisión en sus derechos con el objetivo de proporcionarles una protección eficaz. En este devenir, el interés del menor puede consistir en brindar protección al menor, garantizar sus derechos fundamentales como persona y fomentar el libre desarrollo de su personalidad, siempre valorando caso por caso cuáles resultarán las medidas más idóneas para cada circunstancia concreta, incluyendo la posibilidad de limitar o restringir el ejercicio de derechos fundamentales por parte del menor cuando resulte indispensable para su protección.

En definitiva, es importante destacar que la normativa que regula el desarrollo de los derechos fundamentales de los menores de edad, acomodando el ejercicio a las particularidades de la minoría de edad se hace eco en todo momento de esta dicotomía: proporcionar al menor, autonomía para ejercitar sus propios derechos, pero a su vez, garantizar la posibilidad de que, la íntegra protección de los derechos fundamentales del menor puede conllevar la restricción en la capacidad de los menores de edad.

4.2.3. El desarrollo normativo de los derechos fundamentales adaptado a la minoría de edad en la LOPJM. Especial atención a la protección del derecho a la intimidad

Tal y como se ha indicado, el Capítulo II de la LOPM recoge una serie de derechos fundamentales de los que los menores son titulares. No obstante, no significa que los menores de edad solamente se consideren titulares de los derechos recogidos en dicho Capítulo, sino que también se consideran titulares de los derechos fundamentales que la CE les confiere como sujetos dotados de personalidad. En este sentido, el legislador ha

[96] En ese sentido se manifiesta la Sentencia del Tribunal Supremo 864/2015, Sala 1ª de lo Civil, de 10 de diciembre de 2015, (rec. 6401/2015) en un supuesto en el que una menor de edad estaba siendo víctima de un delito y la madre corroboró la comisión de dicha actuación delictiva sobre su hija accediendo a los mensajes de la menor en el teléfono móvil sin permiso de aquella. El TS afirmó que el derecho a la intimidad no posee carácter absoluto y que podía verse sometido a restricciones en los casos en los que se acredita un interés constitucionalmente prevalente al interés de la persona a mantener en privado determinada información (como puede tratarse en este caso, el interés superior del menor).

creído conveniente a través de la LOPJM, prestar desarrollo a una serie de derechos fundamentales recogidos en la Sección 1ª del Capítulo Segundo del Título I de la CE en orden a adaptar su ejercicio a la minoría de edad.

La finalidad del presente desarrollo normativo, reside en proporcionar una protección más intensa al ejercicio de determinados derechos fundamentales cuando el titular es menor dada su especial vulnerabilidad. Así, los derechos fundamentales del menor de edad se consideran doblemente protegidos: por una parte, estos derechos recogidos en la CE, cuentan con sendas normativas de desarrollo vía Ley Orgánica en aras de otorgarles protección; por otra parte, en el caso de que el titular de dichos derechos no alcance la mayoría de edad, también deberá observarse la regulación que la LOPJM establece para dicho derecho, ya que esta se propone brindar una mayor protección a dichos derechos dada la particularidad de los titulares del mismo.

Concretamente, la LOPJM dota de desarrollo los siguientes derechos fundamentales que mencionaremos brevemente.

En primer lugar, el derecho del menor a ser oído en procedimientos administrativos y judiciales (art 9 LOPJM) en desarrollo del art. 24 CE continente del derecho a la tutela judicial efectiva. Esta adaptación halla su razón de ser en la consideración del menor como sujeto activo y participativo además de capaz de ejercitar autónomamente sus propios derechos. Así las cosas, se deberá escuchar al menor en cualquier procedimiento que le afecte siempre que tenga madurez suficiente[97].

En segundo lugar, ha LOPJM ha desarrollado el derecho a la libertad de expresión e información (art 20.4 CE) de los menores en los arts. 5 a 8. Los menores de edad tendrán derecho a expresarse libremente y a recabar información, ahora bien, el matiz aportado por la LOPJM se halla en que estos derechos se encuentran circunscritos al ámbito familiar. Antes bien, en el ámbito de las TIC, dichos derechos han alcanzado un protagonismo sin precedentes. En efecto, Internet y las redes sociales se han posicionado como el mecanismo de comunicación principal por el que las personas se expresan libremente y recaban información, entre otros. En concreto, los más jóvenes tienden a expresar sus ideas, sentimientos y opiniones tanto en la red como, especialmente en las

[97] En efecto, así lo dispone el art. 770.1.4ª., de la Ley 1/2000, de 7 de enero de 2000, de Enjuiciamiento Civil, Boletín Oficial del Estado, de 8 de enero de 2020, núm. 7.

redes sociales. Sin embargo, el ejercicio del derecho a la libertad de expresión *online* puede vulnerar otros derechos, igualmente fundamentales como el honor, la intimidad personal o familiar y la propia imagen, con alcance ilimitado en la red. Esta circunstancia, a pesar de no ser objeto de análisis de la presente investigación, consideramos debe estudiarse con especial cautela en el caso de menores de edad.

En tercer lugar, el art. 6 de la LOPJM reconoce al menor el derecho a la libertad ideológica, conciencia y religión (art. 16 CE). En este sentido, los progenitores o representantes legales poseen el deber de cooperar en la formación y desarrollo de la conciencia ideológica y religiosa del menor (art 27.3 CE y 6.3 LOPM). Como puede apreciarse, la aportación de la LOPJM en dicho desarrollo es prácticamente inexistente, en cuanto que solamente reproduce preceptos constitucionales ya recogidos en la CE. Ahora bien, en relación al análisis que se realiza mediante la presente investigación, los datos sobre ideología y religión constituyen datos sensibles, cuya protección requiere de garantías adicionales. En el caso de menores, cabe visibilizar que dicha información concerniente a los mismos, es doblemente sensible, pues atañe a información de carácter personal de sujetos especialmente vulnerables. Sin ánimo de ser rigurosos pues, no es objeto de estudio del presente capítulo, las redes sociales prevén apartados en los que, el usuario puede compartir en su perfil sus creencias religiosas e ideológicas. Desde luego, la aludida opción, debilita considerablemente la protección de información especialmente sensible, sea de personas adultas o menores de edad.

En cuarto lugar, la LOPJM desarrolla los derechos de asociación y reunión de los menores de edad (art. 7 LOPJM) en desarrollo de los arts. 21 y 22 CE. A pesar de la buena intención de la Ley de protección jurídica del menor, se corresponde con dos derechos que quedan supeditados al ejercicio de la patria potestad. Motivo por el que los menores podrán gozar de dichos derechos si los progenitores conceden su permiso[98].

Por último, los derechos al honor, a la intimidad y a la propia imagen (art 18 CE) se desarrollan por la LOPJM en el art. 4. La decisión de tratar estos derechos en último lugar viene dada por estrecha relación de los mismos para el presente estudio que abordaremos en las siguientes líneas.

En este orden de cosas, deseamos recalcar las cuestiones que siguen. La LOPJM articula una confusa regulación del derecho al honor, intimidad y propia imagen que

[98] PASCUAL MEDRANO, A., "Los Derechos fundamentales y la Ley de Protección del Menor", *op. cit.*, p. 256.

colisiona con la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia imagen[99]. Pero lo más incoherente, a nuestro juicio y en relación con el estudio que este trabajo ofrece, se halla en que, el art. 18 CE alberga en su seno un derecho fundamental más[100]. Nos referimos a la protección de la intimidad y el honor frente al uso de la informática o el derecho a la protección de los datos personales (art 18.4 CE) y el legislador, sorprendentemente no lo ha incluido en la LOPJM.

Dicha ausencia de regulación podía deberse en aquel entonces a que, en el año 1996, las TIC no gozaban de un uso extendido en nuestra sociedad. Si bien comenzaban los primeros pasos en su empleo, que este no se constituyera de manera generalizada pudo llevar al legislador a desechar la necesidad de regular dicho ámbito en la protección de los menores de edad. Sin embargo, esta decisión carece de coherencia legalmente, en el sentido que, la primera norma sobre protección de datos personales, como se verá en el capítulo segundo del presente trabajo, data del año 1992. Además, a pesar de que el derecho a la protección de datos personales no gozó de autonomía propia hasta aproximadamente el año 2000 a través de dos célebres sentencias del TC de 30 de noviembre del 2000, que analizaremos con detenimiento en capítulos posteriores[101], la inquietud sobre la incidencia que las TIC podían poseer sobre los derechos fundamentales de las personas ya existía en el año 1996, cuando se aprueba la Ley de protección jurídica de los menores de edad.

5. TRANSFORMACIÓN DIGITAL Y LOS DERECHOS FUNDAMENTALES DEL MENOR

Determinados derechos fundamentales cuya titularidad recae en menores de edad, quedan expuestos a una erosión mayor facilidad ante el manejo de las TIC lo que inevitablemente conduce a reclamar una mayor protección. Sin embargo, con carácter previo, deviene indispensable conceder determinadas líneas al estudio de la evolución

[99] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, Boletín Oficial del Estado, de 14 de mayo de 1982, núm. 115.

[100] SÁNCHEZ GÓMEZ, A., "El marco normativo tradicional para la protección de los derechos de la personalidad del menor. ¿Alguna asignatura pendiente en el siglo XXI?", *op. cit.*, pp. 9-10.

[101] Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, Boletín Oficial del Estado, de 4 de enero de 2001, núm. 4, pp. 70-93 y Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, Boletín Oficial del Estado, núm. 4, pp. 104-118.

sufrida en la interpretación de los derechos fundamentales ante la aparición de estas herramientas digitales.

5.1. Los derechos de la personalidad del menor y su vulneración en el entorno digital

El extendido uso de las TIC constituye una nueva forma de relación personal y profesional del siglo XXI. En la actualidad, Internet se constituye como una herramienta básica, no solo de recopilación de información, como acostumbraba a ser, sino de relación social[102]. Efectivamente, la web 2.0 irrumpió en la sociedad para permanecer en ella, revolucionando por completo las diversas utilidades que hasta la fecha nos proporcionaba esta herramienta[103].

Actualmente, este espacio *online* ese configura como un espacio colaborativo en el que, el usuario edita, comenta y comparte información en tiempo real. Como señala SÁNCHEZ GÓMEZ, Internet constituye una red que comunica millones de usuarios del mundo de modo que, la información resulta también accesible a millones de usuarios en un tiempo indefinido[104]. Precisamente, esta inmediatez además de la globalidad en la recopilación de información representa uno de sus grandes atractivos. No obstante, esas mismas características sitúan a la red, no solo como un instrumento atractivo para la sociedad, sino como un riesgo para la intimidad y privacidad de las personas que acceden a la misma.

Las posibilidades que la navegación por Internet puede ofrecer son prácticamente infinitas: chatear, enviar y compartir ficheros, realizar videollamadas, llamadas de sonido, compartir fotografías, etc. En efecto, las relaciones interpersonales tienden a desarrollarse de manera virtual tanto a través de páginas web, como de las redes sociales de ocio. Este nuevo paradigma, ha propiciado una reinterpretación de los derechos fundamentales más tradicionales, ya que estos nuevos medios de interacción social han conllevado la

[102] Véase GIL ANTÓN, A., "Redes sociales y privacidad del menor: un debate abierto", *Revista Aranzadi de Derecho y Nuevas Tecnologías parte Cuestiones,* 2014, núm. 36, p. 5: «[…]la gente pensaba en Internet como una gran enciclopedia, un gran repositorio de información. Internet era, básicamente, una gran y enorme biblioteca. Ya no vemos a la web de esa manera. Hoy es algo diferente. […]».

[103] El término Web 2.0 se emplea por primera vez por TIM O´REILLY en 2004 para referirse a una segunda generación en el desarrollo de la tecnología web basada en la proliferación de comunidades de usuarios y una gama de nuevos servicios como redes sociales, blogs etc., que alientan la colaboración y el intercambio de información con una gran celeridad entre usuarios. BARRIUSO RUIZ, C., "Las Redes sociales y la protección de datos hoy", *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, p. 303.

[104] SÁNCHEZ GÓMEZ, A., "Las Nuevas Tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: carencias, interrogantes y retos del legislador", *Revista de Derecho, Empresa y Sociedad,* 2016, núm. 9 julio-diciembre, p. 81.

aparición de nuevas y más sofisticadas técnicas de vulneración de los derechos fundamentales[105]. En este contexto de intromisión para los derechos de la personalidad, los menores merecen una particular atención en el presente trabajo en cuanto a su especial situación de vulnerabilidad.

En este nuevo entorno característico del siglo XXI, cobran especial protagonismo los menores de edad, y concretamente aquellos menores nacidos de manera posterior a 1995 para los que la doctrina ha acuñado el calificativo de *Digital babies* o "nativos digitales"[106]. Desde que adquieren uso de razón e incluso antes, estos menores de edad crecen rodeados de dispositivos electrónicos con los que, entre otras actividades (docentes, educativas…), desarrollan sus habilidades sociales hasta tal punto que, tal y como señala GIL ANTÓN, viven dentro de las redes sociales, donde pasan el tiempo compartiendo novedades, fotografías, imágenes y vivencias personales, segundo a segundo[107]. Antes bien, no se debe olvidar que el manejo masivo de las TIC por menores de edad, no implica necesariamente que estos posean competencias digitales suficientes para protegerse *online*[108].

La aparición de las TIC ha traído consigo la necesidad de adaptar la interpretación de determinados derechos fundamentales a este nuevo escenario *online* que se plantea en el siglo XXI.

Efectivamente, la correcta protección de derechos fundamentales susceptibles de intromisión, implica necesariamente una adecuación y evolución paralela de los mismos a los cambios sociales y tecnológicos acaecidos; ya que, lo contrario predispone la exposición de los mismos a resultar vulnerados con mayor facilidad. En este contexto, el entorno digital se presenta como un nuevo exponente en la evolución de las conductas sociales; un nuevo paradigma del actual siglo que, por supuesto, conlleva a reinterpretaciones y adaptaciones de los derechos relacionados con la personalidad y más concretamente aquellos que protegen la privacidad de los individuos. Es destacable que,

[105] Véase en ese sentido la preocupación visibilizada por la ONU en relación a la protección de los derechos humanos en Internet mediante la Resolución 20/08 del Consejo de la Asamblea General de las Naciones Unidas, sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, de 27 de junio de 2016.

[106] PRENSKY, M., "Digital Natives, Digital Immigrants", *MCB University Press,* 2001, vol. 9, núm. 5, pp. 1-6.

[107] GIL ANTÓN, A., *El derecho a la propia imagen del menor en Internet.* Madrid, Dykinson, 2013. p, 67.

[108] Véase así la Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones, sobre una "Estrategia europea en favor de una Internet más adecuada para los niños", del 2 de mayo de 2012, COM (2012)196 final, p. 6.

la sociedad en general y los menores en particular, son cada vez menos cautelosos de su privacidad. Esto es, la protección de determinada información del resto de personas no se configura como una prioridad tan manifiesta en la actualidad, ya que los menores de edad comparten gran parte de su vida diaria en un portal expuesto a la totalidad del mundo[109].

Por ello, en un entorno menos preocupado por ocultar lo personal, lo privado, aquellos derechos que consagran su protección precisan de una reinterpretación. Con total certeza, cuando en 1978 el legislador incluyó estos derechos en la CE no alcanzaba a imaginar la irrupción de las TIC de un modo tan masivo en el día a día de los ciudadanos, por lo que, en la actualidad, una nueva interpretación de los mismos resulta indispensable con el fin de proporcionar un adecuado marco de protección.

En este entorno de intromisión para la privacidad como el que predispone la red, aquellos derechos que protegen la dignidad de la persona se consideran especialmente vulnerables y necesitados de reinterpretación, puesto que su finalidad reside en proporcionar cobijo a la esencia de cada ser humano y sus cualidades más importantes (art 10.1 CE)[110]. En concreto, las TIC ponen en tela de juicio constante el derecho a la intimidad reconocido en la CE de 1978 en su art. 18. Sin embargo, el art. 18 recoge diversas manifestaciones de la intimidad que merecen especial protección. Específicamente, las TIC constituyen una amenaza para los derechos al honor, a la intimidad personal y familiar y a la propia imagen (art 18.1 CE) pero también sitúan en una posición vulnerable el derecho a la protección de datos personales (art 18.4 CE).

Al hilo de lo expuesto, deviene indispensable diferenciar tres etapas en el tiempo en el uso de este tipo de plataformas para comprender la razón de la vulnerabilidad de los derechos expuestos. Un primer momento en el que, el menor de edad consiente el tratamiento de datos personales mediante la aceptación de políticas de privacidad como requisito previo indispensable para darse de alta como usuario. Un segundo momento, identificado por el habitual manejo de este tipo de plataformas una vez que ya se considera usuario de las mismas, como compartir información en formatos variados que, pueden variar desde imágenes a vídeos, audios, chats, opiniones…y, por último, cuando desea darse de baja de dicha red social ya que, en muchas ocasiones la operación de

[109] En ese sentido, GIL ANTÓN, A., "La privacidad del menor en Internet", *Revista de Derecho, Empresa y Sociedad*, 2013, núm. 3, p. 65.
[110] GIL ANTÓN, A. "Redes sociales y privacidad del menor: un debate abierto", *op. cit.*, p. 5.

cancelación de la cuenta no garantiza una completa eliminación de los datos personales que se vuelcan en la misma.

Mientras que en el primer instante pierde parte de su privacidad al consentir el tratamiento de datos relativos a su persona, exponiendo así su derecho a la protección de datos personales a posibles vulneraciones, en el segundo permitirá de forma reiterada y constante la intromisión en su derecho a la intimidad y datos personales, pudiendo llegar a verse afectados también tanto su derecho al honor, como el derecho a su propia imagen. Sin embargo, los menores de edad no parecen tomar conciencia de las fatales consecuencias que estos actos conllevan respecto a sus derechos fundamentales.

No obstante, todos y cada uno de los derechos fundamentales mencionados, gozan de independencia los unos de los otros[111]. Ello se traduce en que, cada uno de ellos posee su propio contenido esencial que conviene diferenciar, ya que, si bien es cierto que, todos ellos buscan en última instancia la protección de la dignidad de la persona, no todos protegen idénticas esferas de la misma.

Procedemos en las siguientes líneas a proporcionar, aunque no exhaustivamente, una aproximación a cada uno de los derechos susceptibles de sufrir una intromisión ante el empleo de las TIC. Tal y como establece el art. 18.1 CE: *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

El primer derecho fundamental que regula el artículo, es el derecho al honor. Como señala HERRÁN ORTIZ, este alude al juicio de valor que los demás individuos practican sobre las propias cualidades o sentimientos. Esto es, el derecho al honor trata de proteger al individuo de cualquier valoración subjetiva que pudiera privar a la persona titular del mismo del respecto a su dignidad humana[112]. Tal y como señala ROMERO COLOMA, el derecho al honor se entiende como el daño o perjuicio producido al individuo en sus relaciones externas con la comunidad, generando este una disminución

[111] Sin embargo, esta afirmación no fue siempre tan rotunda. Tal y como afirma MARTÍNEZ DE PISON, cuando el reconocimiento del derecho a la intimidad era todavía reciente, la doctrina se encontraba dividida. Parte de la misma partía de la consideración del derecho a la intimidad como único, pero con ramificaciones (derecho al honor, intimidad personal y familiar, imagen…) Por el contrario, otra parte de la doctrina afirmaba que se trataban todos ellos de derechos fundamentales independientes los unos de los otros, los cuales gozaban de autonomía propia, aunque todos proviniesen de la misma matriz: la intimidad o privacidad, y en última instancia, la dignidad de la persona. MARTÍNEZ DE PISÓN, J., "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo", *Derechos y libertades,* 2017, núm. 37, Época II, pp. 58-59.

[112]. En ese sentido, HERRÁN ORTÍZ, A.I., *La violación de la intimidad en la protección de datos personales,* Madrid, Dykinson, 1999, pp. 38-39.

de su estimación entre los miembros de esta[113]. Los jóvenes internautas pueden ver menoscabado su honor en la red de manera casi constante, en el sentido que, el elevado volumen de información que en ella se maneja, no siempre afecta de manera positiva a la imagen que los demás pueden hacerse de la persona.

Por otra parte, la finalidad del derecho a la propia imagen reside en proteger la difusión de los rasgos físicos de la persona que puedan llegar a alcanzar difusión pública. Así, se prohíbe la obtención, reproducción y publicación de la propia imagen por un tercero sin el consentimiento del titular de dicho derecho. En relación a lo expuesto, se consideran intromisiones ilegítimas sobre el derecho a la propia imagen: la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos[114].

Ciertamente, una de las actuaciones principales al darse de alta en una red social consiste en aportar una fotografía personal al perfil del usuario. A pesar de considerarse una aportación relativamente voluntaria, dicha imagen adquiere una difusión máxima en la red[115]. Además, constituye una conducta habitual compartir imágenes de amigos y amigas en la red, o incluso realizar una captura de pantalla de imágenes de otros individuos y compartirlas con otras personas, motivo por el que, la imagen de los menores se expone de manera constante por ellos mismos, o a través de las cuentas de sus contactos, no siempre de una manera consentida.

El derecho a la intimidad personal y familiar, por su parte, protege aquel ámbito que los individuos que no desean mostrar a terceros. Esto es, proporciona cobertura a la conservación de una esfera en la que desenvolver la vida de modo reservado, sin que personas ajenas posean libre acceso a ella[116]. Desde luego, nadie podrá acceder a dicho ámbito privado y oculto de la persona sin el consentimiento de la misma.

---

[113] ROMERO COLOMA, A.M., *Los bienes y derechos de la personalidad*, Madrid, Trivium, 1985, p. 75.

[114] Véanse los arts. 7.5 y 7.6 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. En relación a lo expuesto, con destacado acierto señala ROMERO COLOMA que la captación de una imagen de una persona en un centro comercial y su difusión, no se constituye como un acto íntimo, ni lesiona la reputación o estima personal, pero ello no supone que pueda considerarse un acto público que puede divulgarse sin el consentimiento de la persona interesada. ROMERO COLOMA, A.M., *Los derechos al honor y a la intimidad frente a la libertad de expresión e información. Problemática procesal*, Barcelona, Serlipost, 1991, p. 71.

[115] No son pocas las personas que al introducir una búsqueda con su nombre y apellidos acceden a una fotografía en la web sobre su persona, sin que pueda considerarse a los mismos responsables de colocarla voluntariamente en dicha dirección de Internet.

[116] HERRÁN ORTÍZ, A.I., *La violación de la intimidad en la protección de datos personales*, *op. cit.*, p. 31.

Sin embargo, la mención del derecho a la intimidad nos conduce a traer a colación un debate, ya superado, entre los conceptos de intimidad y la privacidad (*privacy)*, en los ordenamientos anglosajones). Los derechos fundamentales mencionados hasta ahora, pertenecen a los conocidos como "Derechos fundamentales de primera generación". Sin embargo, la evolución experimentada por la sociedad y la aparición de nuevas amenazas para los derechos fundamentales destinados a la protección de la vida privada, han propiciado la aparición de lo que la doctrina identifica como "Derechos Fundamentales de tercera generación"[117].

Estos derechos a diferencia de los anteriores, no surgen con el fin de proteger derechos económicos, sociales, y culturales propio de los "Derechos humanos de segunda generación" o derechos individuales de libertad, sino que su razón de ser, radica en las relaciones entre individuos condicionadas por la tecnología informática. Este grupo de derechos, nace con la necesidad enfrentar las necesidades de los individuos propias de la era tecnológica[118].

En este contexto, mientras que el derecho a la intimidad se circunscribe a la protección de la esfera interna o esencial de la persona, la privacidad genera un derecho a controlar la información, que incide en derechos y libertades de las personas y que se refiere a las facetas del ser humano que, no integrando la parte esencial de su personalidad de manera aislada, pueden llegar a perjudicar al individuo si se relacionan entre sí, ya que desvelarían aspectos de la persona que esta posee derecho a mantener ajenos al conocimiento y utilización de los mismos por terceros[119].

Las TIC suponen una amenaza para ambos conceptos, ya que la red se constituye como un gran portal abierto al mundo en el que la información fluye de manera muy veloz

[117] PÉREZ LUÑO, A.E., "Las generaciones de derechos humanos", *Revista del Centro de Estudios Constitucionales*, 1991, núm. 10, p. 205-209.

[118] Véase en ese sentido la aportación de HERRÁN ORTÍZ cuando señala que podemos encontrar tres tipos de generaciones de derechos fundamentales. Una primera generación de derechos humanos, guiados por la necesidad de garantizar una esfera de autonomía, es decir, asegurando la no intromisión de los gobernantes en la esfera íntima de cada individuo. La segunda generación de derechos humanos, conocidos también como la generación de derechos económicos, sociales y culturales cuyo fin reside en imponer a los poderes públicos la realización de actividades cuyo objetivo resida en garantizar el ejercicio de dichos derechos. Por último, encontramos la tercera generación de derechos fundamentales que nacen con ocasión de defender al ser humano de la amenaza que suponen las nuevas tecnologías para su vida, sea esta privada o no. HERRÁN ORTÍZ, A.I., *La violación de la intimidad en la protección de datos personales, op. cit.*, pp. 70-72.

[119] Véase HERRÁN ORTÍZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales,* Madrid, Dykinson, 2002, p. 51.

y en varias ocasiones, fuera del ámbito de control de las personas usuarias. No es improbable que la información personal se desvele y pueda conocerse en las redes sociales. Sin embargo, ante estas modernas formas de intromisión, los derechos fundamentales también requieren de la garantía de protección en ámbito del individuo que, sin constituir el núcleo de su personalidad, pueden verse afectados[120].

Así, la protección integral de la privacidad de las personas, conlleva a la protección de los datos personales de las mismas regulado en el art. 18.4 CE que reza como sigue: *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

Este derecho fundamental, considerado de tercera generación, garantiza a su titular un poder de control sobre sus datos personales, concretamente, sobre su uso y destino, con el fin de impedir el tráfico ilícito y lesivo de los mismos para la dignidad de las personas, tal y como señala la sentencia del TC 290/2000, de 30 de noviembre. La operación de alta como usuario de una red social, implica la obligatoria aportación de un elevado número de datos personales, a saber: el nombre, apellidos, la edad, aficiones, fotografía del usuario, empleo…desde ese preciso instante, las empresas prestadoras del servicio, se encuentran autorizadas para tratar dichos datos personales, propiciando en el usuario la pérdida del control de dicha información desde ese preciso instante, y también la de aquella que compartirá posteriormente en el seno de su perfil. Estos datos aportados, si bien individualmente podrían no suponer un menoscabo en la intimidad de las personas, el cruce de los mismos que las TIC pueden realizar en cuestión de segundos desvela cantidad de datos que, el deseo de la persona consistiría en que continuaran considerándose anónimos (nuestros gustos, ubicación, viajes…)[121].

Tal y como apunta con destacado acierto MORILLAS FERNÁNDEZ, no debe velarse únicamente por la protección de aquellos datos que desvelan información privada o íntima (para ello ya goza de aplicabilidad el art. 18.1 CE), sino que una adecuada protección de la privacidad debe ofrecer cobertura jurídica a todos los datos que

[120] En efecto, tal y como señala URABAYEN, no todo aquello que se considera privado goza además de la naturaleza de íntimo, porque la intimidad se caracteriza por afectar a la esfera más propia e interna del individuo. Ciertamente, vida privada e intimidad no constituyen sinónimos, porque lo íntimo se indentifica con el núcleo más interno que lo meramente privado. URABAYEN, M., *Vida privada e información: un conflicto permanente*, Pamplona, EUNSA, 1977, p. 347.

[121] En ese sentido se manifiesta con acertado criterio URBANO CASTRILLO, E., "Derechos de la personalidad e Internet", *Revista Aranzadi Doctrinal*, 2010, núm. 9, p. 3.

identifiquen o permitan identificar a una persona, sirviendo esta recopilación para la elaboración de su perfil ideológico, racial, sexual, etc.[122].

De todo ello se desprende que, la aparición de las TIC representa una amenaza más palpable, con consecuencias mucho más lesivas en el tiempo presente para los derechos mencionados. Esa facilidad con la que la información personal puede convertirse en no solo pública, sino viral en cuestión de segundos, protagoniza dicho temor[123]. De esta manera, la protección de los derechos relacionados con lo personal, con lo privado de cada individuo, constituye un auténtico reto para el legislador en la actualidad, más aún cuando los usuarios de las TIC no han alcanzado aún la edad adulta.

En estos casos, el reto puede considerarse doble, ya que, por una parte, los menores de edad crecen desde edades muy tempranas manejando las nuevas tecnologías; Por otra parte, el riesgo al compartir fragmentos de la vida privada, incluso sufrir injerencias en la misma en la red o consentir el tratamiento de datos personales a empresas, propicia que la privacidad se encuentre cada vez más expuesta en la vida de los más jóvenes sin que desarrollen verdadera conciencia sobre ello. Así, sus gustos, preferencias, fotografías, viajes…resultan accesibles a la totalidad de la población, pero para estos, la privacidad ha sido relegada a segundo plano, anteponiendo sus relaciones sociales a su privacidad. Esta afirmación justifica que, dada la especial situación de vulnerabilidad de los menores, el legislador deba abogar por reforzar la protección de dichos derechos, que el menor por sí mismo no puede acometer cuando es usuario de las TIC.

Siguiendo a COLÁS ESCANDON, esta posible vulnerabilidad, justifica la necesidad de velar por la protección de los sujetos que se encuentran en tránsito a la plena madurez, desarrollando normativas que proporcionen una protección añadida que los

[122] MORILLAS FERNÁNDEZ, M., "El menor y su derecho a la intimidad ante los riesgos en la utilización de redes sociales", *Revista de Derecho, Empresa y Sociedad*, 2013, núm. 1 enero-abril, p. 171.

[123] El término "viral" se refiere al fenómeno en el que el contenido difundido a través de Internet o redes sociales alcanza un elevado número de visitas en un espacio corto de tiempo. MARTÍNEZ-RODRIGO, E.; MARTÍNEZ-CABEZA JIMÉNEZ, J., "Desafíos de la Protección de Menores en la Sociedad digital. Internet, redes sociales y comunicación", *Tirantonline.com.* O btenido de: https://www-tirantonline-com.proxy-oceano.deusto.es/base/tol/doctrina/searches?token_id=6311d6f994c32d00132b7051 (última consulta el 2 de septiembre de 2022)

menores de edad necesitan respecto a los posibles ataques a los derechos fundamentales de los que son titulares[124].

5.2. De la necesidad de proteger específicamente el derecho a la protección de datos personales cuya titularidad recaiga en menores de edad

Tal y como se ha evidenciado en el presente estudio, el derecho a la protección de datos personales se erige como uno de los derechos inherentes a la personalidad susceptible de vulneración con gran facilidad en el entorno *online*. Esta aseveración nos conduce a la irrefutable afirmación consistente en reconocer que el menor es titular del derecho a la protección de datos personales.

En efecto, siguiendo a ALÁEZ CORRAL, la edad no es en sí misma considerada como una condición o requisito que delimite la titularidad de los derechos fundamentales por parte de los menores de edad, ni siquiera respecto del derecho de sufragio. Así pues, el menor de edad se considerará titular de todos los derechos que por su inherencia a la persona correspondan originariamente a cualquier individuo con independencia de su nacionalidad[125]. El TC, por su parte, también se ha pronunciado sobre la materia en la sentencia 141/2000, de 29 de mayo de 2000, en la que afirma rotundamente que los menores de edad son titulares plenos de sus derechos fundamentales[126].

Sin ánimo de exhaustividad, puesto que se dedicará un capítulo a su desarrollo, el derecho a la protección de datos personales se identifica como un derecho de la personalidad de nueva generación consagrado en el art. 18.4. CE[127]. La finalidad del mismo reside en limitar el uso de la informática para proteger el derecho al honor, y a la intimidad personal y familiar. A pesar de ello, su configuración como derecho autónomo e independiente del derecho al honor e intimidad personal, regulado también en el art. 18 CE, no se reconoció hasta muchos años después de la promulgación de la CE de 1978. En este hacer, el TC incorpora el derecho a la protección de datos personales, también conocido inicialmente como el derecho a la autodeterminación informativa como un

[124] COLÁS ESCANDÓN, A. Mª., "La defensa del interés del menor en el conflicto entre el derecho a la intimidad de los menores de edad y los derechos y obligaciones derivados de la patria potestad de sus progenitores", *Revista Doctrinal Aranzadi Civil-Mercantil,* 2017, núm. 9, p. 11.
[125] ALÁEZ CORRAL, B., *Temas clave de la Constitución Española. Minoría de edad y Derechos Fundamentales, op. cit.,* pp. 107-108.
[126] Sentencia del Tribunal Constitucional 141/2000, de 29 de mayo, Boletín Oficial del Estado, de 30 de junio de 2000, núm. 156, pp. 40 a 46. En concreto véase el Fundamento jurídico 5º.
[127] VÁZQUEZ DE CASTRO, E., "Protección de datos personales, redes sociales y menores", *Revista Aranzadi de Derecho y nuevas Tecnologías*, 2012, núm. 29/2012 parte Doctrina, p. 1.

nuevo derecho fundamental en sus sentencias 290/2000 de 8 de noviembre y 292/2000, de 30 de noviembre[128].

Así las cosas, cuando los menores de edad se convierten en usuarios de las redes sociales, su derecho a la protección de datos personales se expone a múltiples intromisiones, motivo por el que, en este nuevo contexto digital en el que los menores se desenvuelven en el siglo XXI, se precisa de una protección añadida de este en un entorno tan habitual en su día a día. Como quedará de manifiesto en apartados posteriores, el manejo de las nuevas tecnologías alberga no pocos riesgos, amenazas e incertidumbre para los derechos fundamentales, concretamente para los derechos al honor, intimidad personal y familiar y propia imagen, así como el derecho a la protección de datos personales.

Además, los riesgos se multiplican exponencialmente en el caso de que el usuario de las redes sea un menor de edad por dos motivos. El primero de ellos es que, el menor de edad se encuentra en una situación de tránsito hacia su madurez, de la que la normativa debe velar por su protección tal y como se ha afirmado en apartados precedentes. El segundo motivo, reside en que los menores de edad crecen y se relacionan en las redes sociales, las mismas constituyen un pilar fundamental en su desarrollo personal, lo que, sin duda incrementa notoriamente a la posibilidad de que, en algún momento, sus derechos puedan verse vulnerados sin que ellos sean plenamente conscientes de los abusos a los que pueden verse expuestos ante el tratamiento de sus datos personales.

En esta dicotomía, la línea a seguir debe venir definida por un sistema que propicie la protección integral del menor cuando es usuario de las redes sociales respecto a los derechos de la personalidad que pueden verse seriamente erosionados sin ser plenamente consciente de dicho riesgo. En total acuerdo con CAZURRO BARAHONA, los menores muestran una habilidad innata para manejarse en la red, lo cual lleva aparejados riesgos que la inmadurez o la falta de conocimientos de los menores no siempre permiten identificar[129].

Consciente de esta situación, la UE ha mostrado su continua preocupación por el impacto de las TIC en los derechos de la personalidad, especialmente entre los menores.

[128] Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre y Sentencia del Tribunal Constitucional 292/2000 de 30 de noviembre citadas ambas previamente.
[129] CAZURRO BARAHONA, V., *Derecho digital. Perspectiva interdisciplinar,* Barcelona, Boch Editorial, 2017. pp. 244-245.

Esta circunstancia ha llevado a las instituciones europeas a adoptar Recomendaciones e Informes de Evaluación sobre el grado de cumplimiento de las mismas. Como es sabido, el gran inconveniente de las Recomendaciones reside en que no poseen carácter vinculante para los Estados miembros, por lo que queda al albur de los mismos seguir o no sus dictados.

En el año 1998, el Consejo europeo aprueba la Recomendación 98/560/CE, cuyo fin reside en lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana en el ámbito de la industria europea de servicios audiovisuales y de información[130]. La Recomendación encuentra su justificación en los diversos peligros que entraña el desarrollo de los medios de comunicación digitales para los menores e insta a los Estados miembros a tomar medidas para reforzar la protección de los menores en los ámbitos de radiodifusión e Internet.

Dos años más tarde, la Comisión elaboró diversos Informes de Evaluación entre los que destacan el Informe de Evaluación de 27 de febrero de 2001[131], sobre protección de los menores y la dignidad humana en el que se afirma que las medidas propuestas resultan satisfactorias y además gran parte de los Estados miembros al hilo de la Recomendación preveían campañas en aras de fomentar una utilización más segura de Internet[132].

Ya en 2006, se adopta una nueva Recomendación con el fin de complementar la antigua Recomendación de 2001 citada previamente. Así, el texto invita a los Estados miembros a avanzar hacia una instauración de cooperación eficaz entre la industria, Estados y demás partes interesadas en materia de protección de los menores y de la dignidad a la luz de los avances tecnológicos acaecidos.

Como puede apreciarse, y si bien las Recomendaciones no son vinculantes para los Estados miembros, la UE procura concienciar a los Estados miembros de los riesgos que las TIC suponen para los más jóvenes en el ámbito europeo. Para lo que insta a los países a adoptar medidas protectoras de los menores frente a los riesgos que estas herramientas virtuales suponen.

---

[130] Recomendación 98/560/CE del Consejo, de 24 de septiembre de 1998, Diario Oficial de la Unión Europea, L 270, de 7 de octubre de 1998.

[131] Informe de Evaluación de la Comisión, de 27 de febrero de 2001, sobre la aplicación de la Recomendación del Consejo, de 24 de septiembre de 1998, COM (2001) 106 Final no publicado en el DOUE.

[132] MARCOS MARÍN, T., "Los derechos de la personalidad de las personas-menores en el contexto internacional y su aplicación en el ordenamiento español*", op. cit.*, p. 13.

5.3. Una nueva configuración legal de los derechos fundamentales del menor en la LOPJM: de la necesaria revisión legislativa ante la irrupción de la sociedad de la información

Como se ha señalado en el presente trabajo, la protección jurídica del menor se articula específicamente en la legislación nacional a través de la LOPJM. Por medio de dicho cuerpo normativo, se confiere desarrollo a los derechos fundamentales que el legislador considera deben acomodarse a la minoría de edad con el fin de proteger a este colectivo. Recordemos que el derecho a la protección de datos personales no alcanza de desarrollo adaptado a la minoría de edad en la LOPJM de 1996, si bien, dicha ausencia podía venir justificada en la no consolidada irrupción de la tecnología en el día a día de los menores de edad por aquel entonces.

Tras veinte años de vigencia de la LOPJM, las Leyes orgánicas 8/2015 y 26/2015 modificaron diversos aspectos de la normativa vigente hasta ese entonces[133]. El motivo principal de dicha modificación residía en la obsolescencia que arrastraban la configuración de derechos y el sistema de protección jurídica diseñados en los años noventa. Tal y como establece el propio Preámbulo de la Ley 8/2015, tras veinte años de la aprobación de la citada norma, han acontecido importantes cambios sociales que inciden en la situación de los menores y demandan una mejora de sus instrumentos de protección jurídica con el fin de cumplir de modo efectivo el art. 39 CE.

De la lectura del Preámbulo se desprende que las modificaciones introducidas siguen una clara estela en la adaptación de la LOPJM a las necesidades de la sociedad del siglo XXI. Tal y como se expone en el apartado anterior del presente trabajo, este nuevo siglo se encuentra marcado por las nuevas formas en las que se entablan las relaciones sociales, especialmente entre menores. Este nuevo paradigma de evolución vertiginosa, expone al menor a nuevos riesgos que pueden llevar a generar intromisiones en sus derechos fundamentales que años atrás resultaban impensables.

Por ello, es razonable pensar que el extendido uso de las TIC y de las redes sociales entre los más jóvenes se encuentra dentro de esas nuevas necesidades que es posible que en el año 1996 pasaran desapercibidas dada su falta de entidad y por ello, no

[133] Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema a la infancia y a la adolescencia, citada anteriormente y Ley Orgánica 26/2015, de 28 de julio, de modificación del sistema a la infancia y la adolescencia, Boletín Oficial del Estado, de 29 de julio de 2015, núm. 180.

fueran introducidas en la primera LOPJM de la era postconstitucional; pero el legislador, una vez advertida dicha obsolescencia acomete la tarea de actualizar la normativa jurídica protectora de los menores de edad en un nuevo contexto, la era digital.

En este orden de cosas, la reforma llevada a cabo en 2015 se presentaba como una oportunidad excelente para adaptar la protección de los menores edad a los nuevos riesgos en la vulneración de sus derechos fundamentales, especialmente en el entorno digital. El encaje de dichas modificaciones en la LOPJM resultaba idóneo puesto que, el interés superior del menor que desea proteger la LOPJM en su art. 2 implica la protección y garantía de los derechos fundamentales de los menores con el fin de fomentar el libre desarrollo de su personalidad. Por ello, una protección de los derechos del menor en el entorno digital, conlleva necesariamente una protección reforzada y adaptada a la minoría de edad de los derechos íntimamente ligados a la personalidad del menor como usuario de las TIC, refiriéndonos concretamente a la protección de los derechos al honor, intimidad, imagen y la protección de datos personales.

Por todo lo anterior, ha de lamentarse la oportunidad perdida, habida cuenta que la reforma de 2015 del sistema de protección jurídica del menor, al igual que en 1996, desconoce del derecho a la protección de los datos personales de los menores de edad en plena era digital[134]. Únicamente encontramos una breve referencia en la LOPJM a las TIC cuando el art. 5 se preocupa por el derecho de información del menor, así como su alfabetización mediática con el fin de evitar situaciones de riesgos derivadas del empleo de estas nuevas herramientas.

Desde luego, los riesgos que las nuevas tecnologías suponen no afectan únicamente al derecho de los menores a recibir información, si bien es de destacar el esfuerzo de formar a los menores en el uso adecuado de Internet y las redes sociales, una protección íntegra de los menores en el entorno digital lleva aparejada necesariamente la protección de todos los derechos que pueden sufrir una intromisión cuando el menor emplea las TIC. Es posible que, dicha omisión en la mención se deba a la intención del legislador de regular específicamente la minoría de edad en la futura norma sobre

[134] Acorde con dicha decepción se muestra GARCÍA GARNICA cuando apunta que la reforma se presentaba como una buena ocasión para una regulación más ambiciosa de la tutela de los derechos del menor, y en especial, el de protección de datos personales. GARCÍA GARNICA, M.C., "Datos personales y menores de edad", en GONZÁLEZ PACANOWSKA, I., (Coordinadora), *Protección de datos personales*, Valencia, Tirant lo Blanch, 2020. p. 172.

protección de datos personales, sin embargo, como veremos posteriormente en el presente trabajo, ello no tuvo lugar del modo que cabe esperar, a nuestro juicio.

Consideramos que una correcta protección conlleva, por lo menos, la inclusión en la LOPJM, de los derechos al honor, intimidad personal y familiar y propia imagen, así como el derecho a la protección de sus datos personales[135]. De una revisión no exhaustiva de la norma después de la reforma se desprende que, la LOPJM incluye en su articulado (art. 4) el desarrollo de los derechos al honor, intimidad personal y familiar y propia imagen, adaptando el ejercicio de los mismos a los menores de edad, pero no encontramos desarrollo legislativo alguno sobre el derecho a la protección de datos personales adaptando su ejercicio a la minoría de edad.

Este olvido normativo reviste especial gravedad, pues, el siglo XXI se caracteriza por el vertiginoso crecimiento en el uso de Internet y las aplicaciones de la web 2.0, especialmente entre los más jóvenes. Ello ha supuesto un cambio en los instrumentos por los que pueden erosionarse los derechos sin que la nueva normativa de protección jurídica de la infancia haya acomodado dicha circunstancia a su sistema de protección. Lo cierto es que, el apartado cuarto de la Exposición de Motivos de la Ley 26/2015 constituye una declaración de intenciones vacía de contenido en el sentido que, el mismo desea introducir los cambios necesarios en la legislación en aras de continuar garantizando la protección de la infancia y adolescencia en el Estado, pero a posteriori, no acoge en su articulado el cambio más necesario respecto a los derechos fundamentales de los menores de edad: la potencial vulneración del derecho a la protección de datos de los menores cuando son usuarios de las TIC.

Así las cosas, cuando los menores emplean las TIC, y concretamente las redes sociales, deben diferenciarse dos momentos. Un primer momento, el cual vendría presidido por la prestación del consentimiento para el tratamiento de datos personales cuando el menor se da de alta en una red social, conducta mediante la cual expone el derecho a la protección de datos a ser potencialmente vulnerando. Un segundo momento, cuando el menor realiza actividades propias como usuario de la red social cuando ya se ha dado de alta como interactuar con otros contactos, compartir fotografías, vídeos etc.

[135] De acuerdo con NÚÑEZ ZORRILLA, a día de hoy se echa de menos una regulación en la LOPJM que contemple las neuvas formas de vulneración de los derechos de los más jóvenes en el campo de las tecnologías avanzadas. NÚÑEZ ZORRILLA, Mª.C., "Menor de edad e inteligencia artificial avanzada. Nuevos desafíos jurídicos", *Actualidad civil*, 2019, núm. 12, p. 10.

que principalmente podrán restringir los derechos a la intimidad, honor o imagen, así como la protección de datos personales.

Con mayor o menor acierto, pues no se ha encontrado libre de críticas, los derechos al honor, intimidad y propia imagen disponen de un desarrollo legislativo en la LOPJM que descansa principalmente sobre la madurez del menor a la hora de determinar la posibilidad de consentir el tratamiento de su imagen[136]. A pesar de ello, debemos advertir que la regulación actual de los derechos al honor, imagen personal e intimidad pivota sobre dos normas tratándose de menores: por una parte, la Ley Orgánica 1/1982, y por otra, el art. 4 de la LOPJM adaptando el ejercicio del mismo a la minoría de edad. Lamentablemente, esta regulación ya no protege adecuadamente dichos derechos, pues sus postulados se encuentran marcados por una concepción tradicional de los derechos, y no contemplan en su texto la irrupción de Internet y de las redes sociales entre las posibles vulneraciones de dichos derechos[137].

Sin embargo, no se debe pasar por alto que el peligro para el menor como usuario de las TIC no se encuentra presente únicamente cuando comparte aspectos sobre su vida privada o personal, como fotografías o videos; sino que, el riesgo también se constata en la ingente cantidad de datos personales sobre los que presta el consentimiento para su tratamiento, como condición necesaria para convertirse en ansiado usuario de la red social[138].

Esta circunstancia conduce a una indefensión prácticamente total de los menores de edad cuando navegan en la red, ya que el derecho a la protección de sus datos personales no se regula de manera específica en la LOPJM; y su honor, intimidad e imagen pueden verse reiteradamente vulnerados mediante el uso de las TIC sin que la Ley Orgánica 1/1982 y la LOPJM configuren una protección íntegra de la esfera privada del menor. Lejos de la intención del legislador, la reforma de 2015 cuyo propósito residía en acomodar las nuevas realidades y peligros del siglo XXI para una mejor protección los derechos fundamentales de los menores, tampoco ha incluido en la LOPJM uno de los

[136] SÁNCHEZ GÓMEZ, A., "El marco normativo tradicional para la protección de los derechos de la personalidad del menor. ¿Alguna asignatura pendiente en el siglo XXI?", *op. cit.*, p. 14.
[137] ESCRIBANO TORTAJADA, P., "Algunas cuestiones sobre la problemática jurídica del Derecho a la intimidad, al honor y a la propia imagen en Internet y en las redes sociales", en FAYOS GARDO, A., y CONDE COLMENERO, P., (Coordinadores), *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Madrid, Dikynson, 2015, p. 63-64.
[138] SÁNCHEZ GÓMEZ, A., "El marco normativo tradicional para la protección de los derechos de la personalidad del menor. ¿Alguna asignatura pendiente en el siglo XXI?", *op. cit.*, p. 20.

derechos fundamentales que más caracteriza la nueva era digital: la protección de los datos personales[139].

Por todo lo expuesto, han de lamentarse la ausencia de previsiones específicas en torno a la protección del menor en este ámbito, máxime considerando que en el empleo de las TIC y de las redes sociales, ambas categorías de derechos fundamentales recientemente expuestas pueden sufrir intromisiones. El menor de edad para exponer su vida privada en las redes sociales previamente ha de consentir el tratamiento de datos personales para darse de alta en la red social. Por lo que, hubiera sido acertado incorporar a la LOPJM el desarrollo de ambos derechos inherentes a la personalidad para dotar a la privacidad del menor de una protección reforzada y específica en el ámbito digital tan empleado por los nativos digitales.

En definitiva, la LOPJM se centra exclusivamente en la protección de la intimidad, es decir, en el concepto más tradicional de este derecho y, además, de una manera manifiestamente obsoleta, no adaptando su protección jurídica a un concepto más amplio como resulta la privacidad, en este caso de los menores de edad.

La protección jurídica del menor constituye un pilar fundamental en el ejercicio de los derechos fundamentales por parte del mismo. Así, la autodeterminación de los menores de edad en el ejercicio de dichos derechos conserva un límite establecido: la protección del interés superior del mismo. En el contexto digital, reiteramos que, los menores de edad no advierten los riesgos y amenazas que las TIC suponen para sus derechos a la privacidad. Esta ausencia, sin duda alguna justifica la necesidad de que el sistema jurídico de protección del menor vele por los derechos a la privacidad que el menor de edad no es capaz de proteger por sí mismo, esto es, aquellos que es incapaz de proteger de manera autónoma.

De conformidad con ABA CATOIRA, en plena revolución tecnológica, no se ha formado a los menores en un empleo de manera responsable del gran abanico de

[139] Sorprendentemente, no se considera este un error exclusivo del legislador, ya que se manifiesta a su vez como un error habitual entre la doctrina. En concreto, autores como DÍAZ analizan las vulneraciones que las redes sociales predisponen sobre los derechos del menor, centrando sus esfuerzos en conceder un repaso a aquellos derechos fundamentales susceptibles de vulneración; pero contemplamos con asombro que, si bien se centra en desarrollar las posibles colisiones con el derecho al honor e imagen personal, no centra su análisis en el derecho a la protección de datos personales a pesar de referirse a la privacidad del menor. DÍAZ, J., "Redes sociales: Incumplimiento sistemático de los controles técnicos versus vulneración reiterada de los derechos del menor", *Diario la Ley*, diciembre 2018, núm. 9326, p. 4-5.

herramientas tecnológicas que estos poseen a su alcance. A mayor abundamiento, esta ausencia de formación tecnológica aparejaba que los menores no advirtieran que los derechos fundamentales podían sufrir una amenaza. Además, constituye un factor a considerar que los menores en no pocas ocasiones navegan solos en la red a edades muy tempranas sin ningún tipo de control[140]. Antes bien, en épocas más recientes, puede ser que los menores hayan recibido cierta formación sobre las TIC; sin embargo, convenimos que, a pesar de ello, no perciben los riesgos en suficiente medida o si los advierten, no constituye una prioridad su defensa.

En el contexto descrito, difícilmente se puede confiar en que los menores se protejan autónomamente al amparo de la autodeterminación que la Exposición de Motivos LOPJM reclama, resultando completamente imprescindible una protección legal que la LOPJM no ha diseñado, ya que un único artículo de la LOPJM (art. 5) es francamente insuficiente para lograr una protección integral del menor frente a la amenaza que constituyen las TIC.

Es cierto que un entorno digital seguro conlleva la necesidad de que los usuarios actúen de manera responsable y cautelosa, tomando en consideración los peligros que el mismo engloba, pero en el caso de menores alcanzar dicho grado de responsabilidad autónomamente resulta complejo. Sin perjuicio del protagonismo que corresponde a los progenitores (art. 154 CC, entre otros), educadores e Instituciones en este proceso de concienciación, la normativa específica de protección de los derechos fundamentales debiera proporcionar seguridad y protección al menor cuando socializa virtualmente y así cumplir el mandato constitucional del art. 39 CE que aboga por la protección de la infancia. Desde luego, desde la promulgación de la CE, la protección del menor no constituye tarea exclusiva de sus progenitores, sino que también ha de garantizarse por los Poderes Públicos (art. 39.1 y 39.2 CE). De conformidad con PIÑAR MAÑAS, ningún derecho fundamental debe dejarse en manos exclusivas de la autorregulación[141].

Tal y como se expone en apartados precedentes, un correcto sistema de protección de la infancia debe combinar dos dimensiones que se encuentran íntimamente ligadas entre sí como son: la autonomía, esto es, la posibilidad de que los menores de edad

[140] ABA CATOIRA, A., "Los menores ante Internet", *Congreso Internacional de Derecho y Nuevas tecnologías*, Bilbao, Universidad de Deusto, 2009.
[141] PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales" en PIÑAR MAÑANAS, J.L., (Coordinador), *Redes sociales y privacidad del menor*. Madrid, Reus, 2011, p. 83.

ejerciten por sí mismos los derechos fundamentales de los que son titulares, reconociéndose para tal fin una capacidad acorde a su madurez; y la protección, que debe velar en todo momento por la salvaguarda dicho ejercicio de derechos fundamentales del menor como sujeto especialmente vulnerable. Solamente una correcta combinación entre ambos conceptos desemboca en un desarrollo de la personalidad garantista del menor, y en esencia, acorde a su interés superior.

Únicamente bajo la previsión de dichas condiciones en la normativa de protección del menor, el entorno digital se tornará un paso más seguro para los menores de edad, esto es, cuando se les conceda determinado ámbito de autonomía cuando navegan por la red o redes sociales, pero a su vez, se prevea un íntegro sistema específico de protección jurídica que vele por su interés superior. Este marco normativo sólido garantizará al menor la ausencia de abusos en el tratamiento de sus datos personales y una adecuada protección a sus derechos al honor, intimidad e imagen personal cuando interactúa a través de las TIC.

Por todo lo expuesto, la construcción de dicho marco normativo específico que dote de protección al menor cuando es usuario de las TIC, debe estar definido por la inclusión del derecho a la protección de datos personales en la LOPJM, así como por una nueva adaptación a la era digital del art. 4 de la citada norma sobre el desarrollo de los derechos al honor, intimidad y propia imagen. No obstante, nos mostramos conformes con que, la LOPJM comience por visibilizar el derecho a la protección de datos personales al fin de actualizar su articulado a la era digital, y que los controles y garantías normativas para la información personal del menor continúen desarrollándose en la normativa específica sobre protección de datos personales de cuya suficiencia, nos pronunciaremos en capítulos posteriores.

CAPÍTULO II:

LA CONSTRUCCIÓN NORMATIVA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES. SU CONFIGURACIÓN A LA LUZ DEL INTERÉS SUPERIOR DEL MENOR

El ordenamiento jurídico español no se encuentra provisto de un cuerpo normativo cuyo objeto recaiga en la protección específica del derecho fundamental a la protección de datos personales de los más jóvenes. En efecto, en 2015 el legislador abogó por adaptar la normativa sobre protección jurídica del menor al nuevo paradigma digital sin prever en su articulado la regulación del derecho a la protección de datos personales como derecho de la personalidad íntimamente relacionado con la privacidad.

Esta falta de previsión normativa, quizás podría deberse a la intención del legislador de regular la descrita circunstancia en las leyes orgánicas de protección de datos personales. Por ello, resulta de vital relevancia dilucidar si, las mentadas disposiciones normativas, amparan los datos personales de los más jóvenes como sujetos especialmente vulnerables.

1. ANTECEDENTES NORMATIVOS DE LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO INTERNACIONAL

La evolución del derecho a la intimidad, que terminaría con el reconocimiento de un derecho fundamental a la protección de datos personales, puede situarse entre la segunda mitad del siglo XX y la primera década del siglo XXI. Así, el primer antecedente del derecho a la intimidad, estrechamente ligado a este derecho fundamental se encuentra en el art. 12 de la Declaración Universal de los Derechos del Hombre aprobada en París por la Asamblea General de las Naciones Unidas (ONU) el 10 de diciembre de 1948, que establece que, nadie podrá ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o a su reputación. Continúa el precepto disponiendo que, toda persona poseerá el derecho a la protección de la ley frente a tales injerencias o ataques[142].

Poco después, el art. 8 del Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales firmado en Roma el 14 de noviembre de 1950,[143] y los arts.

[142] Resolución 217 A (III) de la Asamblea General de las Naciones Unidas, por la que se adopta la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948.

[143] Recordemos que el art. 8 del Convenio de 4 de noviembre de 1950, sobre la Protección de los derechos Humanos y las Libertades Fundamentales, hecho en Roma. de 24 de noviembre de 1977, dispone que toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia. Así, no podrán llevarse a cabo injerencias por parte de la autoridad pública en dicho derecho, salvo que esta se prevea por ley o constituya una medida que, en una sociedad democrática, se precise necesaria para la

17 y 19 del Pacto de los Derechos Civiles y Políticos firmado en Nueva York el 19 de diciembre de 1966, citada anteriormente en la presente investigación, contienen referencias a la vida privada o el derecho a no ser molestado.

No obstante, la sociedad ha sufrido una transformación tecnológica imposible de predecir medio siglo atrás, que ha modificado de manera significativa tanto los comportamientos de las personas como las relaciones entre ellas. A día de hoy, las personas se relacionan de manera muy diferente, cuestión que el Derecho, desde luego, ha tratado de regular con el fin de continuar ordenando los comportamientos humanos transformados por la revolución tecnológica[144]. En este devenir, los diversos organismos internacionales procedieron a afrontar el reto de regular nuevos derechos que otorgaran protección suficiente frente a los riesgos y amenazas que el nuevo contexto digital comenzaba a generar.

Así las cosas, cabe destacar la labor, tanto de la ONU como de la OCDE en la configuración y transformación del derecho fundamental a la protección de datos de carácter personal, regulación que, posteriormente influirá decisivamente sobre la normativa comunitaria y nacional de los Estados.

1.1. Las valiosas aportaciones de la ONU y la OCDE en torno al tratamiento de datos personales

En 1968 tiene lugar en Teherán la Conferencia Internacional de los Derechos del Hombre en la que se recomienda a la ONU que proceda al estudio de las cuestiones planteadas en relación a los derechos del hombre que resulten afectados por el desarrollo de la técnica y la ciencia[145]. Las conclusiones alcanzadas en dicha Conferencia Internacional influyen decisivamente en la Resolución 2450 (XXIII), de 19 de diciembre de 1968 en la que se dispone la necesidad de establecer determinados límites a las aplicaciones de la electrónica por su incidencia en los derechos de la persona[146].

seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[144] RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales 1978-2018", *Revista de Derecho político,* 2018, núm. 100, p. 642.
[145] HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales, op. cit.,* p. 55.
[146] Resolución 2450 (XXIII) de la Asamblea General de la ONU sobre Derechos Humanos y progresos Científicos y Tecnológicos, de 19 de diciembre de 1968.

Advertidos los riesgos que la informática puede conllevar respecto a los derechos humanos, el estudio sobre la incidencia de las nuevas tecnologías en los derechos humanos culmina en 1983 cuando la Comisión de Derechos Humanos elabora un informe relativo al estudio de los principios rectores que habrán de regir en la utilización de ficheros informatizados de datos de carácter personal[147]. Fruto de dicho estudio, en el año 1990, la Asamblea General de la ONU concede libertad a cada Estado para la reglamentación de los ficheros computadorizados de datos personales, pero elabora una suerte de orientaciones que los Estados deberán observar en sus respectivas normativas mediante la Resolución 45/95, de 14 de diciembre de 1990 por la que se aprueban los principios rectores para la reglamentación de los ficheros computadorizados de datos personales[148].

También en el ámbito internacional y como veremos a continuación, la OCDE contribuye a visibilizar la necesidad de protección de la intimidad frente a la informática. Ahora bien, en contraposición a la libertad concedida a los Estados por la ONU mediante la Resolución 45/95, la OCDE aboga por una normativa de protección de datos armonizada. Para dicho cometido, el organismo internacional procede en el año 1978 a la constitución de un Grupo de Trabajo específico cuya labor culmina con la aprobación por el Consejo de la OCDE de la Recomendación de 23 de septiembre de 1980 sobre protección de la privacidad y flujos transfronterizos de datos personales[149].

Tal y como destaca el propio texto, las directrices elaboradas poseen vocación de unanimidad en el ámbito internacional en lo relativo a las guías generales que deberán respetarse en la recogida y gestión de información personal. Ciertamente, las Directrices reconocen que las leyes y políticas nacionales pueden diferir, pero ello no obsta a que, los Estados posean un interés común en proteger la privacidad de los individuos, conciliando a tal efecto la privacidad y el libre flujo de información. Sin embargo, preocupa

[147] Informe final de la Comisión de Derechos Humanos de la ONU sobre "El estudio de los principios rectores pertinentes a la utilización de ficheros computadorizados de datos personales", de 30 de junio de 1983.

[148] Resolución 45/95, por la que se aprueban los principios rectores para la reglamentación de los ficheros computadorizados de datos personales, de 14 de diciembre de 1990. Obtenido de: http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf (última consulta el 8 de marzo de 2022).

[149] OCDE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* París, de 23 de septiembre de 1980.

especialmente a la OCDE que las heterogéneas legislaciones nacionales puedan llegar a obstaculizar los flujos transfronterizos de datos, que constituyen una nueva forma de relación entre los países que contribuye al desarrollo socioeconómico. Concretamente, la verdadera preocupación del mencionado organismo internacional, residía en que el establecimiento de óbices injustificados a los flujos transfronterizos de datos personales pudiera ocasionar la disparidad de legislaciones. Circunstancia que lo condujo a valorar de manera urgente la implementación de las Directrices de manera efectiva por los Estados miembros. A pesar de que las Directrices poseen un marcado carácter económico, la privacidad y valores fundamentales de los individuos reciben acomodo en las mismas, ya que el texto subraya que los flujos transfronterizos de datos no menoscabarán la privacidad de las personas. En adición a lo expuesto, el texto de la OCDE establece una serie de principios básicos de aplicación nacional que posteriormente, terminan por cristalizar en normativas nacionales, incluida la española[150].

A la presente Recomendación le sigue la Declaración sobre flujos de datos transfronterizos de 11 de abril de 1985[151], texto que destaca por el compromiso adquirido por los gobiernos que conforman la OCDE en desarrollar enfoques comunes ante materias relacionadas con flujos de datos transfronterizos, así como por la necesidad de adoptar soluciones armonizadas en caso de que fuera preciso. De manera más reciente, la OCDE celebró en Ottawa la conferencia de ministros sobre "Un mundo sin fronteras: determinación del potencial del comercio electrónico" en la que estos reiteraron su compromiso sobre la protección de la privacidad de las redes globales a efectos de garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales. Fruto de dicha conferencia, se aprueba la Declaración ministerial sobre la protección de la privacidad en las redes globales de 18 de diciembre de 1998[152].

[150] Las Directrices, de 23 de septiembre de 1980 elaboradas por la OCDE, recientemente citadas, incluyen un listado de principios básicos de aplicación nacional como son el principio de limitación de recogida, el principio de calidad de los datos, el principio de especificación de los fines, el principio de limitación de su uso, el principio de salvaguarda de la seguridad, el principio de transparencia, el principio de participación individual y, por último, el principio de responsabilidad.
[151] Declaración sobre flujos de datos transfronterizos aprobada por la OCDE, de 11 de abril de 1985. Obtenido de: https://www.oecd.org/sti/ieconomy/15590267.pdf (última consulta: 22 de septiembre de 2020)
[152] Declaración Ministerial elaborada por el Grupo de Trabajo sobre Seguridad de la Información e Intimidad de la Dirección de Ciencia, Tecnología e Industria relativa a la protección de la intimidad en las redes globales, Ottawa, 7 a 9 de octubre de 1998, (98)10/FINAL.

Con todo, la OCDE reafirma los objetivos establecidos en las Directrices elaboradas en el año 1980 y la Recomendación sobre flujos de datos transfronterizos de 1985, citadas ambas anteriormente, manteniendo dichos textos como máximos referentes de protección de la intimidad, ahora en las redes globales. De este modo, los principios básicos establecidos desde 1980, que deben regir los tratamientos de datos personales, guiarán también el tratamiento de los mismos a través de las redes globales. Cabe destacar que la OCDE toma conciencia de la, cada vez más intensa, irrupción de las TIC desde el año 1998, para lo que trata de continuar aportando un marco uniforme en el flujo de datos personales entre diversos países con el fin de proteger la intimidad de las personas. Sin embargo, lo más remarcable reside en el deseo de la OCDE de facilitar orientaciones prácticas a los Estados acerca de la puesta en práctica de las Directrices en entornos en línea, teniendo en cuenta, los diferentes enfoques de protección de la intimidad adoptados por los diversos países. En épocas más recientes, y en directa consonancia con lo expuesto, el Consejo de la OCDE continuó elaborando recomendaciones con dicho matiz, a través de las Recomendaciones de 25 de julio de 2002, para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad y la Recomendación, de 12 de julio de 2007, relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad[153].

En el contexto descrito, los citados textos internacionales evidencian la preocupación existente a nivel internacional, desde épocas relativamente tempranas en proteger la intimidad de las personas frente a las amenazas que el empleo de la informática supone. Desde luego, el tratamiento de datos que la informática proporciona, conlleva no pocos riesgos que amenazan los derechos fundamentales de los usuarios de la misma pese a constituir un gran desarrollo para el ser humano. Por ello, de acuerdo con HERRÁN ORTIZ, resulta imprescindible evitar que la tecnología se pueda volver contra la persona, por lo que es necesario encauzar adecuadamente los medios que esta ofrece[154].

Sin embargo, los textos internacionales sobre los que venimos trabajando en el

[153] Recomendaciones de la OCDE, para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad, de 25 de julio de 2002 y Recomendación sobre a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad de 12 de julio de 2007. Ambas recomendaciones se encuentran disponibles en la siguiente dirección: https://www.oecd.org/sti/ieconomy/34912912.pdf (última consulta el 5 de septiembre de 2022).

[154] HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales, op. cit.,* p. 60.

presente epígrafe, poseen un impacto muy limitado en las normativas nacionales sobre protección de datos personales. Podemos destacar la virtud de dichos textos como responsables de visibilizar los riesgos que la informática puede acarrear para los datos de carácter personal, así como la necesidad de una evolución normativa lo más armonizada posible con el fin de evitar obstaculizaciones innecesarias en los flujos de datos. En aquellos años en los que la informática no había alcanzado el nivel de desarrollo actual, la relevancia que la OCDE deseó conceder al nuevo fenómeno de tratamiento de datos personales resulta más que positivo, ya que incluso trató de orientar a los Estados para que los tratamientos de datos personales se regularan de la manera más homogénea posible, cuestión desde luego especialmente beneficiosa. Pero a pesar de los esfuerzos en procurar la armonización en el tratamiento de datos personales por medio de las Directrices elaboradas en el año 1980, y su adaptación al nuevo contexto de redes globalizado en 1998, dicha armonización no se alcanzó, principalmente porque las Recomendaciones emitidas por la OCDE no poseen carácter jurídicamente vinculante.

Consecuentemente, los Estados desarrollaban sus normativas sobre tratamiento de datos personales de forma no paralela, sin advertir que, dicha falta de sintonía desembocaría, por una parte, en sendas dificultades para el intercambio y tráfico de datos personales; y por otra parte, en la desprotección de los datos personales de las personas cuyos datos se recababan. A dicha circunstancia cabe añadir, que la minoría de edad no se regula en ninguno de los textos internacionales. No obstante, este hecho deviene lógico, pues en aquel entonces la irrupción de las TIC no había acontecido, y los menores no se consideraban por aquel entonces ávidos usuarios de dichos servicios.

1.2. La contribución del Consejo de Europa a la protección de datos personales: El Convenio nº 108 y sus posteriores modificaciones

En el año 1967, la Comisión Consultiva del Consejo de Europa aborda el estudio de las nuevas tecnologías y la influencia de las mismas en los derechos de la persona. Dicho análisis, culmina con la aprobación de la Resolución 68/509/CE de la Asamblea del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos y técnicos[155]. El principal cometido de la Recomendación residía en invitar al Comité de Ministros a estudiar la idoneidad de la regulación interna sobre tratamiento de datos

[155] Resolución 68/509/CE, de la Asamblea Parlamentaria del Consejo de Europa sobre los derechos humanos y los nuevos logros científicos y técnicos, de 31 de enero de 1968.

personales de cada Estado miembro con el fin de garantizar la protección de la vida privada en relación con la moderna evolución de la tecnología[156]. Tras la conclusión del estudio y constatada la insuficiencia existente en las legislaciones internas respecto a la protección de datos personales, el Comité de Ministros adoptó dos resoluciones, a saber: la Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado[157];y la Resolución R (74) 29, sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público[158].

Las cuestiones más relevantes de ambas resoluciones se acogen por las legislaciones internas de cada Estado miembro, sin embargo, el temor del Consejo de Europa al desarrollo normativo no armonizado en cada uno de los Estados, evidenció la necesidad de elaborar una norma de carácter internacional con alcance obligatorio; y así evitar lo que GARRIGA DOMINGUEZ califica con acierto como paraísos de datos[159]. Es decir, surge la necesidad de brindar una protección común uniforme y adecuada para que los datos circulen libremente además de garantizar el respeto al derecho a la vida privada[160].

Desde luego, el miedo a que la protección de datos personales no avanzara de modo uniforme, propició que, en 1976 el Comité de Ministros del Consejo de Europa encargara a un Comité de expertos la elaboración de un Convenio para la protección de la vida privada en relación, por una parte, al tratamiento automatizado de datos personales; y por otra, a la transmisión internacional de datos. Así las cosas, el 28 de enero de 1981 se aprueba el Convenio número 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, cuya

[156] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data y de la Computación ubicua*, Madrid, Dykinson, 2016, p. 149.
[157] Resolución R (73) 22, del Comité de Ministros del Consejo de Europa relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973.
[158] Resolución R (74) 29 del Comité de Ministros del Consejo de Europa sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, de 20 de septiembre de 1974.
[159] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data y de la Computación ubicua, op. cit.*, p. 150. En efecto, de conformidad con la autora, las disparidades normativas pueden conducir a que empresas responsables del tratamiento busquen Estados con normativas menos estrictas en relación a la protección de datos de carácter personal.
[160] El Consejo de Europa advierte al igual que la OCDE de la imperiosa necesidad de armonizar el tratamiento de datos de carácter personal, con el fin de evitar que la circulación de los mismos entre diversos Estados se tornara imposible a futuro dadas las disparidades existentes en sus respectivas legislaciones.

entrada en vigor data del 1 de octubre de 1985[161]. Tal y como dispone el Preámbulo del Convenio, se reconoce la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de información entre pueblos, constituyendo una necesidad de primer orden proteger el derecho a la vida privada ante la intensificación de la circulación de datos que se tratan de manera automatizada a través de las fronteras. Con la publicación del Convenio, se regulan por primera vez, de manera jurídicamente vinculante, los principios básicos para la protección de datos personales, que, desde ese preciso instante, los Estados ratificantes deberán respetar en las regulaciones nacionales relativas a la materia. Así, el Consejo de Europa, al igual que la OCDE, toma plena conciencia sobre la gran relevancia que adquiere la confección de una normativa uniforme y armonizada en la materia. Pero a diferencia de la OCDE, cuyo deseo de armonización podía verse frustrado al no elaborar dichas directrices mediante un texto jurídicamente vinculante, el Consejo de Europa ataja dicha cuestión a través de la adopción de un convenio jurídicamente vinculante.

Cabe señalar, que a pesar de que el Convenio emana de un órgano europeo como el Consejo de Europa, en consagración del art. 8 del Convenio Europeo de Derechos y Libertades Fundamentales, de 4 de noviembre de 1950, la vocación del Convenio 108 reside en que el mismo se ratifique por Estados no pertenecientes a Europa. En ese sentido, al Convenio número 108 se le atribuye vocación global como estándar internacional en la protección de datos personales y se posiciona como primer instrumento internacional jurídicamente vinculante para los Estados. En efecto, el Convenio 108, además de permitir una armonización en el Derecho interno de los Estados en la protección de datos personales, contribuyó a la fijación de los elementos principales del contenido del derecho a la protección de datos personales[162]. Así, influyó

[161] Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, de 28 de enero de 1981. Instrumento de ratificación de España del 27 de enero de 1984, Boletín Oficial del Estado, de 15 de noviembre de 1985, núm. 274.

[162] Los principios básicos que se establecen los siguientes, a saber: 1 º) *Calidad de los datos*. Los datos de carácter personal objeto de tratamiento automatizado deberían: a) obtenerse y tratarse leal y legítimamente registrándose para finalidades determinadas y legítimas, y no utilizándose de forma incompatible con dichas finalidades; b) ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hubieran registrado; c) ser exactos y actualizados; d) conservándose exclusivamente durante un tiempo necesario para las finalidades para las cuales se hubieran registrado. 2º) *Datos sensibles*. Los datos que revelasen origen racial, opiniones políticas, convicciones religiosas u otras convicciones, y los relativos a condenas penales, a la salud o a la vida sexual, no podrían tratarse automáticamente salvo con las garantías apropiadas. 3º) *Seguridad de los datos*. Deberían adoptarse las medidas de seguridad apropiadas para la protección de datos registrados en ficheros automatizados para evitar su destrucción o pérdida accidental y el acceso, modificación o difusión no autorizados. 4º) *Derechos de acceso, rectificación y cancelación*.

positivamente en el reconocimiento y tutela del derecho fundamental a la protección de datos personales en la UE, y en la posterior elaboración de un marco normativo europeo de protección de datos cuyo análisis abordaremos en líneas posteriores del presente estudio[163].

Antes bien, hemos de señalar que, de conformidad con CONDE ORTIZ el Convenio presentó dos importantes debilidades, que en cierta medida provenían de la no aplicabilidad directa del Convenio a los Estados firmantes, los cuales debían adoptar leyes nacionales que propiciaran el cumplimiento del mismo[164]. En primer lugar, el texto normativo permitía a los Estados el desarrollo del contenido de los principios en él contenidos. En consecuencia, a pesar de existir determinados principios fijados por el Convenio, el desarrollo de las legislaciones podía continuar evolucionando de manera no uniforme. En segundo lugar, concedía libertad a los Estados para diseñar las excepciones al tratamiento de datos, por lo que, podía ocurrir que los datos personales protegidos por el Convenio no recibieran tal protección en el Estado adherido al incluirse los mismos en el ámbito de aplicación de la exclusión del tratamiento.

En adición a las debilidades expuestas, a nuestro juicio, la falta de ratificación del Convenio por parte de la mayoría de los Estados también influyó decisivamente en que el Convenio 108 no alcanzara los objetivos planteados. Así, el texto normativo debía firmarse y ratificarse por los Estados en un determinado plazo, y una vez ratificado el mismo, incorporar el contenido vinculante de este en sus normativas nacionales. Desde luego que, la ausencia de ratificación del Convenio 108 auguró una consecuencia muy clara: las normativas de los Estados continuaban su desarrollo de manera no uniforme, propiciando que, la posibilidad de armonizar la materia de protección de datos resultara

Cualquier persona tendría derecho a: a) obtener a intervalos razonables, sin demora ni gastos excesivos la confirmación de la existencia de ficheros automatizados de datos que le conciernan y la comunicación de dichos datos en forma inteligible; b) la rectificación o borrado de dichos datos cuando se hubieran tratado infringiendo estos principios básicos; c) y disponer de un recurso de no atenderse las peticiones anteriores. Las limitaciones a los principios y los derechos anteriores únicamente podrían referirse a: a) la seguridad del Estado, seguridad pública, los intereses monetarios del Estado o represión de infracciones penales; b) ficheros automatizados de datos para fines estadísticos o de investigación científica. Los Estados se comprometerían a establecer sanciones y recursos contra las infracciones de los principios básicos para la protección de datos. RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de los nuevos derechos digitales (1978-2018)", *op. cit.*, pp. 648-649.

[163] TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, 2012, núm. 43, pp. 18-19.

[164] CONDE ORTIZ, C., *La protección de datos personales,* Madrid, Dykinson, 2006.

cada vez más compleja dada la mayor distancia que paulatinamente se advertía entre las normativas nacionales de protección de datos. Estas debilidades se consideraron las responsables de que, sin duda, a nivel europeo quedara de manifiesto la necesidad de armonizar la materia sobre protección de datos personales, cometido que, en aquel entonces culminaría con la aprobación de la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[165] (en adelante, Directiva 95/46/CE), que se someterá a estudio en apartados siguientes.

Tras veinte años de vigencia del Convenio 108, el Consejo de Europa aprobaba el 23 de mayo de 2001 el Protocolo Adicional para la protección de las personas con respecto al tratamiento automatizado de datos personales relativo a las autoridades de control y a los flujos transfronterizos de datos personales[166]. Dos son las cuestiones por las que destaca la elaboración del Protocolo expuesto. La primera de ellas reside en que, el texto se propone el refuerzo de la puesta en marcha y la aplicación efectiva de los principios enunciados en el Convenio 108, en especial, en lo relativo al repentino crecimiento de flujos transfronterizos de datos de carácter personal llevados a cabo entre un Estado parte del Convenio y un Estado tercero u organización que no reviste tal condición. La segunda de las cuestiones reside en que el Consejo de Europa tomaba conciencia de los no pocos riesgos que las nuevas tecnologías y la globalización de intercambios internacionales podían suponer para la efectividad de la protección de los derechos regulados en el Convenio[167]. No obstante, la preocupación por el riesgo que las TIC suponían para la salvaguarda de los datos de carácter personal, ya se había puesto de manifiesto por la organización mediante la Recomendación (99) 5, de 23 de febrero de 1999, sobre la protección de la vida privada en Internet[168], procediendo el Protocolo a su inclusión en la

[165] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial de la Unión Europea, L 281, de 23 de noviembre de 1995.
[166] Protocolo Adicional al Convenio para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, de 8 de noviembre de 2001, hecho en Estrasburgo por el Consejo de Europa. Instrumento de ratificación de España de 24 de septiembre de 2009, Boletín Oficial del Estado, nº 228, de 20 de septiembre de 2010, pp. 79619-79624.
[167] PAVÓN PÉREZ, J.A., "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", *Anuario de la Facultad de Derecho. Universidad de Extremadura,* 2002, s/n, pp. 241-242.
[168] Recomendación (99) 5, adoptada por el Comité de Ministros durante la 660ª reunión de Delegados de Ministros sobre la protección de la vida privada en Internet. Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información", de 23 de febrero de 1999.

normativa jurídicamente vinculante. Lamentablemente, a nuestro juicio, a pesar de valorar positivamente dichas referencias que el Protocolo Adicional realizaba en su articulado, la efectividad del mismo no sufrió modificación alguna tras su publicación. Esto es, la normativa de protección de datos de carácter personal regulada por el Convenio 108 y el Protocolo Adicional de 2001 no configuran un suficiente nivel de protección de los datos personales ante el alcance de las TIC al proclamarse como una mera declaración de principios.

Si bien el Consejo de Europa ha procurado adaptar la normativa vigente, con mayor o menor éxito, a las nuevas situaciones recientemente expuestas que pueden incidir en la protección de datos de carácter personal, la protección de los datos de carácter personal de los menores de edad no ha gozado de la misma suerte. El Protocolo aprobado en 2018 por el Consejo de Europa *amending the Conovention for the Protection of Individuals with regard to Automattic Processing of Personal Data*[169], solamente cita a los menores en relación al rol de las Autoridades de control de la Convención, recordando a las mismas que deben promover la concienciación entre los responsables y encargados del tratamiento, de su responsabilidad en el tratamiento de datos, especialmente atendiendo a los derechos de los menores y de otras personas vulnerables. En definitiva, el Consejo de Europa continúa sin acoger en su seno una normativa especialmente dirigida a la protección de los datos personales de la minoría de edad, pues, ni tan siquiera regula un aspecto tan fundamental como las condiciones para la validez del consentimiento prestado por menores de edad[170].

1.3. La proyección internacional del derecho a la protección de datos en el siglo XXI. Una tímida visibilización de la protección del menor

En épocas más recientes, la ONU ha continuado elaborando textos en relación a la protección de datos personales, sentando como objetivo principal la protección de la privacidad frente a la informática acorde con la evolución que dicha herramienta ha

[169] Decisión del Comité de Ministros del Consejo de Europa por la que se adopta el Protocolo *amending the Conovention for the Protection of Individuals with regard to Automattic Processing of Personal Data,* 18 de mayo de 2018. Obtenido de: https://rm.coe.int/16808ac918 (última consulta el 5 de septiembre de 2022).

[170] BENEDITO CAÑIZARES, M.T., "La autorregulación en el Reglamento General de Protección de Datos como solución frente al mercado digital fragmentado: el menor y los Registros", *Revista Crítica de Derecho Inmobiliario,* 2018, núm. 770, p. 3139.

sufrido en las últimas décadas[171]. Es más, el globalizado uso, ya no únicamente de Internet, sino de las redes sociales, la computación en la nube, el *big data*, han supuesto la aparición de sofisticadas técnicas de tratamientos de datos personales, que la ONU ha sabido advertir e intentar dotar de protección.

Así las cosas, el mencionado organismo celebra, el 16 de diciembre de 2015, una reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información en la que se apercibió a los Estados sobre la necesidad de proteger los derechos humanos de las personas usuarias de las Nuevas Tecnologías [172]. Siguiendo dicha estela, la Resolución de 5 de julio de 2018 del Consejo de Derechos Humanos de la ONU sobre la promoción, protección y disfrute de los derechos humanos en Internet, insta a los Estados a reformar, en caso de revestir necesidad, las leyes, políticas, reglamentos y medidas relativas a la protección *online* de los datos personales y la privacidad, con el fin de prevenir, mitigar y remediar la recolección, retención, procesamiento, uso y revelación arbitrarios o ilícitos de datos personales en Internet que pudieran violar derechos humanos. Como puede apreciarse, la ONU ha mantenido presente en sus sesiones la preocupación por la

171
- Resolución 68/167, de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital, de 18 de diciembre de 2013.
- Resolución 69/166, de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital, de 18 de diciembre de 2014.
- Resolución 71/199, de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital, de 19 de diciembre de 2016.
- Resolución 73/179, de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital, de 17 de diciembre de 2018.
- Resolución 28/16, del Consejo de Derechos Humanos sobre la privacidad en la era digital, de 26 de marzo de 2015.
- Resolución 32/13, del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet, de 1 de julio de 2016.
- Resolución 34/7, del Consejo de Derechos Humanos sobre la privacidad en la era digital, de 23 de marzo de 2017.
- Resolución 38/7, del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet, de 5 de julio de 2018.

[172] La propia Resolución 70/125, de la Asamblea General de la ONU sobre Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, de 16 de diciembre de 2015, recoge en su contenido los riesgos y amenazas que el extendido uso de las tecnologías la Sociedad de la Información puede conllevar para los derechos humanos: «Reafirmamos, además, que los mismos derechos de los que las personas gozan fuera de línea también deben ser protegidos en línea. Ponemos de relieve que el progreso hacia la visión de la Cumbre Mundial sobre la Sociedad de la Información debería considerarse no solo una función del desarrollo económico y la propagación de las tecnologías de la información y las comunicaciones, sino también una función de los progresos realizados en lo que respecta a la realización de los derechos humanos y las libertades fundamentales».

salvaguarda de la privacidad, así como la necesidad de adoptar medidas necesarias con el fin de preservarla, concretamente en el entorno en línea.

De manera más específica, y en relación directa con la presente investigación, la Resolución de 19 de diciembre de 2016, de la Asamblea General de la ONU se refiere en su contenido por primera vez a los menores de edad como sujetos sobre los que las violaciones y transgresiones de la privacidad en plena era digital pueden repercutir especialmente, por lo que alienta a los Estados a que continúen elaborando o manteniendo medidas preventivas y procedimientos de recurso que puedan afectar a todas las personas, pero particularmente a niños, mujeres y personas vulnerables o marginadas. Este mismo deseo se manifiesta nuevamente en las resoluciones posteriores sobre el derecho a la privacidad en la era digital como la Resolución 73/179, de 17 de diciembre de 2018 citada anteriormente. Si bien resulta esperanzador que dichas cuestiones se visibilicen en organismos internaciones como la ONU, llama la atención que, dicha visibilidad no se haya conferido hasta años tan recientes como 2016. Recordemos que, los jóvenes nacidos a partir de 1995, calificados por la doctrina citada en el presente estudio como *digital babies*[173], se encuentran inmersos en el pleno manejo de estos dispositivos desde hace años, por lo que, sorprende la existencia de una inactividad de más de dos décadas en la sensibilización y preocupación por la privacidad de los menores en la era digital.

Sin embargo, la sensibilización sobre la protección de la privacidad en el ámbito de las redes globales no se advierte únicamente por la ONU, los diversos Gobiernos han mostrado, cada vez en mayor medida, interés en las preocupaciones que un mundo sin fronteras como Internet puede propiciar. A modo de respuesta, puede hallarse un consenso entre los diversos Estados en la aprobación de unas normas consensuadas de protección de la privacidad, pero como cabe esperar, esta circunstancia ha conllevado a que los Estados deban alcanzar determinados estándares internacionales de protección de datos personales, tarea que ha recaído en las Autoridades de control correspondientes. Pese a ello, estos estándares nunca han llegado a materializarse, aunque sí se han llevado a cabo determinadas actuaciones al efecto como la 30ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Estrasburgo en el año 2008 con el fin de

[173] Recuérdese que el término *digital babie* fue empleado por PRENSKY, M., por primera vez en "Digital Natives, Digital Immigrants", obra citada en el presente trabajo.

elaborar una Resolución que albergara una Propuesta Conjunta de estándares internacionales sobre privacidad y protección de datos. Así, la Resolución de Estándares Internacionales se aprueba finalmente en la 31ª Conferencia Internacional sobre Privacidad y Protección de datos celebrada en Madrid en el año 2009[174].

A dicha Conferencia le siguen otras más recientes como la 41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Tirana en octubre de 2019 cuyo eje central radica en la búsqueda de fórmulas que contribuyan a reforzar los niveles globales de protección de datos en la era digital[175]. Lamentablemente, las conclusiones alcanzadas en dichas conferencias, no poseen valor jurídico vinculante, de modo que, la existencia de esfuerzos internacionales en el camino al consenso, resultan loables, pero han de canalizarse en una norma de carácter vinculante que obligue a los Estados a garantizar un nivel adecuado de protección de los datos personales de las personas usuarias de servicios de la sociedad de la información.

En la línea de lo expuesto, en mayo de 2011 se celebraba en la ciudad francesa de Deauvill la Cumbre del G-8 dedicada a Internet. En la misma, los diversos Gobiernos convenían en la necesidad de establecer un marco jurídico de protección de datos personales eficaz, al fin de asegurar su avance próspero sobre la base del respeto a la privacidad, a la propiedad y a los derechos de las personas. En este sentido, se defendió la insuficiencia de la autorregulación en el campo de las TIC, deviniendo indispensable la transmisión de confianza a los usuarios de las mismas. No obstante, no todos los participantes de la Cumbre se mostraban de acuerdo con la necesidad de establecer un marco jurídico homogéneo de privacidad. En concreto, por aquel entonces presidente de *Google,* Eric Schmidt destacaba que la tecnología habitúa a avanzar más rápido que la capacidad de los Gobiernos en legislar dicha materia, asesorando a estos que no legislaran previo a conocer si la propia tecnología puede resolver los problemas[176]. Nada más lejos de la realidad, en un ámbito en el que el cruce de datos resulta constante y globalizado,

[174] Resolución Estándares Internacionales aprobados en la 30ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Madrid, 2009. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf (última consulta: 22 de septiembre de 2020)

[175] 41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Tirana los días 21 y 24 de octubre de 2019, sobre elevación de los estándares globales de protección de datos en la era digital, Obtenido de: https://privacyconference2019.info/ (última consulta el 22 de marzo de 2023).

[176] En ese sentido se manifestó en Eric Schimidt en su Intervención en el Congreso Internacional Barcelona Mobile World Congress, en febrero de 2012.

deviene necesario un marco jurídico uniforme, que establezca los límites oportunos, pues, de lo contrario, los derechos fundamentales de las personas podrían verse seriamente agraviados.

Si bien es cierto que la tecnología avanza a un ritmo más acelerado que la capacidad legislativa de los Gobiernos, no debe relegarse la solución de los problemas y riesgos que puedan acontecer a los propios prestadores de dichos servicios como, por ejemplo, *Google*, cuyos intereses empresariales no coinciden con el derecho a la privacidad de los usuarios. De modo que, la legislación de los diversos Gobiernos debe configurar un régimen jurídico que proteja los derechos fundamentales implicados y, en especial, el derecho a la protección de datos personales. De conformidad con TRONCOSO REIGADA, la autorregulación se constituye como una solución que goza de legitimidad mientras falte una regulación jurídica al respecto, esto es, la autorregulación solamente procede como complemento a las legislaciones nacionales e internacionales y nunca como garantía única de privacidad de los usuarios[177].

No obstante, lo verdaderamente destacable de la 31ª Conferencia Internacional citada anteriormente, además de por el establecimiento de dichos estándares internacionales en la protección de datos, reside en la elaboración de la Resolución sobre la intimidad de los niños en línea propuesta por el Comisario de Protección de Datos Personales de Canadá[178]. Dicho texto, expresa de manera detallada el nuevo contexto que Internet supone para la interacción social entre los más jóvenes, que deben enfrentarse a las dificultades y desafíos inherentes a la protección de su información personal en línea sin una reglamentación sobre numerosos servicios de Internet, lo que dificulta considerablemente la protección de la privacidad.

Continua la Resolución apuntando que las aplicaciones más populares entre la juventud recopilan un volumen de datos personales que los menores de edad ignoran, bien

[177] TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *op. cit.*, p. 25.

[178] Resolución sobre la intimidad de los niños en línea, adoptada en la 30ª Conferencia Internacional de Autoridades de protección de datos y privacidad, propuesta por el Comisario de Protección de datos de Canadá, adoptada en Estrasburgo, octubre de 2008. Obtenido de https://edps.europa.eu/sites/default/files/publication/08-10-17_strasbourg_children_online_es.pdf (última consulta el 8 de marzo de 2022)

por la falta de lectura de las políticas de privacidad o por la ausencia de transparencia, en el sentido que, se redactan en un lenguaje técnico, poco sencillo y difícilmente comprensible para los jóvenes. A dicha contextualización de la situación en la que se encontraban los menores le siguen una suerte de principios adoptados por los comisarios orientados a la protección de los menores como usuarios de las TIC. Entre dichas orientaciones, destaca la petición que la Resolución dirige a las autoridades para que aprueben leyes que limiten la recogida, utilización y comunicación de datos personales de los niños, incluidas las disposiciones necesarias en caso de incumplimiento de estas exigencias. La Resolución también incita a las páginas web destinadas a los niños para que adopten políticas de privacidad y acuerdos de utilización claros, sencillos y comprensibles.

La constatable preocupación a nivel global por el gran desarrollo de las TIC y los riesgos que estas entrañan, también ha generado preocupación en la comunidad internacional sobre la situación en la que se encuentran los menores de edad como usuarios de Internet. Así, UNICEF elaboraba un Decálogo en 2004 sobre los derechos de la infancia en Internet titulado Los e-derechos de los niños y las niñas[179], en el que se reconoce a los niños el derecho a no proporcionar datos personales a través de la Red. A mayor abundamiento, en 2009 en el seno del seminario sobre Derechos, Adolescentes y Redes sociales, se elabora un Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Dicho documento, aborda la tarea de concienciar sobre las redes sociales e Internet, porque además de constituir un avance extraordinario, también albergan no pocos riesgos que no deben pasar inadvertidos. El Memorándum adopta una serie de recomendaciones al respecto dirigidas a comunidades educativas, entidades privadas y Estados[180]. Ahora bien, el documento expuesto, se constituye nuevamente, como un cuerpo normativo no vinculante.

[179] UNICEF. "Los e-derechos de los niños y las niñas", 2004. Obtenido de: http://www.ciberderechos-infancia.net/e-derechos-unicef.html#:~:text=Dec%C3%A1logo%20UNICEF%3A%20Los%20e%2Dderechos,%2C%20lugar%20de%20residencia%2C%20etc.&text=Derecho%20a%20la%20libre%20expresi%C3%B3n%20y%20asociaci%C3%B3n. (última consulta 17 de septiembre de 2020)

[180] Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, Montevideo, 2009. Obtenido de: http://www.iijusticia.org/Memo.htm (última consulta el 8 de marzo de 2022) apunta las siguientes recomendaciones, entre las que destacan las acciones preventivas y educativas para un uso seguro y responsable de las nuevas tecnologías.

Por todo lo expuesto, gran parte de los textos normativos internacionales jurídicamente vinculantes cuyo fin reside en la salvaguarda de la información personal, permanecen ajenos a la protección de la privacidad en el entorno *online*. En efecto, la Declaración Universal de los Derechos del Hombre de 1948 citada en apartados precedentes, la Recomendación de 23 de septiembre de 1980 sobre protección de la privacidad y flujos transfronterizos de datos personales (no vinculante), entre otros, se consideran textos pertenecientes al siglo pasado en el que, la irrupción de las TIC no había acontecido en la sociedad. Consecuentemente, a pesar de percibir cierta conciencia, visibilizada por medio de resoluciones y Conferencias internacionales posteriores, respecto a las posibles intromisiones a las que se expone la privacidad en plena era digital, el ordenamiento jurídico internacional continúa sin ofrecer una respuesta normativamente garantista con la privacidad de las personas[181].

Es cierto que en épocas recientes se ha aprobado el Tratado Internacional que actualiza el Convenio número 108. El propio Consejo de Europa reconoce que, entre sus objetivos principales se encuentra, por una parte, la adaptación del Convenio a la nueva era digital; por otra parte, el refuerzo de la aplicación efectiva del Convenio, para lo que crea un Comité de vigilancia en los arts. 22 a 24. Antes bien, si bien destacamos positivamente los esfuerzos del Consejo de Europa, nos sorprende que dicho Tratado Internacional no regule la específica protección de la información personal de los menores[182]. Consideramos que, habida cuenta que el nuevo Convenio número 108 se aprueba en 2018, debería prever la protección de los datos personales cuando el titular de

[181] Tal y como indican PALOMAR OLMEDA, A., y PÉREZ GONZÁLEZ, C., en *La protección de datos: su marco constitucional y el contexto del nuevo Reglamento*, Pamplona, Editorial Aranzadi, 2008, p. 18. «No contamos con instrumentos internacionales universales cuya naturaleza sea vinculante en los que el derecho a la protección de datos de carácter personal se consagre como un derecho autónomo […]. Desde luego que, la no regulación del derecho a la protección de datos de carácter personal en la normativa internacional vinculante influye de manera negativa en la protección de la privacidad de las personas, pues estas se muestran indefensas, ante la falta de una normativa internacional garante de dicha circunstancia. Dicha situación se ve manifiestamente agravada cuando, además, los datos personales pueden verse expuestos en el entorno on-line, ya que la normativa ni siquiera protege los datos de las injerencias en los datos privados más tradicionales».

[182] En octubre de 2011 comenzaron las reuniones en Estrasburgo con el fin de analizar las posibles modificaciones del Convenio 108 y su Protocolo adicional. Dichas propuestas de reforma se debatieron en el Pleno del Consejo del Comité Consultivo Europeo el 29 de noviembre de 2011. Tras dichas reuniones, existen tanto un documento sobre propuestas de modernización, de 27 de abril de 2012, como un documento final sobre dicha modernización del Convenio 108, de 17 de septiembre de 2012.

los mismos es menor de edad, ya que, en la actualidad se ha manifestado la especial vulnerabilidad de los menores en este ámbito.

Tal y como se ha evidenciado en presente trabajo de investigación, el marco jurídico internacional ha cobrado especial protagonismo dado su papel de guía y referencia para los Estados; por lo que, a día de hoy, deviene indispensable reconocer en la normativa internacional la rápida evolución que las TIC han supuesto para los derechos humanos. En consonancia con MURILLO DE LA CUEVA, el fenómeno de Internet escapa de las posibilidades de control desde un determinado Estado en concreto, demandando soluciones globales, que lejos se hallan de ser alcanzadas; por ello, resulta indispensable la labor de adoptar criterios internacionales globalmente aceptados que desemboquen, con el tiempo, en estándares internacionales en la protección de datos de carácter personal. Y es que, no es menos cierto que la elaboración de una normativa que albergue criterios comunes, podrá incidir decisivamente en la superación de los obstáculos derivados de la territorialidad de los ordenamientos jurídicos estatales y responda al carácter global de Internet y de las redes[183].

Todo ello nos lleva a advertir que la privacidad de los menores de edad en la era digital se expone en mayor medida a posibles vulneraciones de la misma, pues, no se prevé una regulación internacional específicamente adaptada a las circunstancias de los más jóvenes, bien como usuarios de las TIC o incluso para tratamientos de datos personales convencionales que no se desarrollan en aplicaciones en línea. En definitiva, podemos observar que la comunidad internacional toma conciencia de las circunstancias descritas desde hace una década; sin embargo, la normativa internacional permanece hierática ante un cambio que, además de trepidante, lleva sucediendo desde hace tiempo sin que se adopten soluciones jurídicamente vinculantes.

2. LA UE ANTE EL RETO NORMATIVO DE DESARROLLAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

En el ámbito europeo, la UE también tomó conciencia temprana sobre la notoria incidencia que las TIC causaban en los derechos y libertades de las personas. Sin embargo, el reconocimiento del derecho a la protección de datos personales,

[183] MURILLO DE LA CUEVA, P. L., "El objeto de la Ley Orgánica de Protección de Datos de carácter personal" en TRONCOSO REIGADA, A., (Coordinador), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Editorial Aranzadi, 2010, pp. 95-96.

comunitariamente, protagonizó una evolución pausada debido al manifiesto carácter económico del que adolecía la institución europea. En efecto, cuando se constituyó la UE, los Tratados Constitutivos no incluyeron un catálogo de Derechos Fundamentales en su articulado, considerando suficiente el Convenio Europeo de Derechos Humanos, de 4 de noviembre de 1950, como garante de los mismos. La mentada circunstancia, influirá decisivamente en la evolución normativa del derecho a la protección de datos personales en este contexto.

2.1. La compleja configuración de los derechos fundamentales en la UE: el marcado carácter económico de la normativa europea hasta la aprobación de la Carta Europea de Derechos Humanos, de 7 de diciembre de 2000

El carácter económico de la UE pronto influyó en los derechos fundamentales de las personas, propiciando que, a mitad del siglo XX el TJCE planteara la posibilidad de proporcionar una protección eficaz a los derechos fundamentales en el ordenamiento jurídico comunitario[184]. Efectivamente, los tribunales nacionales solicitaban la anulación de disposiciones europeas alegando que las mismas lesionaban derechos fundamentales de sus Constituciones nacionales, pero el TJCE rechazaba pronunciarse sobre tales cuestiones alegando su incompetencia en la interpretación y aplicación de normas nacionales. Ante esta circunstancia, el TJCE, con el beneplácito de los Tribunales Constitucionales nacionales, inició paulatinamente una labor de reconocimiento sobre su competencia para pronunciarse sobre derechos fundamentales en el ordenamiento jurídico comunitario. En consecuencia, ante la ausencia de un catálogo de derechos fundamentales, el TJCE lideró la tarea de configurar paulatinamente un catálogo de los mismos a modo de principios generales de Derecho comunitario[185].

[184] ARENAS RAMIRO, M., "La protección de datos personales en los países de la Unión Europea", *Revista Jurídica de Castilla y León*, 2008, núm. 16, pp. 116.

[185] El primer caso en el que el TJCE se pronuncia sobre derechos fundamentales es el caso *Stauder* ventilado en la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 12 de noviembre de 1969, *Caso Stauder*, Asunto 29/69. En dicho pronunciamiento, el tribunal europeo reconoce que los derechos fundamentales se constituyen como una parte integrante de los principios generales del Derecho comunitario. De manera posterior, en la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 17 de diciembre de 1970, *Internacionale Handelsgesellschaft*, Asunto 11/70 se consolida dicha afirmación; por último, en la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 14 de mayo de 1974, *Nold*, Asunto 4/73, se afirma ya que, la protección de derechos fundamentales forma parte del Derecho comunitario. Véase también, GARCÍA DE ENTERRÍA, E., (Director) y ALONSO GARCÍA, R., *La encrucijada constitucional de la Unión Europea*, Madrid, Civitas, 2002, p.123.

En el año 1992, se firma en Maastricht el Tratado de la Unión Europea, cuyo artículo sexto incorporaba la doctrina que el TJCE elaboró progresivamente en torno a los derechos fundamentales. Así, reciben la consideración de derechos fundamentales comunitarios aquellos que figuran en la CEDH, que deberán garantizarse como principios generales del Derecho comunitario. No obstante, el sistema descrito se hallaba lejos de recibir la consideración de un sistema garante y sólido de derechos fundamentales, motivo por el que, en 1999 un Grupo de Expertos concluye un Informe que pone de relieve la acuciante necesidad de reconocer de manera explícita los derechos fundamentales en la Unión Europea[186]. Con motivo de dicho Informe, el 7 de diciembre del año 2000, se procedió a la construcción de un catálogo de derechos fundamentales propio de la UE, que recibió el nombre de Carta de Derechos Fundamentales de la Unión Europea[187].

A pesar de lo expuesto, la Carta de Derechos Fundamentales de la UE únicamente había recibido una proclamación solemne, pero carecía de valor jurídico sólido. Con el fin de dotar a la Carta de Derechos Fundamentales de la UE del valor jurídico necesario a efectos de garantizar los derechos fundamentales en la UE, el texto se inserta en el Tratado por el que se establecía una Constitución para Europa. Lamentablemente, dicho proyecto constitutivo no llegó a entrar en vigor. Tras la crisis en el seno de la UE, motivada principalmente por el fracaso del proyecto por el que se aspiraba a una Constitución para Europa, y a modo de solución, se firma el Tratado de Lisboa, de 12 de diciembre de 2007, cuya entrada en vigor data del 1 de enero de 2009[188], concediendo a la Carta de Derechos Fundamentales de la UE el mismo valor jurídico que a los Tratados constitutivos de la UE[189].

La inclusión de los derechos fundamentales en el TUE supuso un cambio de paradigma más que destacable, pues, la UE abandonaba el marcado carácter económico

[186] Informe de la Comisión Europea sobre "La afirmación de los Derechos fundamentales en la Unión Europea. Ha llegado el momento de actuar", de febrero de 1999, elaborado por un Grupo de Expertos bajo la Presidencia del Sr. D. Spiros Simitis. Obtenido de: https://sid.usal.es/idocs/F8/8.4.1-520/8.4.1-520.pdf (última consulta el 9 de marzo de 2022).
[187] Carta de los Derechos Fundamentales de la Unión Europea, aprobada por el Parlamento Europeo el 7 de diciembre de 2000, Diario Oficial de las Comunidades Europeas, C/364, de 18 de diciembre de 2000.
[188] Tratado de Lisboa, de 12 de diciembre de 2007 por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, Diario Oficial de la Unión Europea, C/306/1, de 13 de diciembre de 2007.
[189] Redacción proporcionada al art. 6 del Tratado de la Unión Europea por el Tratado de Lisboa al Tratado de la Unión Europea firmado en Maastricht el 1 de noviembre de 1993: «La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor».

que inspiraba su normativa hasta le fecha, para incorporar en sus textos jurídicos la salvaguarda de derechos fundamentales. Desde luego, la circunstancia descrita afectará de forma significativa al reconocimiento del derecho a la protección de datos personales por la institución europea como quedará de manifiesto.

2.2. El fundamento jurídico del derecho a la protección de datos personales en el Derecho originario de la UE

La construcción del derecho a la protección de datos personales se ha visto influenciado por las limitaciones en el seno de la UE para regular derechos fundamentales. Durante varias décadas, la garantía de derechos fundamentales se apoyaba en el Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950, en el que el art. 8 abogaba por el respeto al derecho a la vida privada y familiar.

En este contexto, y ante la insuficiencia de dicho cuerpo normativo como garantía de derechos, la primera sentencia del TJCE conocida como el *Caso Stauder* aborda una controvertida cuestión relacionada con los derechos fundamentales, concretamente, con el derecho a la protección de datos personales[190]. El señalado pronunciamiento, conduce al reconocimiento de los derechos fundamentales como principios generales de Derecho Comunitario tal y como se ha mencionado. Con carácter posterior, la promulgación del Tratado de Ámsterdam de 2 de octubre de 1997 constituye un nuevo hito en el reconocimiento del derecho a la protección de datos personales, ya que este incluye en el art. 286 TUE la garantía del derecho a la protección de datos personales[191].

[190] Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 12 de noviembre de 1969, *Caso Stauder*, Asunto 29/69 citada previamente. Inicialmente la ausencia de un reconocimiento de derechos fundamentales en los Tratados constitutivos de la Unión Europea se superó manteniendo que los derechos fundamentales reconocidos en los textos constitucionales de los Estados miembros formaban parte de los principios generales del Derecho comunitario y del acervo comunitario. El TJCE afirmó en la Sentencia *Stauder* que los derechos fundamentales se hallaban comprendidos «en los principios generales del derecho comunitario que el Tribunal garantiza», de manera que «el respeto a los derechos fundamentales forma parte integrante de los principios generales del derecho que el Tribunal de Justicia salvaguarda», protección que se inspira en «las tradiciones constitucionales comunes a los Estados miembros». En ese sentido, véase TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *op. cit.*, p. 12.

[191] Tratado de Ámsterdam, de 2 de octubre de 1997 por el que se modifican el Tratado de la Unión Europea y los Tratados Constitutivos de la Comunidad Europea y determinados anexos. Obtenido de: https://www.europarl.europa.eu/topics/treaty/pdf/amst-es.pdf (última consulta el 9 de marzo de 2022).

Con todo, advertida la insuficiencia en la garantía de los derechos fundamentales en la UE, la promulgación de la Carta de Derechos Fundamentales de la UE de 7 de diciembre de 2000 presenta un nuevo escenario en el reconocimiento del derecho a la protección de datos personales, ya que los arts. 7 y 8 de la misma reconocen explícitamente este derecho fundamental[192].

Sin embargo, recordemos la limitada vinculación jurídica de La Carta de Derechos Fundamentales de la UE, motivo por el que el proyecto para una Constitución Europea recogía en su articulado los preceptos I-51 y I-68 garantes del derecho a la protección de datos personales. Lamentablemente dicho proyecto nunca llegó a entrar en vigor, alcanzándose una solución acorde a todos los Estados miembros mediante la promulgación del mencionado Tratado de Lisboa en el año 2007. Este supuso un antes y un después en el reconocimiento del derecho a la protección de datos personales por dos motivos. El primero de ellos se refiere a que, tal y como se ha mencionado, el Tratado de Lisboa elevaba la Carta de Derechos Fundamentales de la UE a derecho originario junto con los Tratados constitutivos; y, por tanto, también convierte en derecho originario el reconocimiento del derecho a la protección de datos personales a través del art. 8 del citado texto. En segundo lugar, el Tratado de Lisboa modificaba el antiguo art. 286 del TUE proporcionándole no solo una nueva redacción en el art. 16 del nuevo Tratado de Funcionamiento de la UE, sino también un nuevo alcance jurídico, pues, mediante dicho precepto se autoriza expresamente a la UE a regular el derecho a la protección de datos personales[193].

[192] Véase el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, que regula el derecho a la protección de datos personales como sigue:
«1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratar de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedar sujeto al control de una autoridad independiente».

[193] Véase el art. 16 de la Versión consolidada del Tratado de Funcionamiento de la Unión Europea, Boletín Oficial de la Unión Europea, C/326, de 26 de octubre de 2012.

> «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
> Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el art. 39 del Tratado de la Unión Europea».

En definitiva, el derecho a la protección de datos personales ha evolucionado desde la inicial labor interpretativa del TJCE hasta la consagración de una nueva base jurídica para regular expresamente el mismo a través de derecho derivado de la UE. Constituyen así el fundamento jurídico al fin de regular el derecho autónomo a la protección de datos personales, los arts. 6 del TUE, el art. 8 de la Carta de Derechos Fundamentales de la UE y el art. 16 del Tratado de Funcionamiento de la Unión Europea (en adelante TFUE)[194]. Pese a que, resulte loable la construcción de una base jurídica que legitime a la UE a regular derechos fundamentales, como el derecho a la protección de datos personales, se debe lamentar que dicha posibilidad no haya existido hasta el año 2009.

La propia historia de la constitución de la UE, cuyo trasfondo económico más que evidente ha marcado de manera definitiva la regulación del derecho de protección de datos personales, ha motivado que hasta la primera década del siglo XXI no se le haya permitido, jurídicamente, configurar un marco jurídico específico para la regulación de derechos fundamentales. Dicha falta de competencia, ha ocasionado que, durante décadas la evolución de la normativa de la UE que afectaba a derechos fundamentales, solamente haya avanzado desde los postulados del mercando interior. Sin duda, esta circunstancia resulta decisiva en el estudio que se presenta, puesto que, la normativa europea sobre protección de datos ha permanecido estática durante años ante un cambio tan vertiginoso como la irrupción de las TIC en el día a día de las personas. Huelga señalar que dicho inmovilismo, jurídicamente se traduce en posibles inseguridades jurídicas en la protección de la privacidad de las personas usuarias de dichas tecnologías, tal y como se pondrá de manifiesto.

[194] Véase RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político UNED*, 2012, núm. 85, p. 20 cuando afirma que «el Tratado de Lisboa otorgó fuerza jurídica vinculante a la CDFUE y, en concreto, al derecho autónomo a la protección de datos de carácter personal que consagra en su art. 8. Y —lo que resulta más relevante a los efectos del presente estudio— los arts. 6 TUE, 8 CDFUE y 16 TFUE han creado una *nueva base jurídica* que permite la elaboración de una normativa global de la Unión Europea relativa al tratamiento de los datos personales y a la libre circulación de estos datos y, además, con esta nueva base jurídica se autoriza a la Unión a regular específicamente la protección de datos, por medio de una Directiva, en los ámbitos de la cooperación policial y judicial en materia penal». En los mismos términos se manifiesta TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *op. cit.*, p. 6.

2.3. La Directiva 95/46/CE de protección de las personas frente al tratamiento de sus datos personales y de la libre circulación de estos datos. Un modelo normativo superado

Sentado cuanto antecede, el Parlamento Europeo aprueba la Directiva 95/46/CE, el 24 de octubre de 1995, con el fin de brindar una respuesta al fracaso en las expectativas que este había depositado en el Convenio 108 mencionado anteriormente, texto que debía firmarse por los Estados miembros con un plazo límite que concluía en 1982 sin que dicha firma tuviera lugar. Años antes, en 1974, el Parlamento Europeo presentó un estudio en la sesión celebrada el 21 de febrero de 1975 en la que se sentaron las bases para una posterior directiva. El cometido principal de dicho informe, se identificaba con unificar normativas bajo el temor de que, llegado el momento de armonizar las legislaciones estatales, la tarea resultara particularmente compleja debido a las regulaciones dispares existentes entre Estados miembros.

2.3.1. La Directiva 95/46/CE: una respuesta fallida a la necesidad de armonización legislativa en el seno de la UE

Si bien el impulso otorgado por el Parlamento Europeo a la aprobación de una directiva se mitigó en primera instancia por la promulgación del Convenio 108, la falta de ratificación del mismo por parte de la mayoría de los Estados, instigó al Parlamento Europeo a retomar el proyecto de adoptar una Directiva que sirviera de marco común a los Estados miembros en la regulación del derecho a la protección de datos personales. Tras dos propuestas de directiva, una de ellas en 1990 (en adelante, propuesta 1990) y la siguiente en 1992 (en adelante, propuesta 1992)[195], en el año 1995 se aprueba la Directiva 95/64/CE cuyo espíritu armonizador se proponía detener las disparidades que albergaban en las legislaciones nacionales respecto a la regulación del tratamiento de datos personales.

Si bien es cierto que, la Directiva 95/64/CE en su momento respondía a la acuciante necesidad de armonizar la materia, conviene recordar que, en 1995 la UE no se encontraba dotada de una base jurídica que le permitiera aprobar normas de derecho derivado relativas a la protección de datos personales en cuanto a su condición de derecho fundamental, motivo por el que recibió numerosas críticas por la doctrina, entre las que

[195] Consúltense las propuestas de Directiva de la Comisión: COM (90) 314-SYN 287 y 288, de 24 de septiembre de 1990 y COM (92) 422 final, DOC núm. 311, de 27 de noviembre de 1992.

destaca la de RUIZ MIGUEL[196]. A pesar de lo expuesto, el carácter de la Directiva 95/64/CE puede considerarse eminentemente económico, pues, tal y como indica el Considerando octavo, su finalidad principal reside en la eliminación de obstáculos que perjudiquen la libre circulación de datos personales en el mercado interior, ya que este garantiza la libre circulación de mercancías, personas, servicios y capitales, así como de los datos de carácter personal de un Estado a otro. Sin embargo, esta libre circulación se entorpece en la práctica debido a las diferencias jurídicas en la regulación que cada Estado miembro, por lo que, la armonización constituía una necesidad para las instituciones comunitarias.

En todo caso, de acuerdo con RALLO LOMBARTE, la Directiva 95/46/CE constituyó un hito en la historia de la protección de los datos personales de la UE[197]. Ello se debe, principalmente, al intento de tendencia unificadora en las legislaciones nacionales con el fin de garantizar la libre circulación de los datos personales; pero a su vez, sin olvidar la salvaguarda del derecho fundamental a la protección de datos personales. En efecto, la Directiva 95/46/CE al precisar de transposición por los Estados miembros, logró una efectividad mayor que la lograda con el Convenio 108, sin embargo, este proceso resultó prolongado y complicado. Véase que el primer informe sobre la aplicación de la Directiva 95/46/CE, de 15 de mayo de 2003 elaborado por la Comisión Europea[198], advertía de graves retrasos en la aplicación de esta en los Estados miembros, que entorpecían la libre circulación de los datos personales e imposibilitaban un adecuado nivel de protección de los mismos. Años más tarde, concretamente en 2007, este mismo organismo concluía que la aplicación de la directiva había mejorado considerablemente, pues todos los Estados miembros habían procedido a su transposición[199].

A pesar de destacar los aspectos positivos que la Directiva 95/64/CE supuso la UE, también se denunciaron múltiples deficiencias durante su vigencia, que condujeron a la elaboración del actualmente vigente Reglamento (UE) 2016/679 del Parlamento Europeo

[196] RUIZ MIGUEL, C., "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", *RDCE*, 2003, núm. 14, p. 18.
[197] RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *op. cit.*, p. 17.
[198] Informe de la Comisión Europea, de 15 de mayo de 2003, relativo al primer informe sobre la aplicación de la Directiva sobre protección de datos 95/46, COM (2003) 265 final.
[199] Informe de la Comisión Europea, de 7 de marzo de 2007 sobre el Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, COM (2007) 87 final.

y del Consejo, aprobado el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[200] (en adelante, RGPD) responsable de armonizar la normativa referente a la protección de datos personales. Entre dichas deficiencias, destacan las expuestas por TRONCOSO REIGADA, pues todas ellas incidieron en mayor medida en que la UE se decantara por la construcción de una normativa de alcance general y obligatorio como la que proporciona el Reglamento Europeo.

En primer lugar, el motivo principal de la necesidad de una mayor armonización reside en las divergencias sobre protección de datos existentes en las normativas de los Estados miembros. Dichas disparidades provienen tanto de una inadecuada transposición de la Directiva 95/46/CE, como de la incorrecta interpretación de la normativa de protección de datos nacional en cada uno de los Estados de la UE. Las mencionadas divergencias se agravaron, desde luego, por la existencia de cláusulas abiertas en la propia Directiva 95/64/CE, que permitían una transposición diferente de la misma en los distintos Estados. Cierto es que las disparidades normativas pueden derivar del resultado de la propia naturaleza de la Directiva, que no facilita una completa unificación de materias, sino la aproximación de las mismas; pero en el presente caso, los Estados miembros se excedieron considerablemente en la apreciación de dichas cláusulas abiertas, no respetando el margen que la Directiva 95/64/CE concede en estos extremos y rebasando los límites concedidos por esta[201].

En efecto, el segundo motivo que impulsó la unificación en la materia y directamente relacionado con el anterior, se encuentra en la extralimitación de los Estados en el margen de apreciación concedido por la Directiva 95/64/CE en la regulación del tratamiento de datos personales. En ese sentido, la Comisión Europea denuncia varios incumplimientos de la Directiva 95/46/CE, entre los que destaca, la denuncia que interpuso ante el TJCE a las legislaciones de Francia, Alemania, Irlanda, Luxemburgo y Países Bajos con motivo del incumplimiento de la Directiva 95/64/CE protagonizado por dichos Estados[202].

[200] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, aprobado el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Diario Oficial de la Unión Europea, L 119/1, de 4 de mayo de 2016.
[201] TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *op. cit.*, p. 29.
[202] Informe de la Comisión Europea, de 15 de mayo de 2003, relativo al primer informe sobre la aplicación

Por último, otras divergencias provenían de la disparidad en la interpretación y aplicación de la normativa de protección de datos que realizaban cada uno de los Estados a través de sus órganos y autoridades de control. Sin embargo, sobre la labor de cooperación en la aplicación homogénea de la Directiva 95/64/CE cabe destacar el papel del Grupo de Trabajo regulado en el art. 29 de la Directiva 95/46/CE. Dicho órgano, conformado por participantes de las autoridades de protección de datos de los Estados miembros, ha propiciado una cooperación más estrecha que ha procurado paliar las divergencias legislativas de los Estados miembros[203].

A mayor abundamiento, tal y como se ha mencionado hace escasas líneas, la Directiva 95/46/CE carecía de fundamento jurídico directo en la adopción de normas de derecho derivado cuyo objeto se identifique con la regulación del derecho fundamental a la protección de datos personales, pues dicha posibilidad no devino posible hasta 2009 mediante la adopción del Tratado de Lisboa. Así, la Directiva 95/64/CE sobre protección de datos personales se sustentaba sobre la base de la libertad de mercado interior y no tanto en la garantía del derecho fundamental de protección de datos personales.

Con todo, tras el intento fallido en la armonización de la normativa sobre protección de datos personales en el seno de la UE por medio de la Directiva 95/46/CE, la UE comenzó la construcción de un marco homogéneo de protección de datos personales, abogando por la constitución de una normativa coherente entre los Estados miembro, cuya materialización se encauzaría por medio de la aprobación de un Reglamento Europeo de alcance general y directo.

2.3.2. La protección de datos personales de los menores: el silencio de la Directiva 95/46/CE

En otro orden de consideraciones, cabe destacar la falta de mención de la Directiva 95/46/CE sobre la protección de datos personales de los menores. Efectivamente, dicho cuerpo normativo omite cualquier mención a la minoría de edad en su articulado, no apreciando la necesidad de proporcionar una atención especial a estos. Ciertamente, durante más de 20 años de vigencia de la Directiva 95/46/CE, el consentimiento prestado

de la Directiva sobre protección de datos 95/46, COM (2003) 265 final, p.3.

[203] El Grupo de Trabajo del Artículo 29 de la Unión Europea se trata de un consejo asesor de carácter independiente cuya especialidad radica en la protección de datos y la privacidad. El mismo se crea por el mandato de la Directiva 95/46 CE.

por los menores de edad en lo que al tratamiento de sus datos personales se refiere, se ha regulado por las normas generales sobre capacidad de los respectivos Estado miembro.

No obstante, a medida que los años transcurrían, la UE toma conciencia paulatina sobre la rápida evolución de las TIC y su gran influencia sobre los menores de edad como principales usuarios de las mismas. En ese contexto, el Grupo de Trabajo del Artículo 29 publicaba el 11 de febrero de 2009, el Dictamen 2/2009 sobre la protección de datos personales de los niños[204]. Dicho dictamen, se sitúa en el contexto de la iniciativa impulsada por la Comisión Europea descrito en la Comunicación Hacia una Estrategia de la Unión Europea sobre los derechos de la Infancia. Así, el dictamen procura la protección de la información sobre los niños, para lo que emprende el refuerzo del derecho fundamental de los niños a la protección de datos personales.

El dictamen elaborado por el Grupo de Trabajo del artículo 29 denuncia que, la Directiva 95/46/CE no menciona expresamente los derechos de los menores a la intimidad, ni se toma en consideración las particularidades de la vida de los niños en su articulado. Esta circunstancia no ha pasado inadvertida para la doctrina; y por ello, GÓMEZ-JUÁREZ SIDERA advierte de la preocupante relajación por parte de la UE en una cuestión tan delicada como la que atañe a la protección de datos personales de los menores de edad[205]. En efecto, no podemos sino mostrarnos de acuerdo con dicha aseveración, dado que, el propio desarrollo normativo en la materia ha demostrado cómo la UE ha postergado la adecuación de la normativa sobre protección de datos personales a la salvaguarda de datos personales de los menores de edad como personas especialmente vulnerables.

El objetivo del Dictamen emitido por el Grupo de Trabajo del Artículo 29 se centra en analizar los principios generales que deberán aplicarse a la protección de los datos personales de los niños. Ciertamente, el informe se centra en el interés superior del menor que, en todo caso, deberá valorarse y anteponerse para garantizar su protección también en el ámbito de la protección de su intimidad. Además, el Dictamen considera la especial situación en la que se encuentran los menores respecto a su nivel de desarrollo tanto físico como psicológico y cómo dichas cuestiones deben considerarse también en el ejercicio

[204] Dictamen 2/2009 del Grupo Protección de datos del Artículo 29 sobre la protección de datos personales de los niños (Directrices generales y especial referencia a las escuelas), de 11 de febrero de 2009, WP 160.
[205] Véase al respecto GÓMEZ-JUÁREZ SIDERA, I., "Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la Legislación Española", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2006, núm. 11, 2ª parte, p. 2

del derecho a la protección de datos personales del que son titulares. En efecto, la protección de datos personales de los niños debe tomar en consideración dos aspectos fundamentales: el primero, el grado de madurez progresivo de los menores, que establecerá el momento a partir del cual podrán tomar el control sobre sus propios datos; el segundo, en qué medida los representantes legales del menor gozarán del derecho a inmiscuirse en la divulgación de datos personales del menor, especialmente si la misma puede resultar perjudicial para su interés superior.

Para la adaptación de la Directiva 95/64/CE a dichas consideraciones, el Dictamen se decanta por la vía de la interpretación de los principios regulados en la Directiva 95/64/CE, acomodándolos a la minoría de edad. Así, el Grupo de Trabajo del artículo 29 adapta las particularidades de la minoría de edad a los siguientes principios: por un lado, los principios relacionados con la calidad de los datos como los principios de equidad, proporcionalidad, pertinencia y conservación de los datos; y por otro lado, el principio de licitud, seguridad, así como los derechos de Acceso, Rectificación, Supresión o bloqueo y Oposición (también conocidos como derechos ARCO). Desde luego, cabe destacar la especial atención con la que el Dictamen trata la particular situación de tránsito hacia la madurez en la que se encuentran los más jóvenes y cómo ello influye en los derechos mencionados anteriormente.

Finalmente, el Dictamen aborda el consentimiento al tratamiento de datos personales prestado por menores. Sin perjuicio de que se volverá sobre esta cuestión, el documento apuesta por la línea marcada por los organismos internacionales como la ONU, a través de la Convención de los Derechos del niño de 1989, en lo que a la capacidad del menor respecto a sus derechos fundamentales se refiere. El Grupo del Artículo 29, aboga por priorizar la madurez que el menor pueda demostrar a la hora de determinar la posibilidad de prestar consentimiento por sí mismo y no a través de sus representantes legales. Por el contrario, en caso de que el menor de edad no alcance madurez suficiente, los representantes legales, en interés superior del mismo, deberán valorar la pertinencia sobre la prestación del consentimiento al tratamiento de datos personales del menor en cuestión. Antes bien, a pesar de lo expuesto, el Dictamen reconoce a cada Estado regular las condiciones de validez de consentimiento prestado por menores de edad de manera acorde a su propia normativa sobre capacidad.

Así, debe destacarse que, aunque de forma tardía, la UE toma en consideración la especial situación de vulnerabilidad en la que se sitúa la privacidad de los menores de edad, así como del vacío legal que sufre la normativa cuya protección pretende[206]. Durante más de dos décadas de vigencia de la Directiva 95/64/CE, si bien la UE ha procurado interpretar la normativa sobre protección de datos personales a la minoría de edad, no ha existido un marco normativo sólido cuyo fin residiera en la salvaguarda del derecho a la protección de datos personales de estos.

Además, la propia Directiva 95/46/CE terminó por quedar obsoleta ante los nuevos escenarios que las TIC traen consigo y que se presentan a modo de posibles injerencias e intromisiones ilegítimas más sofisticadas en la vida privada de las personas y en el tratamiento de sus datos personales, sobre todo si son menores de edad. En efecto, durante la tramitación de la Directiva 95/64/CE, cuyo comienzo podemos situar en el año 1990 aproximadamente, en sintonía con lo expuesto por MINERO ALEJANDRE, el legislador europeo no alcanzaba a imaginar el reto que supondría la irrupción de Internet en el día a día de las personas[207], ocasionando que la Directiva no fuera capaz de adaptarse al nuevo escenario digital.

2.3.3. La obsolescencia de la Directiva 95/46/CE ante el avance de la sociedad de la información y su incidencia sobre la protección de los datos de menores de edad

En directa relación con la circunstancia descrita sobre la manifiesta obsolescencia de la Directiva 95/46/CE ante el avance de las TIC, merece especial mención la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Un enfoque global de la protección de datos personales en la Unión Europea", de 4 de noviembre de 2010[208], en la que la

[206] Esa preocupación por la protección los más jóvenes como personas vulnerables frente a las TIC se ha puesto de manifiesto por la UE en años posteriores a 2009 a través de textos como la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre "Una agenda de la UE en Pro de los derechos del Niño, de 15 de febrero de 2011 citada anteriormente, que como cita textualmente: «La Comisión pretende alcanzar un alto nivel de protección de los niños en el ciberespacio que abarque sus datos personales, protegiendo al mismo tiempo su derecho de acceso a Internet en aras de su desarrollo social y cultural. Mediante el programa "Una Internet más Segura", la Comisión coordina y apoya las labores destinadas a capacitar a los niños y dispensarles protección en sus actividades en línea».

[207] MINERO ALEJANDRE, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario jurídico y Escurialense,* 2017, núm. 50, p. 22.

[208] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Un enfoque global de la protección de datos personales en la Unión Europea", de 4 de noviembre de 2010, COM (2010) 609 final.

Comisión, repara en la gran modificación que han supuesto la rapidez de la evolución tecnológica y la globalización, propiciando la aparición de nuevos retos en materia de protección de datos personales. Ejemplo de dicho vertiginoso cambio constituyen la aparición de las redes sociales, donde la información personal circula continuamente a tiempo real, la computación en la nube donde los usuarios almacenan información personal en un servidor remoto, o, en definitiva, el *big data*, empleo de algoritmos y elaboración de perfiles a partir de la información personal que las personas usuarias comparten en Internet y redes sociales. Con motivo de la nueva realidad descrita, la Comisión manifiesta el deseo de emprender la modernización del régimen jurídico de la UE para la protección de los datos personales.

Recordemos que la rapidez e inmediatez con la que la información se genera y comparte en el entorno *online*, acentúa la posibilidad de convertir en pública información a nivel mundial en cuestión de segundos. A dicha circunstancia debemos añadir que las empresas privadas y autoridades públicas utilizan datos personales a una escala sin precedentes. En ese sentido, actuaciones tan cotidianas como abrir una cuenta bancaria *online*, darse de alta en una red social, reservar un vuelo *online*, recibir una receta médica electrónica se identifican como situaciones en las que los datos proporcionados a dichos prestadores de servicios resultan personales.

Además, el consentimiento prestado para el tratamiento de dicha información personal, no siempre viene acompañado del conocimiento sobre el destino y tratamiento que dichas empresas o autoridades realizarán con dicha información, circunstancia que, desde luego puede afectar gravemente a la privacidad de las personas a falta de una regulación específica. En consonancia con lo expuesto, la encuesta realizada por el Eurobarómetro en el año 2011, reflejaba que el 72% de los usuarios de Internet de la Unión Europea, mostraban su preocupación ante la ingente cantidad de datos personales que se solicitan en línea, además de apuntar que, tenían la sensación de haber perdido el control sobre sus datos personales al no recibir información adecuada sobre su destino, transmisión y fines para los que se emplean[209].

[209] Euro barómetro especial número 359, Actitudes hacia la protección de datos y la identidad electrónica en la Unión Europea, de junio de 2011. Obtenido de: https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=es (última consulta el 20 de noviembre de 2022), p. 23.

Así las cosas, la Comisión advierte e intenta concienciar sobre la incidencia de las TIC en la salvaguarda del derecho a la protección de datos personales, cuestionándose si la legislación de la UE, vigente en aquel entonces en materia de protección de datos, se mostraba capaz de enfrentarse de manera eficaz a dichos retos. A lo que debemos añadir que dicho cuestionamiento por parte de la Comisión, debe resultar aún mayor en el caso de los menores de edad, pues estos jóvenes se exponen a sofisticadas vulneraciones sobre su información personal cuando manejan las TIC sin que, en la mayoría de los casos, tomen plena conciencia de los riesgos. Véase que los menores de edad suelen navegar por la red de manera despreocupada, facilitando datos personales tanto propios, como del entorno familiar y amistades, sin advertir de manera consciente quién recibirá dicha información y cómo empleará esta e incluso, en ocasiones, proporcionando acceso de forma inconsciente a su información personal[210]. Además, como veremos en apartados posteriores, las particulares circunstancias de los menores de edad no se positivizan en una norma hasta la publicación del ya citado RGPD, relegando a los menores de edad a una situación de indefensión más que evidente respecto a su privacidad durante varios años.

Sirvan como ejemplo de dicha inseguridad jurídica las situaciones que se exponen como sigue. Durante la vigencia de la Directiva 95/46/CE, valorar la madurez de los menores de edad con el fin de dotar de validez el consentimiento prestado *online* para el tratamiento de sus datos personales, tal y como sugiere el Dictamen 2/2009, se presentaba como una tarea de suma dificultad que generaba inseguridad jurídica por constituirse como un concepto muy flexible en orden a valorar la validez del consentimiento. En ese sentido, la falta de contacto personal con los menores que desean consentir el tratamiento de datos personales para iniciar su actividad en una red social, se considera como uno de los escollos principales con los que dicha interpretación de la validez del consentimiento podía encontrarse en la práctica, y que la normativa no dotaba de solución suficiente y satisfactoria.

Asimismo, la falta de madurez de los menores de edad predispone que estos no entiendan las dificultosas políticas de privacidad en las que se expone información tan crucial como quién recogerá y tratará sus datos personales, la manera en que dicho tratamiento deberá acometerse, los motivos, duración y, en definitiva, los derechos de los

[210] El comportamiento descrito puede materializarse por medio de la instalación de una *cookie* que recabará los hábitos de uso del dispositivo por parte del usuario.

que dispondrán en dicho contexto. Por ello, la UE aboga por un acceso sencillo a la información, que debe revestir facilidad de entendimiento mediante el empleo de un lenguaje claro y sencillo. Es más, en el caso de que los usuarios sean menores de edad, dicho lenguaje debe revestir mayor claridad, pues estos pueden resultar menos conscientes de los riesgos derivados del consentimiento del tratamiento de datos personales, además de que su capacidad de entendimiento de las políticas de privacidad puede resultar menor, dada su situación de tránsito hacia la plena madurez. Sobre este particular volveremos más adelante.

Con carácter posterior a la Directiva 95/46/CE, la UE procedió a la aprobación de la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[211], que prevé una remisión expresa a la Directiva 95/46/CE en lo referente a la protección de datos personales; en consecuencia, tampoco menciona a los menores de edad en su articulado. Según se ha podido advertir, sus modificaciones posteriores tampoco prevén la inclusión de la minoría de edad en su articulado cuando los menores pretenden contratar servicios de telecomunicaciones, entre otros.

En virtud de lo expuesto, ha quedado de manifiesto que los menores de edad se encuentran en una posición de indefensión al no existir un control real y efectivo por parte del ordenamiento jurídico europeo que proteja la privacidad de personas especialmente vulnerables. A lo que se debe añadir que este desamparo adquiere mayor entidad cuando estos jóvenes emplean las TIC, pues en esos casos, se enfrentaban a una doble indefensión: la obsolescencia de la Directiva 95/46/CE en relación a las TIC y la ausencia de regulación en la misma de las particularidades que la minoría de edad presenta en relación al derecho de protección de datos personales (como usuarios de las TIC o no). Desde luego que la elaboración de determinados informes y dictámenes que carecen de vinculación jurídica, no constituían garantía suficiente en la protección de los derechos

[211] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, Diario Oficial de la Unión Europea, L 24/1, de 30 de enero de 1998 derogada por la Directiva 2002/58/CE del Parlamento Europeo y del consejo de 12 de julio de 2012, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, Diario Oficial de la Unión Europea, L 201, de 31 de julio de 2002; y finalmente, la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, relativa al servicio universal que modificó varias directivas del sector de las telecomunicaciones, Diario Oficial de la Unión Europea, L 337, de 18 de diciembre de 2009.

fundamentales de los más jóvenes. Es más, en el entorno *online*, tal y como se ha puntualizado recientemente, la solución aportada por el Dictamen 2/2009, de 11 de febrero del Grupo de Trabajo del artículo 29, carece de aplicabilidad para el consentimiento que se presta en línea.

Asimismo, la verdadera irrupción de las TIC podemos situarla aproximadamente en los primeros compases del siglo presente, cuando la UE ya se encontraba dotada de competencia para regular el derecho a la protección de datos personales. Sin embargo, dicha regulación que incorpora los menores de edad en su articulado no se aprueba hasta el año 2016 y su aplicación de manera efectiva hasta 2018, de modo que, no podemos calificar dicho olvido sino de una verdadera falta de previsión con la seguridad de los datos personales de los menores de edad en un entorno especialmente presente en su vida cotidiana y que trae consigo verdaderos riesgos.

2.4 Hacia un marco normativo europeo homogéneo de protección de datos personales: el Reglamento 2016/679

Tras 21 años de vigencia de la Directiva 95/46/CE, el 25 de mayo de 2016 entra en vigor el Reglamento General de Protección de Datos Personales citado anteriormente en el presente estudio. Pese a ello, la aplicación efectiva del mismo no acontece hasta mayo de 2018, pues los Estados miembros disponían de dicho lapso de tiempo con el fin de adaptarse los nuevos postulados del Reglamento.

El deseo de proporcionar una nueva regulación al tratamiento de datos personales en la UE nace en 2012, cuando la Comisión Europea propone reformar la legislación vigente a través de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) de 25 de enero de 2012[212]. Por medio de dicha propuesta, la Comisión Europea reconocía que, a pesar de que los objetivos y principios contenidos en la Directiva 95/64/CE continuaban gozando de validez, la fragmentación de normativas más que palpable en el contexto europeo, desembocaba en la aparición de riesgos e inseguridad

[212] Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 25 de enero de 2012, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), Comunicación (COM) 2012 11 final.

jurídica, particularmente en el entorno *online*[213]. Así, ante los múltiples retos que la evolución de la tecnología suponía para la normativa vigente, la UE proponía generar confianza en el entorno en línea, respetando la salvaguarda y protección de los datos personales desde un marco legal coherente y homogéneo que resistiera al transcurso del tiempo.

Tal y como se pone de relieve en el Considerando 9 del RGPD, la normativa sobre protección de datos personales se hallaba fragmentada en el seno de la UE, por lo que constituye objetivo de este nuevo texto normativo garantizar un nivel elevado y uniforme y equivalente en cada uno de los Estados que conforman la Unión. No en vano, recordemos que el Reglamento, como tipología de norma, regulado en el art. 288 TFUE, goza de aplicabilidad directa, esto es, no requiere de transposición a la normativa nacional, poseyendo alcance general y obligatoriedad en todos sus elementos en los Estados miembros[214]. Con total certeza, las mentadas características inspiraron al legislador en la elección de dicha técnica normativa con el fin de construir el marco sólido y coherente del que no ha gozado durante años el tratamiento de datos personales en el seno de la UE. Nótese que la innecesariedad de transposición por parte de los Estados del contenido del Reglamento, elimina los riesgos de adaptar las normativas nacionales de modo no armonizado, como terminó aconteciendo con la Directiva 95/46/CE. No obstante, sus expectativas se han visto frustradas en determinados aspectos, pues el RGPD permite determinado margen a las legislaciones nacionales a efectos de adecuar su contenido en determinadas materias.

Aunque la aprobación de una normativa a través de un Reglamento europeo constituya un avance significativo en la homogeneización de la normativa europea sobre protección de datos personales, circunstancia solicitada tanto por la Comisión Europea como por el Supervisor Europeo de protección de datos en el Resumen elaborado por este último[215], el RGPD no se ha encontrado libre de críticas en lo que al logro de dicha

[213] Recordemos que la protección de datos personales en el entorno *online* se regula no solo a través del RGPD sino también a través de la Directiva 2009/136/CE, de 25 de noviembre del Parlamento Europeo y del Consejo de 25 de noviembre, relativa al servicio universal que modificó varias directivas del sector de las telecomunicaciones.

[214] MANGAS MARTÍN, A., y LIÑÁN NOGUERAS, D., *Instituciones y Derecho de la Unión Europea*, Madrid, Tecnos, 2011. pp. 348-349.

[215] Resumen de conclusiones del dictamen del Supervisor Europeo de Protección de Datos sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital, Diario Oficial de la Unión Europea, C 463/08, 13 de diciembre de 2016. Obtenido de:

uniformidad se refiere. Ciertamente, el RGPD continúa concediendo un amplio margen de apreciación a los Estados miembros que, a nuestro juicio, puede contribuir a no lograr un nivel de homogeneidad y coherencia suficientes en diversas materias como, por ejemplo, la relativa a los datos de salud, genéticos o biométricos[216], o incluso el establecimiento de la edad mínima comprendida entre los 13 y 16 años para prestar válidamente consentimiento al tratamiento de datos personales por menores de edad[217]. En definitiva, es cierto que, tal y como advierte GARCÍA MEXÍA, nos encontramos ante un Reglamento que difiere del resto, pues permite la interpretación en materias que cabe intuir que plantearán problemas[218]. En efecto, tras varios años de su entrada en vigor, se ha podido constatar que varios aspectos que permiten interpretaciones han generado fricciones, tal y como quedará de manifiesto.

Por otra parte, el RGPD constituye el primer cuerpo normativo aprobado desde la instauración de la nueva base jurídica del derecho a la protección de datos personales (art. 8 CDFUE y art. 16 TFUE). Así, la norma pone de manifiesto que la protección de las personas físicas en relación con el tratamiento de datos personales se configura como un derecho fundamental, que los principios y normas relativos a la protección de la misma deberán respetar en todo momento. Queda en evidencia así el alejamiento del RGPD del marcado carácter económico que la Directiva 95/46/CE. A pesar de ello, el RGPD no abandona por completo la marcada visión socioeconómica, en el sentido que, efectivamente la circulación de datos personales resulta indispensable en dicho contexto para un mayor crecimiento de la UE. Ahora bien, el abandono del carácter económico recientemente mencionado, propicia que dichos tratamientos de datos, garanticen el control de la información personal de los residentes en la UE desde la perspectiva de la

https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_es.pdf (última consulta, 6 de julio de 2020)

[216] En ese sentido, ÁLVAREZ-RIGAUDIAS critica que el RGPD permite a los Estados la potestad de incluir condiciones adicionales en relación con los datos biométricos, genéticos o de salud, circunstancia que puede incidir negativamente en la normativa pues predispone continuar una senda de fragmentación. Y es que, a nuestro juicio, esos márgenes de apreciación son los que bajo la vigencia de la Directiva 95/46/CE han contribuido en gran medida a la fragmentación de la normativa. Véase al respecto ÁLVAREZ-RIGAUDIAS, C., "Tratamiento de Datos de Salud", en PIÑAR MAÑAS, J.L., (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad,* Madrid, Reus, 2016, p. 178.

[217] Véase al respecto BENEDITO CAÑIZARES, M.T., "La autorregulación en el Reglamento General de Protección de Datos como solución frente al mercado digital fragmentado: el menor y los Registros", *op. cit.*, p. 3125.

[218] GARCÍA MEXÍA, P., "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos" en PIÑAR MAÑAS, J.L., (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad,* Madrid, Reus, 2016. pp. 31-33.

regulación del derecho fundamental a la protección de datos personales, en lugar de centrarse en la libertad de circulación de los datos personales como se regulaba hasta la fecha. Sin duda, esta última circunstancia no ha contentado a varias de las empresas prestadoras de Servicios de la Sociedad de la Información, pues han señalado el riesgo de que una normativa tan estricta como la contenida en el RGPD pueda suponer un inconveniente en el desarrollo de muchos negocios internacionales para los cuales el tratamiento de datos personales deviene indispensable[219].

Tomamos conciencia de que se constituye como una tarea de suma dificultad conjugar la circulación de datos personales con la defensa de los derechos y la privacidad de las personas. Sin embargo, el RGPD se constituye como un ambicioso marco normativo que desea encontrar el equilibrio entre dichas realidades, procurando articular un mecanismo efectivo a la par de garantista con la libre circulación de datos personales, pero siempre que la misma asegure la protección del derecho fundamental de protección de datos personales (Considerando 10 RGPD).

2.4.1. Las claves de un nuevo sistema normativo de protección de datos personales adaptado al actual contexto digital

La normativa de protección de datos personales en la UE acusaba carácter convencional en la salvaguarda de dicho derecho fundamental. En efecto, la Directiva 95/46/CE se mostraba incapaz de aportar una respuesta a la pluralidad de retos que las TIC plantean en la garantía de la privacidad de las personas y más específicamente, del derecho a la protección de datos personales. Con el fin de superar dicho vacío normativo, el RGPD adapta la normativa europea a la nueva era digital, circunstancia que se manifiesta expresamente en el Considerando 6, que reconoce que la evolución tecnológica y la globalización han conllevado la aparición de nuevos retos para la protección de datos personales.

Aun así, el riesgo para los derechos de las personas no reside de manera exclusiva en la capacidad que la tecnología posee para recabar una cantidad sumamente ingente de información personal que circula a través de un flujo diario de información tecnológica y digital que no conoce barreras de espacio y tiempo, sino en la desarrolladísima capacidad

[219] CRISTEA UIVARU, L., *La protección de datos de carácter sensible: historia clínica digital y Big Data en salud*, Barcelona, Boch Editor, 2018, p. 236.

de análisis y conectividad de las TIC con el fin de que esta arroje informaciones más precisas y consecuentemente, más sensibles.

Las empresas privadas e incluso autoridades públicas utilizan nuestros datos personales y en muchas ocasiones sensibles, a una escala sin precedentes; es más, nunca en la historia se había presentado la posibilidad de tratar volúmenes tan elevados de datos personales de manera inmediata. Como consecuencia de ello, las probabilidades de sufrir una intromisión en la vida privada nunca había resultado tan posible como en el presente, por lo que la UE, consciente de esta situación, advierte que la falta de regulación específica podía conllevar tratamientos de datos personales no consentidos por los titulares de los mismos[220]. Por todo ello, la UE se propone facilitar a las personas más instrumentos para el control sobre su información personal.

En este orden de cosas, destacamos varias de las alusiones que el RGPD realiza al nuevo contexto digital, tratando de incluir en su normativa fenómenos típicamente característicos un siglo XXI globalizado y dependiente del entorno *online*[221]. En definitiva, tras un largo período de reflexión liderado por la Comisión Europea, pluralidad de situaciones especialmente intrusivas en la privacidad de los ciudadanos, especialmente en el contexto *online*, acceden a un texto jurídicamente vinculante. De esta suerte, la necesaria adaptación del RGPD al nuevo contexto digital implicó superar la perspectiva tradicional de los principios y derechos de protección de datos personales. Así, a los tradicionales derechos ARCO, se les unen una variedad de derechos y garantías adaptados al contexto tecnológico del siglo XXI[222]. Sobre su estudio riguroso, volveremos más adelante.

Sin embargo, cabe señalar que la mayor innovación que proporciona el RGPD en relación a los principios del tratamiento vinculantes para los responsables del tratamiento la constituyen dos principios de carácter general, que habrán de proyectarse sobre la

[220] *Ibid*, p. 227.
[221] Sirvan como ejemplo los siguientes, a saber: el Considerando 18, menciona de manera específica las redes sociales cuando se refiere a la exclusión del RGPD en las actividades de índole exclusivamente personal o doméstica; el Considerando 30 toma conciencia de las *cookies* y elaboración de perfiles; el Considerando 32 relativo al consentimiento, incluye por vez primera una mención al consentimiento al tratamiento de datos otorgado por medios electrónicos, especificando que el mismo puede otorgarse marcando una casilla web diferenciada; el derecho de supresión o al olvido mencionado en el Considerando 65 adapta la supresión de dichos datos en Internet; el Considerando 71 conciencia sobre la elaboración de perfiles a raíz de la información que permanece en la red, etc.
[222] HERRÁN ORTÍZ, A.I., "Aproximación al derecho a la protección de datos personales en Europa. El Reglamento General de Protección de Datos personales a debate", *Revista de Derecho, Empresa y Sociedad*, 2016, núm.8, p. 186.

totalidad de las obligaciones a las que las organizaciones que tratan datos personales habrán de someterse según dispone DOPAZO FRAGUÍO[223]. Nos referimos, así, al principio de responsabilidad proactiva y al enfoque desde el riesgo.

El primero de los elementos, alude a la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, con el fin de garantizar y poder demostrar que el tratamiento que llevan se muestra acorde al RGPD. En la práctica, este principio invita a las organizaciones a que analicen cuidadosamente qué datos tratan, con qué finalidades y qué tipo de operaciones de tratamiento llevan a cabo. Una vez que dicho análisis se ha realizado, deben determinar la forma en la que aplicarán las medidas previstas en el RGPD. A modo de síntesis, este principio plantea la adopción de una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que realicen[224]. Siguiendo la idea expuesta por PIÑAR MAÑAS, el nuevo modelo propuesto por el RGPD aboga por la adopción por parte de los responsables del tratamiento de una actitud de cumplimiento y responsabilidad en orden a dejar atrás la actitud sancionadora del modelo de protección de datos anterior bajo la vigencia de la Directiva 95/46/CE[225]. Ciertamente, el cambio de cultura en el tratamiento auspiciado por el RGPD se alinea con la rápida evolución de las TIC, en el sentido que, de implementarse una cultura responsablemente activa por los responsables del tratamiento, el avance de los tratamientos de datos, podría ocurrir de tal modo que no se precisase con excesiva frecuencia un modelo reactivo que castigara los mismos.

El segundo elemento, esto es, el enfoque desde riesgo, plantea que algunas de las medidas que el RGPD establece se aplicarán cuando se advierta un alto riesgo para los

[223] DOPAZO FRAGUÍO, P., "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento General de Protección de Datos)", *Revista Española de Derecho Europeo*, 2018, núm. 68, pp. 7-8.

[224] Tal y como señala la AEPD, no incumplir la normativa sobre protección de datos personales ya no se reputará suficiente. Sino que, los responsables del tratamiento deberán mostrar capacidad de acreditar que cumplen con la normativa sobre protección de datos personales. Guía de las AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; AGENCIA CATALANA DE PROTECCIÓN DE DATOS; AGENCIA VASCA DE PROTECCIÓN DE DATOS sobre el Reglamento Europeo de Protección de datos para responsables del tratamiento, 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf (última consulta el 9 de marzo de 2022), p.3.

[225] PIÑAR MAÑAS, J.L., "Hacia un nuevo modelo europeo de protección de datos", en PIÑAR MAÑAS, J.L., (Coordinador), *Reglamento Europeo de Protección de datos: hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, 2016, p. 21.

derechos y libertades, mientras que otras, deberán graduarse en función del nivel y tipo de riesgo que los tratamientos presenten. En esencia, consiste en que la aplicación de las medidas del RGPD se acomoden y adapten a las características y procesos de las organizaciones.

Sin embargo, a pesar de que el RGPD aporte más novedades[226], deseamos destacar por encontrarse en directa relación con el presente estudio, las siguientes obligaciones en las que algunos de los principios señalados cobran relevancia en relación a la protección del menor: el principio de transparencia en el tratamiento de datos personales (arts. 5 y 12 RGPD), el principio del consentimiento (art.7 RGPD) y el principio de privacidad desde el diseño y por defecto (art. 25 RGPD). En cuanto a los dos primeros principios, sin ánimo de profundizar ahora pues, se dedica un estudio pormenorizado en los mismos en el capítulo tercero de la presente investigación, el RGPD procura el refuerzo de estos en el contexto *online*, estableciendo nuevas obligaciones a los responsables del tratamiento sobre dichos extremos.

A nuestro juicio, el principio de transparencia (art. 12 RGPD), adquiere especial relevancia en el contexto *online*, donde la comprensión de las políticas de privacidad se presenta como una tarea sumamente compleja, pues estas habitúan a no revestir claridad. Por ello, el evidente esfuerzo que el RGPD realiza merece una valoración positiva y abría la esperanza a que este principio de transparencia forzase a los responsables de tratamientos que ofertan servicios de la sociedad de la información a presentar con claridad sus políticas de privacidad, cuestión que deberán llevar a cabo con más cuidado en el caso de menores, ya que estos, como sus principales usuarios, deben comprender las vicisitudes de tratamiento de datos que estas empresas llevarán a cabo con su

[226] En concreto, destacan las novedades sobre las siguientes materias que el RGPD incorpora: la extensión de su ámbito de aplicación tal y como ha sido expuesto; añade nuevos principios que habrán de presidir los tratamientos de datos personales; incorpora nuevas categorías especiales de datos (art. 9 RGPD); incluye novedades en torno al consentimiento del interesado; por primera vez, regula los requisitos que deberá cumplir el consentimiento prestado por menores de edad; así mismo, regula diversos aspectos novedosos respecto al derecho de información o deber de informar de los responsables de datos personales, concretamente clarifica cómo deberá prestarse dicha información; incorpora nuevos derechos a disposición de las personas interesadas en orden a garantizar el control sobre sus datos personales como el derecho a la portabilidad, el derecho a la supresión o el derecho a la limitación del tratamiento; introduce los conceptos de protección de datos desde el diseño y protección de datos por defecto, así como la figura del Delegado de Protección de datos; incorpora algunas novedades a considerar en el modelo de transferencias internacionales; por último, a diferencia de la normativa anterior, el RGPD no aporta un listado de medidas de seguridad, sino que dispone que deberá procederse a realizar una evaluación de los riesgos asociados a cada tratamiento para determinar las medidas de seguridad a implementar. En ese sentido, AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS. Principales novedades del RGPD. Obtenido de: https://apdcat.gencat.cat/es/documentacio/RGPD/novetats/ (última consulta el 12 de mayo de 2021).

información personal. Tal y como dispone el Grupo de Trabajo 29, los responsables del tratamiento deben detallar por separado y en un lenguaje sin ambigüedades cuáles constituirán las consecuencias más importantes del tratamiento, esto es, qué clase de repercusiones posee realmente para el interesado el tratamiento específico descrito en la política de privacidad[227].

Por otra parte, el principio del consentimiento específico otorgado para cada una de las finalidades del tratamiento (art. 7 RGPD), por su parte, presenta nuevas condiciones de validez. Este ha de tratarse de un consentimiento libre, específico, informado e inequívoco de que el interesado acepta, mediante una declaración o una clara acción afirmativa, de que consiente el tratamiento de datos personales que le conciernen. Cabe destacar que, el consentimiento tácito permitido bajo la vigencia de la Directiva 95/46/CE desaparece con la entrada en vigor del RGPD. Ahora bien, el RGPD, también añade que la solicitud del consentimiento se lleve a cabo de manera diferenciada a otros aspectos y que este no se supedite a la consecución de un contrato o servicio. Es más, el Considerando 32 reconoce la posibilidad de que el consentimiento se preste *online*. Sobre estas consideraciones, volveremos en apartados posteriores.

Por último, el principio de privacidad desde el diseño y por defecto (art. 25 RGPD), se incorpora por primera vez en un cuerpo normativo mediante la publicación del presente reglamento europeo. Sin embargo, en contra de lo que pudiera pensarse, la *Privacy by Design* no constituye una herramienta ideada por el RGPD, pues en 2010 se adoptó una Resolución sobre la misma en la 32ª Conferencia Internacional sobre protección de datos celebrada en Jerusalén entre los días 27 y 28 de octubre de ese mismo año[228]. El cometido principal de la misma se identifica con el establecimiento de medidas de control y prevención adecuados, que garanticen un entorno digital más seguro y sólido para la privacidad de las personas. Este principio adquiere gran relevancia en el entorno de Internet y las redes sociales donde la vida privada de las personas puede sufrir intromisiones debido al diseño y finalidad de estos espacios virtuales.

---

[227] Directrices del Grupo de Trabajo del Artículo 29 sobre la transparencia en virtud del Reglamento (UE) 2016/679, de 11 de abril de 2018, WP 260, pp. 6-7.

[228] *Resolution on Privacy by Design*. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalen (Israel), 27-29 October, 2010. Obtenido de: http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf (última consulta el 9 de marzo de 2022).

De este modo, CEPD[229], aporta una serie de Directrices de necesaria mención sobre el principio de protección de datos desde el diseño y por defecto[230]. En orden a resultar más específicos, el organismo europeo aduce que la protección de datos desde el diseño y por defecto implica la obligación esencial para los responsables del tratamiento de aplicar las medidas adecuadas y las garantías necesarias a efectos de garantizar de manera efectiva los principios de protección de datos recientemente citados en la presente investigación, así como los derechos y libertades de los interesados. En términos similares se manifiesta el Considerando 78 RGPD.

En este orden de cosas, la protección de datos desde el diseño y por defecto se constituye como un requisito que habrá de cumplirse por todos los responsables del tratamiento, se traten estos de pequeñas empresas o multinacionales. Ahora bien, este principio se desglosa en dos comportamientos complementarios entre sí. Concretamente, los responsables del tratamiento deberán diseñar sus servicios de tal modo que se respeten los principios y garantías de protección de datos personales y como opción por defecto durante todo el ciclo de tratamiento. Concretamente, la protección de datos desde el diseño, supone la inclusión de aquellas técnicas que habrán de aplicarse desde el mismo momento en el que el responsable determine los medios de tratamiento e incluso mientras dure el mismo debiendo revisar que estas continúan garantizando los principios y derechos de los interesados. Por otra parte, la protección de datos por defecto, conlleva que, el responsable del tratamiento deba, por defecto, llevar a cabo los tratamientos estrictamente necesarios para cumplir con los fines de tratamiento preestablecidos.

Sin embargo, sobre este segundo comportamiento, debemos mencionar, por encontrarse en estrecha relación con la protección de datos desde el diseño y por defecto (art. 25 RGPD), el principio de minimización de los datos, que impone a los responsables del tratamiento las siguientes obligaciones. En primer lugar, deberán verificar la

[229] Tras la aprobación del RGPD, el Comité Europeo de Protección de Datos Personales (CEPD) sustituye al Grupo de Trabajo del Artículo 29 como organismo europeo independiente cuyo cometido principal se halla en aplicar de manera coherente las normas de protección de datos personales en el seno de la UE, además de fomentar la cooperación entre autoridades de protección de datos personales europeas. Obtenido de: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_es (última consulta el 20 de noviembre de 2022). Este organismo se compone por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos. Para más detalle, véase ULLOA RUBIO, I., "Comité Europeo de Protección de Datos (Comentario a los artículos 68 a 76 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 2922.

[230] Directrices 4/2019, del Comité Europeo de Protección de Datos, relativas al art. 25 Protección de datos desde el diseño y por defecto, de 20 de octubre de 2020.

posibilidad de alcanzar los fines pertinentes tratando la menor cantidad de datos posible. En segundo lugar, no deberán conservar los datos personales si ello no deviene necesario para la finalidad del tratamiento. Por último, deberán limitar el acceso a los datos personales, debiendo valorar que la puesta a disposición de datos personales a un número indeterminado de personas puede producir consecuencias negativas sobre los derechos de las personas. Sobre este último aspecto, los responsables, por defecto, deberán ofrecer a los interesados la oportunidad de intervenir de manera previa a que sus datos personales sean accesibles a todo el público, especialmente si son menores de edad[231]. Como veremos posteriormente, este principio adquiere vital importancia en el caso de las redes sociales.

Así, los responsables del tratamiento y especialmente los proveedores de redes sociales deberán garantizar, por una parte, que el diseño de los tratamientos de las plataformas respete lo máximo posible la privacidad de las personas, y por otra parte, que sus espacios constituyan plataformas, por defecto, garantes con la protección de datos personales. Tanto el diseño de los tratamientos que las redes sociales acometen, como los parámetros de privacidad que estas configuran por defecto, no siempre resultan garantistas con los principios y derechos de los interesados. Sirva como ejemplo que los datos pueden encontrarse accesibles por defecto a un número indeterminado de estas; en ese sentido, plataformas como Facebook, durante años han obligado a los usuarios a modificar en los ajustes de privacidad los destinatarios de la información personal que en la plataforma se comparte. Esto es, por defecto, la información se comparte con la totalidad de usuarios de la plataforma salvo que el interesado modifique en los ajustes de la aplicación el número de destinatarios.

Así las cosas, entre aquellas facultades que garantizarán un control a los interesados sobre su información personal, destacan los tradicionales derechos ARCO además de los que han de añadirse fruto de la entrada en vigor del RGPD, a saber: el derecho a la limitación del tratamiento (art. 18 RGPD), el derecho a la portabilidad (art. 20 RGPD) y el derecho a la supresión (art. 17 RGPD). No obstante, no se constituye el objetivo de las siguientes líneas conceder un desarrollo pormenorizado de los mismos.

[231] Véanse las Directrices 4/2019, del Comité Europeo de Protección de Datos, relativas al art. 25 Protección de datos desde el diseño y por defecto, de 20 de octubre de 2020, p. 14.

Por otra parte, es preciso apuntar que el RGDP reafirma su aplicabilidad a todo tratamiento de datos realizado a través de Internet, aunque la empresa titular de un determinado servicio (red social, motor de búsqueda, etc.) posea su sede en un tercer país y pretenda la aplicación de la legislación de ese tercer país[232]. Esta ampliación del ámbito de aplicación del RGPD constituye, sin duda, un avance más que significativo en la garantía del derecho a la protección de datos personales en la era digital, ya que, a causa de la vis expansiva del RGPD y su ámbito global de aplicación, las empresas de países terceros, deberán respetar el derecho europeo a pesar de que no radiquen en territorio de la UE[233].

Por todo lo expuesto, podemos observar, que la UE se propone configurar una regulación que garantice la protección de los datos personales ante el imparable avance de las TIC, incluyendo en su articulado aquellos mecanismos jurídicos que deberán salvaguardar la privacidad de las personas cuando como usuarias de las TIC. Por medio del presente Reglamento, se abandona la regulación tradicional de la protección de datos personales, para inmiscuirse en la protección de dicha información personal cuando los ciudadanos navegan por la red. Ahora bien, HERRAN ORTIZ afirma que, constituye una opinión generalizada entre los expertos que el RGPD nace obsoleto debido a que no menciona fenómenos como el *big data*, computación en la nube o el Internet de las cosas[234]. Aunque nos mostramos conformes con dicha afirmación, en el sentido que, las TIC poseen la capacidad de avanzar de una manera más rápida a la capacidad que el Derecho posee de adaptarse y el RGPD nace sin incorporar dichos fenómenos, toma conciencia de dicha circunstancia en el art. 97.5 RGPD en el que dispone que, la Comisión presentará en caso de advertirse necesario, propuestas para modificar el RGPD, en

[232] Sobre este aspecto, la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González,* Asunto C-131/12 afirma la aplicabilidad de la normativa europea sobre protección de datos personales a Google al poseer esta una filial en territorio español.

[233] En ese sentido, se ha constituido como un comportamiento habitual de empresas prestadoras de servicios de la sociedad de la información alegar que la normativa de la UE no les era de aplicación bajo la regulación de la derogada Directiva 95/46/CE. La consecuencia inmediata de dicha circunstancia se encuentra en negar a los usuarios europeos algunos de los derechos que la normativa les garantiza, así como obligar a los mismos a solicitar la tutela de sus derechos en tribunales internacionales, principalmente estadounidenses. Esta evidente indefensión se soslaya por medio del nuevo ámbito de aplicación del RGPD. Véase a tal efecto la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González,* Asunto C-131/12.

[234] HERRÁN ORTÍZ, A.I., "Aproximación al derecho a la protección de datos personales en Europa. El Reglamento General de Protección de Datos personales a debate", *op. cit.,* p. 199.

particular tomando en consideración la evolución de las tecnologías de la información y a la vista de los progresos de la sociedad de la información.

A nuestro juicio, la inclusión de dicha cláusula reviste vital relevancia, dado que, mediante la incorporación de la misma en el texto normativo, la UE toma conciencia de la vertiginosa evolución de las TIC en nuestra sociedad, evolución que continúa de manera imparable, pretendiendo así de evitar la obsolescencia de la que padeció la Directiva 95/46/CE durante años. En definitiva, tratándose de las TIC resulta inevitable reparar en que, en cierto modo el RGPD nace obsoleto, pero contiene la solución a dicha obsolescencia en el art. 97.5. A futuro, recaerá sobre las instituciones europeas el empleo de dicho mecanismo en orden a garantizar el mantenimiento de la efectividad de la normativa europea en el contexto digital.

2.4.2. La esperada positivización de la protección de datos personales de menores

Por primera vez en el desarrollo normativo de la protección de datos, el RGPD incluye en su articulado las particularidades de la minoría de edad respecto al tratamiento de datos personales. Al amparo del Considerando 38, accede a una norma positiva la necesidad de protección específica de los más jóvenes ante la posibilidad de que tomen menos consciencia de los riegos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales[235]. Como se puede observar, finalmente la UE incorpora a la normativa del derecho fundamental de protección de datos personales los postulados de la Convención de Derechos del Niño de 1989 en lo que al reconocimiento de derechos y a la protección de los mismos cuanto el titular es un menor se refiere.

Así las cosas, el RGPD incorpora tres garantías fundamentales destinadas a la minoría de edad, a saber: la adaptación del principio de transparencia a las vicisitudes de los más jóvenes, previo a prestar su consentimiento (art. 12 RGPD); las condiciones de validez del consentimiento al tratamiento de datos personales, cuando el mismo se

[235] El Considerando 38 RGPD dispone que: «Los niños merecen una protección específica de sus datos personales, ya que pueden resultar menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños».

proporciona por un menor de edad (art. 8 RGPD); y la relevancia que el derecho de supresión " derecho al olvido" adquiere en el caso de que el consentimiento prestado por un menor de edad, para los casos en los que desee suprimir información personal de la red alcanzada la mayoría de edad (art. 17 RGPD).

Definitivamente, a nuestro parecer, el RGPD incorpora la minoría de edad en dos momentos clave en lo que a la protección de los datos personales se refiere. Un primer momento referido a la adaptación de la minoría de edad a las circunstancias concernientes al inicio de la relación entre el responsable del tratamiento y el menor, relación que comienza con la prestación del consentimiento (art. 8). Así como un segundo momento, que identificamos como el final de la relación entre el menor y proveedor de redes sociales que tiene lugar al darse de baja del servicio. Este segundo momento, puede venir de la mano del deseo del interesado, en este caso menor, de eliminar la información personal que pueda circular en la red sobre su persona -incluso puede desear dicha supresión sin necesidad de cancelar su cuenta- (art. 17.3 RGPD).

Seamos conscientes que la adaptación de la situación de los más jóvenes a estos momentos como usuario de redes sociales reviste transcendental relevancia. En el caso del consentimiento, la falta de madurez del menor puede desembocar en una prestación del consentimiento no consciente que lleve a la aparición de diversas vulneraciones de derechos fundamentales del menor, comenzando por el derecho a la protección de datos personales. Por otra parte, en el caso del derecho de supresión, la falta de madurez constituye nuevamente la causa que motiva la previsión de especiales facultades cuando se ejercita por los más jóvenes; en el sentido que, aumentan las probabilidades de que información concerniente a los menores de edad, y no en pocas ocasiones sensible, circule en la red con carácter indefinido a pesar de que finalice la relación entre el responsable.

En consecuencia, el RGPD se preocupa especialmente por ofrecer a los menores de edad (aunque ya no lo sean cuando ejercitan el derecho de supresión) la facultad de solicitar al responsable que elimine toda referencia a dicha información personal. El cambio de paradigma es más que destacable; sin embargo, nos preguntamos si dichos momentos, tan cruciales para la salvaguarda de los datos personales de los más jóvenes, como la prestación del consentimiento y el ejercicio del derecho de supresión o al olvido se encuentran regulados de forma suficientemente garantista.

Por último, el art. 12 del RGPD, arroja luz sobre el principio de transparencia y las condiciones en el que este deberá desenvolverse en el caso de menores de edad. No obstante, recordemos que el principio de transparencia se encuentra íntimamente ligado al momento de prestar consentimiento para aquellas ocasiones en las que este se constituya como la base de legal que legitima el tratamiento. Ello se debe a que su finalidad última se identifica con garantizar la comprensión por parte del interesado de toda la información que debe facilitarse al momento de prestar el consentimiento, para lo que el responsable del tratamiento deberá informar de una manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, especialmente si la información se dirige a un niño. La inclusión de esta circunstancia en la normativa europea resulta obligada, ya que se ha podido constatar que la información facilitada por los responsables del tratamiento no es accesible, no siempre reviste claridad, ni se expone redactada en un lenguaje sencillo, cuestión que, desde luego complica en mayor medida el entendimiento de las mismas por los más jóvenes.

Ciertamente, en el caso de las redes sociales, de manera previa a la publicación del perfil, deviene indispensable la lectura y aceptación de las políticas de privacidad de las respectivas plataformas, de tal suerte que el interesado debe consentir expresamente el tratamiento de datos personales mediante la aceptación de los términos y condiciones de la política de privacidad de la red social. Tal y como señala PÉREZ DÍAZ, el problema reside en que no todas las redes sociales cumplen la normativa de protección de datos personales en este aspecto, habida cuenta que las políticas de privacidad no siempre se encuentran suficientemente destacadas en las páginas de inicio ni en las fases de registro que el usuario debe acometer[236].

Sin embargo, sin perjuicio de que las cuestiones expuestas constituyen objeto de estudio minucioso en el capítulo tercero de la presente tesis, de conformidad con BENEDITO CAÑIZARES, la posición del legislador europeo en el RGPD respecto a los menores de edad puede calificarse, textualmente en palabras de la autora, de tibia[237]. Así, se puede apreciar que tras varias décadas de absoluta desprotección, de las novedades y avances incorporados no se desprende una auténtica evolución en la protección de la

[236] PÉREZ DÍAZ, R., "La protección de los datos del menor en el uso de las tecnologías de la información y de la comunicación (TIC)", *Revista de Derecho privado*, 2018, núm. 102, p. 82.
[237] BENEDITO CAÑIZARES, Mª T., "La autorregulación en el Reglamento General de Protección de Datos como solución frente al mercado digital fragmentado: el menor y los Registros", *op. cit.*, p. 3124.

infancia. En efecto, la mayoría de propuestas elaboradas por el Grupo de Trabajo del Artículo 29 en su Informe 2/2009 *The protection of children's personal data* citado con anterioridad, no se acogen en el RGPD, procediendo a regular la materia a partir de la inclusión en la misma de unos principios generales en los términos de consentimiento, transparencia y derecho a la supresión de los datos. Sobre la ausencia de una normativa más completa en lo que a la protección de los menores se refiere, también se muestra de acuerdo AZURMENDI cuando afirma que el RGPD se inhibe de la protección de datos de los menores y transfiere a los Estados la tarea de legislar de manera más concreta sobre la protección de datos de estos[238]. En definitiva, la adopción de criterios que salvaguarden la protección jurídica del menor puede considerarse tardía, además de poco comprometida con los derechos del menor, tal y como se analizará con rigor en apartados posteriores.

3. UNA APROXIMACIÓN A LA EVOLUCIÓN NORMATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA JURÍDICO ESPAÑOL

El ordenamiento jurídico español no ha permanecido ajeno a la irrupción de la revolución tecnológica acaecida en la sociedad cuyo inicio podemos situar, aproximadamente, medio siglo atrás. Al igual que el resto de Estados contemporáneos, el legislador español se vio inmerso en la necesidad de afrontar el reto de constitucionalizar nuevos derechos fundamentales entre los que se encuentra el derecho a la protección de datos de carácter personal. Sin embargo, dicho camino no se encontró libre de arduos esfuerzos, críticas y la necesidad de interpretaciones jurisprudenciales.

En este contexto, la incorporación de este derecho en los textos constitucionales de la UE, no ha sido temprana, ni pacífica en muchos de los Estados. A ello cabe añadir que, en el caso español, si bien el avance informático se regula en el art. 18.4 CE, se configura como un precepto cuyas lagunas e interrogantes han precisado de desarrollo legal y jurisprudencial, fuertemente debatido en determinadas ocasiones, para su correcto entendimiento. Por ello, resulta de vital importancia exponer la evolución del derecho a la protección de datos de carácter personal en el ordenamiento jurídico nacional, anteriormente conocido como autodeterminación informativa, para poder comprender la

[238] AZURMENDI, A., "Derechos digitales de los menores y datos masivos. Reglamento europeo de protección de datos de 2016 y la Coppa de Estados Unidos", *El Profesional de la información*, 2018, vol. 27, núm. 1, p. 34.

incidencia que la mentada circunstancia ha podido tener sobre la normativa que aborda la protección de datos del menor.

Por último, no debemos olvidar que constituye tarea reservada de la presente investigación propiciar un estudio de las garantías tendentes a la protección de los datos de carácter personal de los menores de edad, por lo que, también ha de analizarse la tardía incorporación de la minoría de edad en la normativa protectora de dicho derecho fundamental en España. Desafortunadamente, se ha precisado del transcurso de aproximadamente tres décadas para que la normativa reguladora del derecho fundamental cuyo estudio se realiza, incorporase en su articulado menciones a la minoría de edad con el fin de propiciar la protección de sus datos de carácter personal.

3.1 De la limitación del uso de la informática a la configuración de un derecho fundamental autónomo de protección de datos de carácter personal

La CE de 1978, junto con la Constitución de Portugal de 1976 se consideran pioneras en el reconocimiento de lo que, a posteriori, se conocerá como el derecho fundamental a la protección de datos personales. Ciertamente, la CE recibió el influjo de la constitución portuguesa que[239], de forma precursora reconocía de manera previa al resto de países europeos la protección de las personas frente al tratamiento de datos personales. Sin embargo, esta afirmación no debe conducir a equívocos, pues nuestra CE no llega a aproximarse al nivel de garantía que proporciona el texto portugués[240].

En efecto, dos son los preceptos de la Constitución portuguesa dedicados a la protección de los datos personales a propósito de los posibles tratamientos abusivos que la informática puede propiciar. Por una parte, el art. 26.2, redactado de manera genérica, pues dispone que la ley establecerá las garantías efectivas contra la utilización abusiva o contraria a la dignidad humana, de informaciones referentes a las personas y a las familias. Por otra parte, el art. 35, que traza de manera más detallada una esfera específica

[239] Constituição da República Portuguesa, Texto originário da Constituição, aprovada em 2 de Abril de 1976. Obtenido de: https://www.parlamento.pt/parlamento/documents/crp1976.pdf (última consulta 7 de mayo de 2021).

[240] En ese sentido se manifiesta RALLO LOMBARTE cuando afirma que en España se fijaron los contornos del desarrollo legislativo del derecho fundamental a la protección de datos personales con menos ambición que en el país luso, pues la CE se limitó a reconocer los riesgos que la informática suponía obligando al legislador a imponer limitaciones en su uso. Véase RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales 1978-2018", *op. cit.*, p. 646.

de actuaciones cuya finalidad reside en la protección de dichos datos personales. A pesar de que su redacción originaria resultaba más precaria, la Constitución portuguesa vio modificado su art. 35 en varias ocasiones, una de ellas en el año 1982, seguida de una nueva modificación en 1989[241], hasta que el legislador constitucional portugués proporciona al mismo- en lo concerniente a los tratamientos de datos personales- la redacción actualmente vigente[242].

Tal y como se ha dispuesto, el nivel de garantía de la norma portuguesa no se alcanza por la CE de 1978. El art. 18.4 CE, único precepto que menciona el fenómeno de la informática, ofrece respuesta a la amenaza que plantea este nuevo contexto digital limitando su uso. No se halla ninguna precisión, más allá del art. 18.4 CE que en aquel momento arrojara claridad sobre el contenido esencial de dicho derecho, ni sobre el bien jurídico objeto de protección, así como sobre las eventuales precisiones sobre su desarrollo. Es más, la CE española no se ha modificado, al contrario de lo que ocurre en el caso portugués, por lo que el texto constitucional español, regula de un modo amplio en comparación con el del país luso en lo concerniente a la protección de las personas ante un evento especialmente cambiante como la tecnología.

3.1.1. El fundamento constitucional del derecho a la protección de datos personales: el debatido artículo 18.4 CE

El art. 18.4 CE dispone que *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".* No en vano, debemos advertir que el fenómeno informático se incorpora en el art. 18 de la CE, cuya finalidad reside en reconocer y proclamar distintos derechos inherentes a la privacidad de las personas, lo que podría llevar a pensar

[241] Para mayor detalle, consúltese GOMES CANOTILHO VITAL MOREIRA, J.J., "Constituçao da Republica Portuguesa, *Lei do Tribunal Constitucional*, 1993, 3ª ediçao revista.

[242] El art. 35 de la Constitución Portuguesa dispone que: «1. Todo ciudadano tendrá derecho a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan esos datos, y podrá exigir su rectificación, así como su actualización, sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales. 2. Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros y la respectiva interconexión, salvo en casos excepcionales previstos por ley. 3. No podrá utilizarse la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo cuando se trata del tratamiento de datos estadísticos no identificables individualmente. 4. La ley definirá el concepto de datos personales para fines de registro informático, así como de bases y bancos de datos y las respectivas condiciones de acceso, constitución y utilización por entes públicos y privados. 5. Se prohíbe la asignación de un número nacional único a los ciudadanos. 6. La Ley determinará el régimen aplicable a los flujos de datos allende las fronteras, estableciendo formas adecuadas desprotección de los datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional». **[**Traducción propia**]**

que, dentro de la esfera del derecho a la intimidad, el art. 18.4 CE se presenta como una manifestación más de la protección de la vida privada. Dicha manifestación albergaría su razón de ser ante la insuficiencia de la antigua proclamación del derecho a la intimidad como protección suficiente frente a la nueva realidad del progreso tecnológico. Es esta afirmación, precisamente, la que protagonizó las no pocas discusiones en seno de debate parlamentario previo a la aprobación de la CE. En efecto, durante la tramitación parlamentaria del texto constitucional, las voces críticas con la aprobación del apartado cuarto del art. 18 de la CE, consideraban innecesaria la incorporación del mismo, ya que a su entender, los derechos de las personas se hallaban suficientemente protegidos mediante el apartado primero del art. 18 frente al avance de la informática[243]. La reticencia de algunos grupos no debe llevarnos a pensar en una absoluta despreocupación del legislador sobre el peligro que la informática supone para los derechos de las personas, también se sucedieron intervenciones que advertían sobre los riesgos de la informática para el disfrute de derechos fundamentales[244].

El transcurso de varias décadas ha demostrado cuán equivocadas se encontraban dichas voces críticas al no considerar necesaria la inclusión del apartado cuarto del art. 18 CE, encargado de visibilizar la informática[245]. Sin embargo, se han precisado varios años y un peregrinar contradictorio de resoluciones jurisprudenciales, para considerar el derecho a la protección de datos personales como un derecho fundamental autónomo e independiente respecto del derecho a la intimidad. Como cabía esperar, de acuerdo con TRONCOSO REIGADA, el constituyente español no fue consciente entonces de la

[243] En ese sentido se manifiesta el SANCHO ROF en la ENMIENDA NUM. 716. CONGRESO DE LOS DIPUTADOS, Diario Oficial de sesiones de las Cortes Generales, núm. 70, de 19 de mayo de 1978.

[244] Véase en ese sentido ZARAZAGA, GRUPO MIXTO: «Tenemos que situarnos en el futuro...vendrán otras muchas técnicas no solo la informática, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera, aun antes de haber salido de la meta...El mundo y las personas están cambiando a ritmo inimaginables. Hemos de prepararnos para entender este mundo y proteger los derechos de los ciudadanos en los ambientes individuales, familiar y social...Hay que evitar la traición de la tecnología; hay que arbitrar nuevos sistemas de valores». SAIZ MORENO, F., CORTES GENERALES: *Constitución Española. Trabajos parlamentarios,* Tomo I, Madrid, Cortes Generales, 1980, pp. 1068 y ss.

[245] En ese sentido, una vez incluído el apartado cuarto del art. 18 CE, a futuro también mostrarían su rechazo al reconocimiento de un nuevo derecho fundamental voces críticas como la encabezada por ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de los ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Granada, Comares, 1994, p. 48 y ss.

importancia que la informática alcanzaría, de su desarrollo futuro y de los peligros que esta podría suponer para los derechos de las personas[246].

El avance en el empleo de las nuevas tecnologías, auspició el desarrollo del art. 18.4 CE. Sin embargo, el precepto recientemente mencionado, no proclamaba ni proclama de manera clara un derecho fundamental a la protección de datos de carácter personal[247], y ello dificultaba considerablemente articular garantías para la seguridad de las personas frente al avance imparable de la informática. Por ese motivo, los esfuerzos jurisprudenciales se concentraron en dotar al derecho a la protección de datos personales de autonomía respecto al derecho a la intimidad, configurando un derecho independiente cuyo bien jurídico a proteger, así como el contenido esencial del mismo distaban del tradicional derecho a la intimidad personal. La consagración del derecho a la protección de datos personales en el ordenamiento jurídico español, además de convulsa, se ha llevado a cabo de manera excesivamente pausada. Dicha lentitud, resulta poco entendible, habida cuenta que otros países como Italia y Alemania partían de una situación menos favorable, pues sus constituciones no mencionaban siquiera el fenómeno informático- al aprobarse sus cartas magnas después de la Segunda Guerra Mundial- y, construyeron sus derechos fundamentales a la protección de datos personales de manera más ágil que el ordenamiento jurídico español.

Así, Italia se decantaba por reconocer un *diritto a la riservatezza,* proclamando una libertad informática como una nueva clase de libertad personal, que se define como la facultad de la persona para controlar las informaciones que sobre ella se almacenan en un ordenador[248]. El caso alemán, también partía de una ausencia de un precepto constitucional que de manera expresa reconociera un derecho a la protección de datos personales, es más, tampoco contaba con un derecho fundamental a la intimidad. Como vía solutoria, el Tribunal Constitucional Federal, ubicó este nuevo derecho fundamental dentro de la dignidad de la persona, proclamando que del principio del libre desarrollo de la personalidad nacen tanto el derecho a la intimidad como el derecho a la autodeterminación informativa. Sobre este último, la Sentencia de 15 de diciembre de

[246] TRONCOSO REIGADA, A., "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público,* (mayo- diciembre 2003), núm. 19-20, p. 246.
[247] RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales,* Valencia, Tirant lo Blanch, 2019, pp. 26-28.
[248] Véase la Costituzione della Repubbdlica Italiana, Gazzetta Ufficiale, el 27 de diciembre de 1947, núm. 298.

1983 proclama el *informationelle Selbstbestimmungsrecht* (autodeterminación informativa) y establece las bases de ese nuevo derecho[249]. Del contenido de la sentencia, nos permitimos destacar que, el Tribunal Federal Alemán, no sólo proclamó un nuevo derecho fundamental, sino que, además, precisó el contenido mínimo y esencial del derecho a la autodeterminación informativa con el fin de salvaguardar la dignidad y libre desarrollo de la personalidad del individuo.

Del estudio de ambos casos, italiano y alemán se desprende que, la posición del legislador español no resultaba tan desfavorable como la de los casos expuestos, dado que el legislador constituyente previó la inclusión del fenómeno informático en la CE, y faltaba entonces perfilar la proclamación de un derecho autónomo e independiente de la intimidad con el fin de dotarlo posteriormente de contenido esencial. Por tanto, sorprende que hasta el año 2000 no se dotara de contenido esencial al derecho de protección de datos personales, mientras que las reformas constitucionales de otros Estados europeos incluían preceptos que garantizan la protección de datos personales; así por ejemplo, países como Finlandia incluían dicho derecho fundamental en el año 1980, mientras que Países Bajos en el año 1983[250].

3.1.2. La intensa labor interpretativa del Tribunal Constitucional en la proclamación de un nuevo derecho fundamental: el contenido esencial del derecho a la protección de datos personales

Al tiempo que gran parte de los ordenamientos jurídicos del entorno europeo reconocían el derecho a la protección de datos personales, en el caso español, correspondió al TC la labor de conceder a este derecho rango de fundamental y autónomo del derecho a la intimidad. Recordemos que, art. 18.4 CE solamente se pronuncia sobre

[249] Sentencia del Tribunal Federal Alemán, de 15 de diciembre de 1983, ref. 1 Bvr. 209/83.

[250] La Ley Fundamental del Reino de los Países Bajos, revisada en 1983, señala en el art. 10 que «la ley establecerá las normas de protección de la intimidad personal en relación a la indagación y difusión de datos personales» y "la ley dictará normas sobre el derecho de toda persona a que se le dé conocimiento de los datos recogidos sobre ella y del uso que se hiciere de los mismos, así como al perfeccionamiento de dichos datos" versión que permanece vigente en la actual Constitución de 21 de diciembre de 2018, Boletín Oficial de Países Bajos, https://wetten.overheid.nl/BWBR0001840/2018-12-21?VergelijkMet=BWBR0001840%3fg%3d2002-03-21%26v%3d0 (última consulta el 16 de marzo de 2022). Por otra parte, la reforma de la Constitución finlandesa de 1980 (art. 8) señala que "la ley establecerá normas de detalle sobre la salvaguardia de los datos de carácter personal" En la actualidad, el precepto constitucional que regula dicho derecho es el art. 10 de la Constitución de Finlandia de 11 de junio de 1999, Boletín Oficial de Finlandia. Obtenido de: https://finlex.fi/sv/laki/ajantasa/1999/19990731 (última consulta el 16 de marzo de 2022). [traducciones propias].

la limitación del uso de la informática con el fin de salvaguardar el honor, intimidad personal y familiar, así como el pleno ejercicio de sus derechos. Por tanto, del mismo, el TC construye un nuevo derecho fundamental independiente con contenido esencial propio. Esta afirmación, no debe conducir a equívoco, arduo fue el camino hasta poder materializar dicha autonomía e independencia como derecho fundamental, pues inicialmente el propio TC calificaba este derecho como una especificación del derecho a la intimidad[251].

Hubo que esperar a las Sentencias 290/2000 y 292/2000, de 30 de noviembre, para obtener un pronunciamiento concluyente del TC. A pesar de ello, los numerosos pronunciamientos del TC hasta dicha fecha, sirvieron para la determinación paulatina del contenido esencial del derecho fundamental a la protección de datos personales.

Así las cosas, el 30 de noviembre del año 2000 se constituye como una fecha señalada en la historia y evolución del derecho a la protección de datos personales en España. Finalmente, el TC se pronuncia sobre el contenido esencial de dicho derecho. De un lado, la Sentencia 290/2000, de 30 de noviembre, reitera conceptos previos, en el sentido que, proclama la consagración de un nuevo derecho en el art. 18.4 CE, cuya finalidad última reside en garantizar a las personas un poder de control y disposición sobre sus datos personales. A tal fin, otorga a su titular un haz de facultades que se consideran elementos esenciales del derecho fundamental a la protección de los datos personales, integradas por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Para dotar de efectividad el contenido del derecho, los titulares de los datos detentan el derecho recibir la información referente a quién posee los datos personales relativos a su persona y con

[251] Cabe destacar, en primer lugar, la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, Boletín Oficial del Estado, de 18 de agosto de 1993, núm. 197, pp. 28 a 34, como la primera Sentencia en reconocer un verdadero derecho fundamental a la protección de datos personales. Ahora bien, reconocida su autonomía, resulta indispensable dotar a dicho derecho fundamental de determinado contenido esencial y es justamente, en dicha argumentación jurisprudencial donde el TC remite el bien jurídico protegido al ámbito de la intimidad. Efectivamente la sentencia dispone que "al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la Administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad". Al presente pronunciamiento, le siguen una estela de resoluciones del TC contradictorias entre sí. En ocasiones, el Alto tribunal aúna esfuerzos en desvincular la protección de datos personales del derecho a la intimida; y en otras, lo imbrica directamente en el mismo. Sirvan como ejemplo los prunciamientos que se exponen como sigue: La Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo, Boletín Oficial del Estado, de 13 de junio de 1994, núm. 140, p. 46 a 51; La Sentencia del Tribunal Constitucional 11/1998, de 13 de enero, Boletín Oficial del Estado, de 12 de febrero de 1998, núm. 37, pp. 48 a 53; y, por último, La Sentencia del Tribunal Constitucional de 144/1999, de 22 de julio, Boletín Oficial del Estado, de 26 de agosto de 1999, núm. 204, pp. 35 a 47.

qué finalidad, el derecho a oponerse a la posesión de dichos datos, así como a su uso. En definitiva, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares (públicos o privados) de ficheros de datos personales, partiendo de que conoce la existencia de tales ficheros y su contenido, así como el uso y destino de los mismos[252].

De otro lado, la Sentencia 292/2000 se corresponde con el último pronunciamiento del TC sobre la configuración y contenido esencial del derecho fundamental. Finalmente, resolviendo el recurso de inconstitucionalidad presentado por el Defensor del Pueblo contra algunos preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[253] (en adelante LOPD) que reproducían preceptos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal[254] (en adelante, LORTAD), dotaba del ansiado contenido esencial al derecho a la protección de datos personales. En efecto, la sentencia del TC 292/2000, de 30 de noviembre se constituye como el pronunciamiento más claro en relación al reconocimiento de un derecho a la protección de datos personales, autónomo respecto del derecho a la intimidad. Pero el Alto Tribunal, además, sienta las bases del contenido de este derecho fundamental diferenciándolo del derecho a la intimidad, esta vez de manera clara. Procedemos pues, a analizar de manera sucinta los argumentos del TC que sustentan la diferencia entre ambos derechos fundamentales regulados en distintos apartados del art. 18 CE.

En primer lugar, el objeto del derecho a la intimidad reside en proteger los datos íntimos de la persona que, por el hecho de reconocérseles tal condición, deben protegerse del conocimiento de los demás, en ese sentido destacamos las palabras de REBOLLO DELGADO cuando afirma que el propio individuo debe determinar qué informaciones quedan reservadas al conocimiento genérico y cuáles, por el contrario, habrán de quedar reservadas[255]; sin embargo, el derecho fundamental a la protección de datos personales

[252] RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", *op. cit.*, p. 652.
[253] Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Boletín Oficial del Estado, de 14 de diciembre de 1999, núm. 298.
[254] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, Boletín Oficial del Estado, de 31 de octubre de 1992, núm. 262.
[255] REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson, 2008, p. 98.

protege cualquier dato, posea este, condición de íntimo o no[256]. Esto es, el derecho a la protección de datos personales, proporciona amparo a toda aquella información que puede resultar conocida por toda la sociedad. Es evidente que, de conformidad con MURILLO DE LA CUEVA, la protección de datos personales brinda una protección más amplia que el derecho a la intimidad[257].

Véase que, se califica como dato personal a aquel que se refiere a datos atribuibles a una persona, a través de los cuales puede procederse a su identificación además de la elaboración de un perfil, aunque no pertenezcan a la esfera íntima de la persona. Esta posibilidad de identificación y elaboración de perfiles, a través de dicha información personal justifica que toda persona posea derecho a controlar sus datos para evitar que se elabore un perfil o un retrato de su personalidad con ellos. En esencia, el contenido nuclear del derecho a la protección de datos personales se encuentra en el control sobre los datos, no en el secreto de dicha información; confiriendo así, la posibilidad a su titular de decidir sobre el uso y destino de sus propios datos personales.

Acorde con este planteamiento, se muestra TRONCOSO REIGADA cuando afirma que, el contenido nuclear de este nuevo derecho fundamental se halla en el control de la información, no el secreto, y en concreto, la facultad de decidir sobre el uso y destino de los propios datos, impidiendo su tráfico ilícito y lesivo para la dignidad del afectado. Adviértase que, tal y como continúa disponiendo el autor, se trata de una injerencia lo que lesiona el derecho a la intimidad, sin embargo, en el caso de los datos personales, es el propio interesado quien revela los mismos. Por ello, resulta de vital relevancia facilitar a la persona una capacidad de control sobre sus datos personales, aunque hayan sido recabados con su consentimiento[258].

De igual modo, RALLO LOMBARTE considera que el contenido esencial del derecho a la protección de datos personales ofrece a sus titulares la capacidad de controlar y disponer de los mismos. Afirmando además, que la proclamación del carácter autónomo del derecho a la protección de datos personales, proporciona un ámbito de protección más

[256] Sobre este aspecto, destacamos la aportación de HERRÁN ORTIZ, A.I., "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos,* 2003, núm. 26, pp. 20-21 cuando afirma que el objeto de protección del derecho fundamental a la protección de datos no se limita a datos íntimos, sino a cualquier información personal, sea esta íntima o no siempre que su tratamiento pueda afectar a derechos y libertades de la persona sean o no fundamentales.
[257] MURILLO DE LA CUEVA, P., *Informática y protección de datos personales,* Madrid, CEC, 1993, pp. 32-34.
[258] TRONCOSO REIGADA, A., *La Protección de Datos Personales: en busca del equilibrio,* Valencia, Tirant lo Blanch, 2010, p. 134-135.

idóneo que los derechos fundamentales tradicionales como el derecho al honor, a la intimidad y al apropia imagen[259]. Así se manifestaba, previo a los pronunciamientos del TC determinado sector de la doctrina, entre los que destaca PÉREZ LUÑO cuando ya en 1981 afirmaba que, la libertad informática consiste en el derecho de autotutela dela propia información, o sea, el derecho a controlar los datos personales[260].

En segundo lugar, el derecho fundamental a la protección de datos personales, se configura como un derecho que atribuye a sus titulares un conjunto de facultades positivas cuyo fin reside en controlar la información personal. Esas facultades consisten en exigir el consentimiento para el tratamiento de datos personales, el derecho a ser informado y los derechos de acceso, oposición, rectificación y cancelación[261]. Ciertamente, el consentimiento se tornará fundamental en el momento de recogida de los datos, debiendo éste recabarse de manera libre y consciente, además de informada, aportando la información indicativa de los posibles destinatarios de dichos datos personales.

Por último, la expresión del art. 18.4 CE no se refiere única y exclusivamente a la tutela de los derechos al honor y a la intimidad, ni tampoco circunscribirse exclusivamente a los derechos fundamentales y libertades públicas. Se protegen así, cualesquiera derechos de la persona, constituyan o no derechos fundamentales que puedan resultar amenazados por el avance de la informática.

De lo expuesto alcanzamos las consideraciones que rezan como sigue: el derecho fundamental a la protección de datos personales se considera un derecho fundamental de reciente creación; además, a diferencia de otros países europeos, la configuración del mismo ha ocurrido de manera tardía y poco pacífica en el sentido que, mientras la gran mayoría de países europeos reconocían un derecho fundamental y autónomo al derecho a la intimidad, el legislador español se mostraba reticente a reconocer la necesidad de dicho derecho, considerando el derecho a la intimidad suficiente garantía de protección frente a la informática; mientras que tribunales constitucionales europeos, como el alemán o el

[259] RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales 1978-2018", *op. cit.*, pp. 651-652.
[260] PÉREZ LUÑO, A.E., "Informática y libertad", *Revista de Estudios Políticos,* 1981, núm. 24, p. 31 y ss. En términos similares se posiciona FROSINI, V., "La protezione della riservatezza nella societá informatica" *Informatica e Diritto,* 1981, VIII, p. 5 a 14.
[261] Véase en ese sentido lo dispuesto por SERRANO PEREZ, Mª. M., "El derecho fundamental a la protección de datos. Su contenido esencial", *Anuario multidisciplinar para la modernización de las Administraciones Públicas,* 2005, núm.1, pp. 253-254.

italiano, construyeron acertadamente y con relativa celeridad sus derechos a la protección de datos personales, el TC español no se pronunció sobre dicho extremo de manera concluyente hasta el año 2000.

En vista de la evolución jurídica, el derecho a la protección de datos personales no parece constituir una prioridad del legislador español que, ante la situación de proporcionar una respuesta normativa a situaciones novedosas, acostumbra considerarse un comportamiento habitual observar la evolución de la normativa tanto internacional, como la que paulatinamente aprueban los restantes Estados europeos a nivel nacional. Por ello, no podemos evitar preguntarnos por qué el legislador español no procedió de la manera descrita postergando injustificadamente tal reconocimiento.

Sin embargo, en la actualidad nos encontramos inmersos en plena era digital en la que, Internet, las TIC, las redes sociales, la computación en la nube, el *big data*, etc., constituyen un elemento indispensable en nuestro día a día. A través de dichas herramientas digitales socializamos, desarrollamos nuestras carreras profesionales, impartimos docencia etc. En consecuencia, determinadas voces, con las que no nos mostramos conformes, consideran que se presenta el momento de hacer frente a las limitaciones que el art. 18.4 CE supone para la garantía de los derechos fundamentales en Internet en pleno siglo XXI mediante el reconocimiento de nuevos derechos constitucionales[262].

Concretamente, proponen que este momento se presenta como idóneo para actualizar la CE y adaptarla a la nueva era digital que se encuentra presente en nuestros comportamientos más cotidianos, mediante la constitucionalización de una nueva generación de derechos[263]. Sobre ese aspecto se manifiesta LEÓN CAMACHO cuando

[262] Así, destaca la reflexión de RALLO LOMBARTE cuando propone un listado de derechos digitales tales como: «a) el derecho de acceso a Internet, b) el derecho a la formación digital, c) el derecho a la neutralidad en la Red, d) el derecho al honor y la propia imagen frente a agresiones específicas procedentes de la Red, e) el derecho a la libertad de expresión y a la veracidad de las informaciones en la Red, f) el derecho de los trabajadores a su intimidad en la utilización de medios digitales y el derecho a la desconexión laboral, g) el derecho de acceso *online* a datos, innovaciones, creaciones y conocimiento generado con fondos públicos h) el derecho a obtener reparación efectiva ante daños causados por conductas ilícitas en la Red, i) el derecho de los menores a su seguridad en la Red». Sobre la inclusión de este último derecho volveremos a incidir en los apartados posteriores de la siguiente investigación. RALLO LOMBARTE, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales 1978-2018", *op. cit.*, p. 666.

[263] La clasificación de los derechos fundamentales en distintas generaciones se emplea por primera vez por KAREL VASÁK en 1979 durante una conferencia en el Instituto Internacional de Derecho Humanos en Estrasburgo. De tal suerte que la primera generación de derechos se identifica con aquellas libertades fundamentales y los derechos civiles y políticos que conforman la génesis de derechos humanos (estos derechos fueron reclamados en la Revolución Francesa); la segunda generación de derechos fundamentales se proclaman en las constituciones liberales del siglo XIX y se identifican como derechos sociales y

aboga por el reconocimiento de una cuarta generación de derechos fundamentales emergentes de la era digital. La razón de ser de esta nueva generación conduce a la consideración del mundo digital como una absoluta realidad que, precisa ya no solo de una regulación específica que vele por la protección de los derechos de las personas usuarias, sino de una amplia y global protección de los nuevos derechos fundamentales digitales que nacen como consecuencia del empleo masivo de la tecnología[264].

En ese sentido, ROIG propone que, los nuevos derechos fundamentales que aparezcan a causa del extendido empleo de las TIC, deberán incluirse en nuestra CE a partir del derecho a la dignidad humana, puesto que, nuestra Carga magna no se encuentra provista de una cláusula de actualización de derechos como sí lo prevén otras constituciones, como por ejemplo la de Portugal. En consecuencia, el TC no posee capacidad para reconocer autónomamente nuevos derechos fundamentales. A su juicio, la CE únicamente menciona el fenómeno informático abogando por la limitación del mismo en orden a garantizar los derechos, pero, según apunta ROIG, los problemas informáticos se han acotado al derecho a la protección de datos personales[265].

No obstante, a nuestro juicio, el art. 18.4 CE no se imbrica exclusivamente en dicho derecho fundamental, recordemos que, la informática deberá limitarse a efectos de garantizar cualquier derecho que pueda verse afectado por su empleo. Por otra parte, el Gobierno ha aprobado una Carta de Derechos Digitales recientemente, en la que, además de reconocer derechos propios de un entorno en línea, también aboga por la protección de los derechos de las personas como usuarias de las TIC[266], sin olvidar, a su vez, el Título

económicos cuyo reconocimiento reside en el movimiento obrero de aquella época, la necesidad de extender a todas las personas el derecho a la educación, la salud, el trabajo, el sufragio universal etc.; por último, la tercera generación de derechos comenzaron a surgir en el siglo XX, identificados con la coexistencia pacífica, al desarrollo (mediante el impulso a los derechos económicos y sociales) y la protección del medio ambiente. Sin embargo, en esta tercera generación también se incluyen los derechos derivados del extendido uso de las tecnologías o la informática. VAŠÁK, K., "Les différents catégories des droits de l´homme", en LAPEYRE, A., DE TINGUY, F., Y VASAK , K., (Directores), *Les dimensions universelles des Droits de l´Homme*, UNESCO-Bru- ylant, Bruxelles, 1990, p. 297.

[264] LEÓN CAMACHO, J., "Evolución desarrollo de los Derechos Humanos. Hacia una cuarta generación" en *El derecho público y privado ante las Nuevas Tecnologías* en MIRANDA GONÇALVES, R., y DA SILVA VEIGA, F., (Coordinadores), Madrid, Dykinson, 2020, pp. 228-234.

[265] ROIG, A., "E-privacidad y redes sociales", *Revista de Internet, Derecho y Política*, 2009, núm. 9, p. 43.

[266] Carta de Derechos Digitales del Gobierno de España. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022). Para mayor profundización sobre el proceso de elaboración de la Carta de Derechos Digitales, véase DE LA SIERRA, S., "Una introducción a la Carta de Derechos Digitales", en COTINO HUESO, L., (Coordinador) *La Carta de Derechos Digitales*, Valencia, Tirant lo Blanch, 2022, p. 27 y ss. Sin embargo, deseamos destacar que a

X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[267] (en adelante, LOPDGDD). Sí convenimos en que los derechos fundamentales deben recibir una reforzada protección en el nuevo contexto digital a fin de que estos continúen salvaguardados en el nuevo entorno TIC. Sin embargo, ello no supone que deban reconocerse nuevos derechos fundamentales constitucionalmente. En efecto, los derechos fundamentales actuales, continúan protegiendo a los individuos, pero se debe intensificar, por una parte, la labor reinterpretativa de los mismos ante el cambiante paradigma que las TIC predisponen; por otra, se deben garantizar en todo momento herramientas eficaces para su protección en este nuevo entorno digital.

3.2 El desarrollo legislativo del derecho fundamental a la protección de datos personales: la salvaguarda de los datos personales del menor en la normativa española de protección de datos de carácter personal

Hasta la fecha, el ordenamiento jurídico español se ha provisto de tres Leyes Orgánicas de protección de datos de carácter personal. Constituye tarea reservada del presente epígrafe repasar brevemente el largo recorrido hasta la aprobación de la normativa actualmente vigente desde el año 2018 sobre protección de datos de carácter personal.

Por una parte, sobre todo la LORTAD, pero también la LOPD se han visto influenciadas por la discusión constitucional expuesta en el apartado anterior, pues estas normas se aprueban en los años 1992 y 1999 respectivamente, cuando el derecho fundamental a la protección de datos personales no se proclamaba como autónomo e independiente del derecho a la intimidad. Por otra parte, podemos afirmar que todas las leyes orgánicas españolas, se aprueban como consecuencia de compromisos internacionales adquiridos por el Estado español en el sentido que, la LORTAD entra en vigor como consecuencia de la inclusión de España en el *Acuerdo Schengen*, así como con el fin de cumplir con el compromiso adquirido mediante la ratificación del Convenio 108 del Consejo de Europa de adaptar la normativa de protección de datos personales a

pesar de que Italia aprobaba de manera pionera su Carta de Derechos Digitales y el Estado español empleó la misma como referencia, la versión italiana se configura como un texto más reducido, menos detallado en la regulación de las materias y sin valor jurídicamente vinculante.

[267] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Boletín Oficial del Estado, de 6 de diciembre de 2018, núm. 294.

las prerrogativas del texto internacional; la LOPD, por su parte, respondía a la necesidad de adaptar la normativa española a la Directiva 95/46 CE mencionada en el presente estudio. Por último, LOPDGDD adecúa el tratamiento de datos personales nacional al Reglamento General de Protección de Datos europeo (RGPD) citado anteriormente.

Por otra parte, no debe pasar inadvertido que, previo a la aprobación de la LORTAD, al contrario de lo que aconteció en España, gran parte de los países europeos ya contaban con legislación en materia de protección de datos de carácter personal[268]. Por lo que, el legislador español contaba con regulaciones exitosas a su alrededor que pudieran servirle de guía en la labor de aprobación de una norma sobre protección de datos personales.

En otro orden de consideraciones, hasta la aprobación de la LORTAD en el año 1992, el Convenio 108 se posiciona como el único texto legal de referencia en la protección de datos de carácter personal en el ordenamiento jurídico español[269]. De modo que, la normativa nacional tendente a proteger dicho derecho, se encontraba dispersa en el ordenamiento jurídico a través de normas inconexas e incoherentes entre sí. Así las cosas, a través de diversas modificaciones legislativas que se fueron sucediendo en textos legales no relacionados con la protección de datos personales, el legislador español regulaba la materia concerniente a la protección de datos de carácter personal con el Convenio 108 como única referencia y guía en la materia[270].

---

[268] Efectivamente, países como Suecia, Francia, Noruega, Dinamarca, Reino Unido e Irlanda aprobaron sus respectivas normas de protección de datos personales antes de los años noventa. Suecia aprobaba su norma en el año 1973, mientras que Francia, Noruega y Dinamarca lo hacían en 1978. Por último, Reino Unido aprueba su primera norma sobre protección de datos personales en el año 1984. Sobre la Ley sueca como precursora, véase para mayor detalle, FROSINI, V., "Bancos de datos y tutela de la persona", *Revista de Estudios Políticos*, noviembre-diciembre 1982, núm. 30, p. 29.

[269] Mientras el ordenamiento jurídico español no se encontraba provisto de una norma específica sobre protección de datos personales, se recurría a la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, intimidad personal y familiar y propia imagen ante las intromisiones ilegítimas en esos derechos que se cometieran mediante el uso de la informática.

[270] Así, entre otras, la Ley 230/1963, de 28 de diciembre, General Tributaria, Boletín Oficial del Estado, de 28 de diciembre, núm. 313, se modifica por las siguientes leyes: Ley 10/1985, de 26 de abril, Boletín Oficial del Estado, de 27 de abril de 1985. núm. 101; Ley 33/1987, de 23 de diciembre, Boletín Oficial del Estado, de 24 de diciembre de 1987, núm. 307; Ley 4/1990, de 29 de junio, Boletín Oficial del Estado, de 30 de junio de 1990, núm. 256; y Ley 31/1991, de 30 de noviembre, Boletín Oficial del Estado, de 31 de diciembre de 1991, núm. 313, en orden a garantizar una utilización racional de los datos. Con idéntico fin, pero esta vez con el espíritu y finalidad de dotar de protección a datos denominados sensibles, la Ley 30/1984, de 2 de agosto, de Medidas de Reforma de la Función Pública (LOREG), Boletín Oficial del Estado, de 3 de agosto de 1984, núm. 185, recibe una nueva redacción proporcionada por la Ley 23/1988, de 28 de julio, Boletín Oficial del Estado, de 29 de julio de 1988, núm. 181.

A pesar de ello, durante los años ochenta, encontramos iniciativas al fin de adoptar normativa específica de protección de datos de carácter personal que instaban al Gobierno a cumplir con el compromiso adquirido mediante la ratificación del Convenio 108[271]. Con el fin de proporcionar cumplimento a dicho compromiso adquirido internacionalmente, se sucedieron múltiples proyectos legislativos de protección de datos desde 1983. Finalmente, es en 1991 cuando se presenta por el Grupo Socialista el proyecto de Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal que, finalmente recibiría la aprobación de las cámaras[272]. Véase que no fue hasta ocho años después de la ratificación del Convenio 108 y catorce después de la aprobación del art.18.4 CE de la CE cuando el legislador español aborda la tarea de aprobar la LORTAD. En adición a lo expuesto, no fueron pocas las críticas recibidas por la norma que, terminaron conduciendo a la presentación de cuatro recursos de inconstitucionalidad. En efecto, dos de los recursos interpuestos se ventilan por el TC en las sentencias anteriormente citadas en el año 2000.

Además, sobre este punto debemos reseñar que el Convenio 108 resultaba vinculante en España desde 1981, por tanto, también la adaptación necesaria al mismo desde ese mismo momento; sin embargo, esta no ocurrió hasta 14 años después. Huelga decir, que la minoría de edad no se configura como objeto de atención en la normativa de protección de datos personal nacional expuesta. Ni tan siquiera una mención a los más jóvenes en aras de proteger los datos de carácter personal de los mismos.

En otro orden de cosas, la LOPD se considera el resultado de una obligada transposición de la Directiva 95/46/CE ante las múltiples divergencias existentes entre la LORTAD y la Directiva 95/64/CE. Cabe destacar que, a pesar de las críticas y recursos de inconstitucionalidad recibidos por dicha norma, el legislador español se muestra

[271] Propuesta presentada por el Grupo Parlamentario Mixto en CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie D, núm. 20, de 4 de diciembre de 1986.
[272] En ese sentido, cabe destacar la proposición no de Ley de 1984 presentada por el Grupo Parlamentario Popular sobre bases de datos y protección a la intimidad, CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, II Legislatura, Serie D, núm. 47, de 20 de septiembre de 1984; La proposición de Ley sobre protección al honor y a la intimidad de las personas frente a la utilización de las bases de datos, CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie B, núm. 68-1, de 27 de abril de 1987; la proposición de Ley Orgánica del Grupo Parlamentario Mixto-Agrupación IU-EC en 1988 sobre la protección de los derechos y libertades en relación con el uso de la informática y las telecomunicaciones, CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie B, núm. 120-1, de 23 de junio de 1988; y finalmente el único proyecto de Ley Orgánica que se materializó, presentado por el Gobierno Socialista en 1991, CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, IV Legislatura, Serie A, núm. 59-1, de 24 de julio de 1990.

partidario a modificar parcialmente la LORTAD reproduciendo artículos de la misma en la LOPD que constituían objeto de recurso ante el TC. No obstante, en algunos grupos parlamentarios imperaba la idea de que, la normativa sobre protección de datos de carácter personal debía rehacerse[273]. Finalmente, la necesidad de transposición de la Directiva 96/46/CE se saldó con la aprobación de un nuevo texto sobre protección de datos de carácter personal (LOPD) pero que, en esencia, se manifestaba prácticamente en los mismos términos que la LORTAD, artículos recurridos constitucionalmente incluidos[274].

En efecto, la aprobación de la LOPD se presentaba como un momento idóneo de enmendar errores cometidos en la primera Ley Orgánica de protección de datos personales, pero lamentablemente dichas enmiendas no tuvieron lugar. La LOPD ha recibido duras críticas que podrían resumirse en las siguientes: en primer lugar, la LOPD no regula ninguno de los nuevos supuestos que surgen desde 1992; en segundo lugar, no respeta la Directiva 95/46/CE cuya transposición pretendía, que además se llevó a cabo forma tardía y fuera de plazo; en tercer lugar, el consentimiento no se encuentra regulado de manera correcta; y por último, el art.18.4 CE no encuentra reflejo en el texto, ni se define por la LOPD[275].

Al hilo de lo expuesto, destacar que, en efecto, entre los nuevos supuestos que la LOPD no menciona, podemos encontrar la falta de inclusión de la minoría de edad en su articulado. Al igual que la Directiva 95/46/CE, la LOPD guarda silencio sobre dicho extremo, a pesar de que, desde 1995 los nativos digitales comenzaran a poseer gran presencia en la red.

La espera se alarga hasta el año 2007 cuando, el legislador español menciona por vez primera la minoría de edad y visibiliza la necesidad de que se establezca una edad mínima por la normativa para dotar de validez el consentimiento al tratamiento de sus datos personales prestado por un menor. Así, el art. 13 del Real Decreto legislativo 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la

[273] Véase HERRÁN ORTIZ, A.I., "El derecho a la protección de datos personales en la sociedad de la información", *op. cit.*, p. 52.
[274] MURILLO DE LA CUEVA, P. L., "El objeto de la Ley Orgánica de Protección de Datos de carácter personal", en TRONCOSO REIGADA. A., (Coordinador) *Comentario a la Ley Orgánica de Protección de Datos de carácter personal, op. cit.*, p. 77.
[275] HERRÁN ORTIZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales, op. cit.*, p. 197.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal regula los límites al tratamiento de datos personales de los más jóvenes[276]. De un análisis no exhaustivo, pues se dedicará un apartado a su estudio en el presente trabajo, procede traer a colación las tres principales novedades que el Real Decreto Legislativo propugna: la primera reside en el establecimiento de una edad a partir de la cual los menores de edad podrán consentir por sí mismos- sin intervención de sus representantes legales- el consentimiento al tratamiento de sus datos personales, estableciendo la misma en los 14 años[277]. La segunda novedad, reside en el derecho de transparencia e información, pues dispone el art. 13 que, cuando el tratamiento de datos se realice sobre datos de menores de edad, quien lleve a cabo el mismo debe dirigirse al menor en un lenguaje claro y sencillo, además de fácilmente comprensible por estos. Por último, el apartado cuarto del artículo citado impone al responsable del fichero o tratamiento garantizar la comprobación de modo efectivo la edad del menor y la autenticidad del consentimiento prestado por los representantes legales en caso de comprender una edad menor a 14 años. En definitiva, el Real Decreto Legislativo sienta el *Habeas data* de los menores de edad como principal instrumento de protección jurídica de esa esfera de derechos y libertades de los niños y niñas. No debemos olvidar que las informaciones de los menores de edad poseen un carácter especialmente sensible y que, por ello, adquiere especial protagonismo el consentimiento del menor de edad[278].

Sin embargo, la normativa actual sobre protección de datos específicamente dirigida a la minoría de edad, no ha variado en exceso de estas obligaciones que se encontraban vigentes en la normativa desde el año 2007 y ya acusaban una insuficiente garantía para el desarrollo tecnológico de aquel entonces. Desde luego que, el hecho de que la inclusión de la minoría de edad en la normativa sobre protección de datos

[276] Véase el art. 13 del 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, de 19 de enero de 2008, núm. 17.

[277] Antes bien, el presente precepto suscitó múltiples críticas por la doctrina por dos razones principales; por un lado, porque el establecimiento de la edad se llevase a cabo por medio de un reglamento de desarrollo; por otro lado, por la elección de sentar un criterio cronológico en orden a valorar la madurez del menor, pues a juicio de estos, el señalamiento de una edad contravenía las normas generales de capacidad del ordenamiento jurídico, y en especial del art. 162 CC. Véanse así, sobre la primera crítica, VÁZQUEZ DE CASTRO, E., "Protección de datos personales, redes sociales y menores", *op. cit.*, p. 54 y ss. Sobre la segunda crítica, GRIMALT SELVERA, P., "Los menores e internet: capacidad versus protección de la vida privada" en CUENCA CASAS, M., ANGUITA VILLANUEVA, J. A., ORTEGA DOMÉNECH, J., (Coordinadores), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, Madrid, Dykinson, 2013, p. 188.

[278] PÉREZ LUÑO. A.E., "El consentimiento de los menores", en TRONCOSO REIGADA. A., (Coordinador), *Comentarios a la Ley Orgánica de Protección de datos de carácter personal,* Cizur Menor, Thomson Reuters, 2010, pp. 484-485.

personales no haya ocurrido hasta casi treinta años después de la promulgación del art. 18.4 CE no hace más que ratificar la reflexión expuesta en el Capítulo I del presente trabajo: la minoría de edad ha resultado erigirse como la gran olvidada jurídicamente.

En relación con lo expuesto, destacar la reflexión realizada por TRONCOSO REIGADA cuando afirma que, la LOPD establece una disciplina de carácter general que, deberá completarse por disposiciones que lleven sus premisas a ámbitos sectoriales necesitados de regulaciones específicas[279]. Entre dichos sectores, el autor destaca la sanidad, la enseñanza en sus distintos niveles, los procedimientos administrativos, la actuación de las Fuerzas y Cuerpos de Seguridad, las relaciones laborales, Internet y las redes. Sin embargo, nos preguntamos si, no goza de idéntica necesidad completar la específica protección jurídica de la minoría de edad en lo que a la protección de sus datos personales se refiere.

Sobre este particular, huelga recordar que tal y como se expone en el capítulo primero la presente tesis doctoral, en 2015 el legislador español abordó la reforma de la LOPJM, con el fin, entre otros, de adaptarla al nuevo contexto digital que podía presentarse como una amenaza para los derechos de los más jóvenes. En ese sentido, reafirmamos que la reforma de la LOPJM se presentaba como el momento idóneo para completar la normativa sobre protección jurídica de la minoría de edad cuando estos son usuarios de las TIC, de tal suerte que, esta proporcionase una protección suficientemente garantista de su información personal en la red. Lejos del deseo descrito, en la LOPJM no se incluye la regulación adaptada a la minoría de edad del derecho fundamental sobre protección de datos personales, relegando la protección del menor en este ámbito a normas generales como la LOPD en vigente en aquel momento, así como al Código Civil en lo concerniente a la capacidad del menor en relación con los derechos inherentes a la personalidad de los que se le reconoce la titularidad.

Por otra parte, resulta ampliamente conocido que, la LOPDGDD se aprueba con el fin de adaptar el ordenamiento jurídico español al RGPD de la UE sobre protección de datos personales, así como para completar sus disposiciones. Sin embargo, el objeto de la norma, dispone un objetivo más en su exposición de motivos que se corresponde con

[279] TRONCOSO REIGADA, A., "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *op. cit.*, p. 323.

garantizar un catálogo de Derechos digitales, que de manera novedosa se incluyen en Título X (arts. 79 a 97). Así, la inclusión de Derechos digitales ocurre como consecuencia de la enmienda presentada por el Grupo Parlamentario Socialista al Proyecto de Ley Orgánica de Protección de Datos personales[280].

Al igual que ocurrió con la aprobación de sus predecesoras, la LOPDGDD se aprueba con un retraso más que ostensible. Véase que el RGPD se aprueba el 25 de mayo de 2016, con una previsión de entrada en vigor de dos años, esto es, 25 de mayo de 2018. Dicho margen, se proporciona a los Estados miembros a efectos de garantizar un plazo razonable en orden a adaptar las normativas nacionales a las premisas del RGPD, que goza de aplicación directa en los Estados sin necesidad de transposición. En el contexto descrito, lo razonable hubiera consistido en aprobar la LOPDGDD dentro del plazo más que suficiente de dos años concedido por el RGPD hasta su entrada en vigor, circunstancia que no tuvo lugar, pues el Gobierno inició con manifiesta demora la tramitación de la Ley orgánica[281].

[280] Véase cómo el Proyecto de Ley Orgánica de Protección de datos personales inicial no contempla el catálogo de Derechos digitales. CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, XII Legislatura, Serie A, núm. 13-1, de 24 de noviembre de 2017.

[281] El Consejo de Ministros aprueba el 10 de noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, esto es, medio año antes del inicio de la aplicación del RGPD. Esto significa que el Gobierno precisó año y medio para elaborar y tramitar el anteproyecto de ley. A lo recientemente expuesto debemos añadir que la tramitación parlamentaria del Proyecto de ley fue compleja. Tras un intenso debate y numerosas enmiendas, la tramitación de la misma se paralizó debido a la moción de censura al Gobierno aprobada el 1 de junio de 2018. La inestabilidad política del momento y el cambio de Gobierno, desde luego, se configuran como factores que afectaron a la aprobación de la esperada norma. Finalmente, el 18 de octubre de 2018, se aprueba la norma por unanimidad en el Pleno del Congreso de los Diputados el Dictamen de la Comisión sobre el Proyecto de Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales. Poco más tarde, el 21 de noviembre de 2018, el Senado aprueba el texto. Finalmente, el 5 de diciembre de 2018 se aprueba la definitiva LOPDGDD. Para mayor detalle sobre la tramitación de la LOPDGDD véase MARTINEZ VÁZQUEZ, F., "La tramitación parlamentaria de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales" en RALLO LOMBARTE, A., (Coordinador), *Tratado de protección de datos personales: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Valencia, Tirant lo Blanch, 2019, pp. 53-79. A modo de resumen, los trámites prelegislativos de la norma comenzaron los días 7 y 8 de febrero de 2017 con la consulta pública de la misma. En este contexto, se presentaron 34 aportaciones de relevantes corporaciones, asociaciones, despachos de abogados etc. Así mismo, tras el nombramiento de la ponencia presidida por Piñar Mañas, se eleva una propuesta de Ley orgánica el 19 de mayo de 2017, que se eleva por el Consejo de Ministros el 23 de junio de 2017. Finalmente, la remisión del proyecto de ley al Congreso tuvo lugar el 14 de noviembre de 2017. A continuación, comenzó la tramitación parlamentaria de la ley orgánica, recibiendo esta únicamente la oposición total al proyecto del partido catalán Partit democrata catalá, oposición que no prosperó tras el debate planteado el 15 de febrero de 2018. Así las cosas, continuando con el íter de aprobación de la norma, se sucedieron varias comparecencias de expertos, entre las que se encontraban la de la directora de la AEPD. En la fase de presentación de enmiendas, se presentaron 368 enmiendas (entre las que destacamos la inclusión del Título X por parte del Grupo socialista ya mencionada). Sin embargo, cabe destacar que el debate sobre las discrepancias se sucedió de modo informal, lo que sin duda alguna permitió al proyecto ganar mayor celeridad en su aprobación dada la cercanía de la fecha de entrada en vigor del RGPD. El informe de ponencia se sometió a debate y votación por la Comisión de Justicia del Congreso de los Diputados en la

Otro de los aspectos controvertidos en la tramitación y aprobación de la LOPDGDD reside en margen de apreciación que el RGPD posibilita sobre determinadas materias. Tal y como se ha dispuesto en apartados anteriores de la presente investigación, uno de los motivos que impulsa a la UE a inclinarse por el Reglamento como instrumento normativo reside en la no necesidad de transposición de la normativa europea a los Estados nacionales. Dicha elección vino motivada por las no pocas divergencias que existían en la regulación de la materia de los Estados miembros ocasionadas por el margen que la Directiva 95/64/CE concedía. Con todo, el Reglamento no precisa de transposición, pero sorprendentemente en determinadas materias, permite a los Estados miembros llevar a cabo previsiones normativas[282]. Así las cosas, el deseo armonizador del RGPD queda en ocasiones desvirtuado al permitir a los diversos Estamos miembros, continuar regulando aspectos normativos en el tratamiento de datos de carácter personal de modo diferente. Destacamos la reflexión de TRONCOSO REIGADA cuando afirma que se pasa de una Directiva que permite una flexibilidad formal a un Reglamento flexible en lo material[283].

Concretamente, una de las materias en las que permite dicho margen de apreciación la constituye la relativa al consentimiento de los menores de edad y autorización parental. De este modo, los Estados podrán disponer la edad a partir de la cual los menores pueden prestar el consentimiento al tratamiento autónomamente. Así las cosas, dicho margen de apreciación propició divergencias en el seno de la tramitación parlamentaria de la LOPDGDD, especialmente en lo relativo la elección de la edad mínima a partir de la cual, los menores podrían prestar consentimiento válido. Cabe destacar, que la edad finalmente establecida por la LOPDGDD se corresponde con los 14 años de edad, mientras que el RGPD fija la edad en 16 años, pero dispone de una horquilla

sesión de 10 de octubre de 2018. Y finalmente, el pleno del Congreso aprobó la norma en la sesión de 18 de octubre de 2018 y el senado el 21 de ese mismo mes y año. A las consideraciones expuestas, debemos añadir que el Gobierno se encontró en funciones desde el 20 de diciembre de 2015 al 29 de octubre de 2016, no contando con iniciativa legislativa en dicho lapso de tiempo. Sin embargo, podía haber avanzado en la elaboración del anteproyecto de ley para no demorarse injustificadamente una vez más en la materia. TRONCOSO REIGADA, A., "La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías Digitales", *Derecom,* marzo-septiembre 2019, núm. 26, p. 138.

[282] Otras materias en las que también se posibilita dicho margen de apreciación son: sanidad, relaciones laborales, tratamientos de categorías especiales de datos por razones de interés público, tratamientos de datos genéticos, biométricos o datos de salud y las habilitaciones legales para la legitimación del tratamiento.

[283] TRONCOSO REIGADA, A., "La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías Digitales, *op. cit.,* p. 134.

entre 13 y 16 años a determinar por los Estados miembros. Sin embargo, el establecimiento de dicha edad- 14 años- no recibe el respaldo de la totalidad de los grupos parlamentarios. El Grupo Parlamentario Confederal de Unidos y Podemos presentaban una enmienda al establecimiento de dicha edad, proponiendo mantenerla en 16 años, tal y como apunta el RGPD, entendiendo que no ha lugar a rebajar dicha edad habida cuenta de que la propia normativa europea establece dicho límite[284].

De la lectura de dicha enmienda destacan determinadas conclusiones relevantes a nuestro parecer que deben exponerse en el presente apartado. Por una parte, los grupos parlamentarios firmantes insisten en que, la rebaja de la edad dispuesta por el RGPD- 16 años- a los 13 años (propósito inicial de legislador español) ha de calificarse de injustificada. En ese sentido, una de las razones expuestas por el legislador en aras de justificar dicha elección, reside en afirmar que, otros países de nuestro entorno establecen la edad mínima en 13 años[285]. De conformidad con los grupos firmantes de la enmienda, dicho razonamiento resulta paradójico si se toma en consideración que, el deseo del RGPD reside en que la edad de todos los Estamos miembros se establezca en los 16 años de edad, sin perjuicio de que permita a los Estados decidir rebajarla[286]. Por otra parte, la enmienda presta especial atención en el interés superior del menor, que debe imperar sobre los intereses del mercado y las empresas que, no en pocas ocasiones poseen intereses lucrativos diferentes a los que inicialmente se disponen. Por último, destacan su descontento, que compartimos, al afirmar que no cabe aceptar que el proyecto escoja sin justificación suficiente el menor nivel de protección permitido por el Reglamento, pues, efectivamente ello entra en colisión con el principio de interés superior del menor que debe anteponerse en todo momento.

En efecto, la edad de 13 años, e incluso 14 años de edad, se antoja un límite insuficiente para proteger a los más jóvenes, especialmente, cuando utilizan plataformas *online*. La gran magnitud de datos que con distintos fines tratan estas empresas coloca a los más jóvenes en una posición de indefensión que, a dicha edad son incapaces de comprender tal y como se verá en el siguiente capítulo del presente trabajo. Afirmamos

[284] Boletín Oficial de las Cortes Genera*les*, XII Legislatura, Serie A, 13-2, enmienda núm. 5, de 18 de abril de 2018, p. 6.
[285] La afirmación desde luego, carece de fundamentación suficiente, en el sentido que, es cierto que Portugal establece la edad mínima en 13 años de edad también, pero estados como Francia disponen que la edad mínima se situará en los 15 años de edad.
[286] Dicho razonamiento se deduce de manera clara de la lectura del art. 8 del RGPD de la UE cuando establece que los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

así que, en la elección de la edad mínima para prestar el consentimiento por parte de los menores, ha parecido primar el interés de los prestadores de servicios al interés superior del menor en aras de su protección como sujeto especialmente vulnerable. No podemos sino compartir todos y cada uno de los argumentos expuestos en la enmienda planteada por los grupos parlamentarios señalados anteriormente.

No obstante, reconocemos la voluntad de abordar la materia pues, tras 18 años del reconocimiento del derecho autónomo a la protección de datos personales, la minoría de edad, finalmente posee acomodo en nuestro ordenamiento jurídico en una Ley orgánica. Así las cosas, la LOPDGDD regula los siguientes aspectos relativos a la minoría de edad y los tratamientos de datos personales: la edad mínima para prestar consentimiento válido (art. 7), la adaptación del ejercicio de los derechos ARCO a la minoría de edad (art. 12.6 º) y, por último, las Garantías Digitales concernientes a menores (arts. 84 y 92). De una primera lectura, advertimos que, el principio de transparencia no menciona la minoría de edad, mientras que el RGPD sí menciona dicho aspecto, por lo que, en dicho supuesto, el art. 12.1º. del RGPD resultará de aplicación directa en el estado español.

Al tratarse pues, la LOPDGDD una norma orientada a la adaptación del ordenamiento jurídico español al RGPD, nos remitimos pues a gran parte de las afirmaciones realizadas en el apartado 2.4.2 del presente capítulo sobre las novedades en materia de menores introducidas por el RGPD.

Tras prácticamente tres décadas desde que se reguló el tratamiento de datos personales en España por primera vez y poco más de una década desde la verdadera irrupción imparable de las TIC, finalmente la minoría edad, colectivo que más emplea estas herramientas, recibe protección en una Ley orgánica sobre protección de datos personales. A pesar de que, destaquemos la positividad de dicho esfuerzo, no podemos inadvertir que el mismo llega con manifiesta demora. Los más jóvenes llevan muchos años, aproximadamente desde 1995, empleando estas herramientas especialmente peligrosas para su privacidad, sin ningún tipo de protección jurídica específica dada su especial situación de vulnerabilidad hasta el año 2007. Cabe añadir que, la Disposición Adicional 19ª de la LOPDGDD informa de que el Gobierno aprobará un proyecto de ley dirigido a garantizar los derechos de los menores ante el impacto de internet, sin embargo, aunque esperamos se apruebe sin la habitual demora con la que el legislador regula la

materia relativa a la protección de datos personales, todavía no parecen haberse iniciado los trámites a tal efecto.

CAPÍTULO III:

EL TRATAMIENTO DE DATOS PERSONALES DEL MENOR COMO USUARIO DE REDES SOCIALES. DIFICULTADES LEGALES EN LA CONFIGURACIÓN EN LÍNEA DEL CONSENTIMIENTO AL TRATAMIENTO OTORGADO POR MENORES DE EDAD

La protección de datos personales como derecho fundamental de tercera generación estrechamente relacionado con el nuevo paradigma digital, se erige como uno de los derechos fundamentales más presentes en el contexto *online*. No obstante, este nuevo mundo interconectado en el que se ha producido un éxodo desde lo analógico hacia lo digital, supone la aparición de nuevos riesgos para la salvaguarda de los datos de las personas. En este devenir, los peligros que las TIC proyectan sobre los datos personales, se acentúan cuando el usuario de estos servicios es menor de edad. En efecto, los jóvenes crecen inmersos en el pleno empleo de dispositivos conectados a la red, entre los que destacan los *Smartphone* de última generación con conexión a Internet.

Los *digital babies*, se entretienen y comunican mediante el teléfono móvil con una habitualidad sin precedentes. Concretamente, las redes sociales se convierten en las plataformas favoritas de estos jóvenes en orden a saciar sus necesidades de entretenimiento y comunicación. Ahora bien, la falta de madurez de estos, unida al modo de funcionar de estas plataformas, entre otros, les expone a unos riesgos para su información personal que habitualmente no perciben.

1. DE LA WEB 1.0 A LA WEB 4.0: LA IRRUPCIÓN DE LA WEB 2.0 COMO UN NUEVO MODO DE RELACIONARSE

La Web 2.0 o web social, constituye una nueva y revolucionaria forma de obtener información, comunicarse, así como expresarse fuertemente arraigada en nuestra vida cotidiana[287]. Este fenómeno, ha dejado atrás la consideración de Internet como un espacio pasivo y estático en el que el usuario no participa ni colabora. En efecto, en la antigua Web 1.0, Internet se mostraba como un gran portal informativo abierto al mundo, pero en el que los usuarios del mismo no colaboraban de manera activa, limitándose únicamente a la búsqueda de información. Las principales características de esta web, que se presentaba como un escaparate al usuario, se exponen como sigue: las páginas web se mostraban estáticas al usuario, esto es, este no podía interactuar de forma alguna con ellas; por otra parte, la renovación de contenidos resultaba poco frecuente, dado que ello implicaba un gran esfuerzo; por último, no se hallaban herramientas de comunicación en

[287] Tal y como se ha expuesto en apartados precedentes, el término Web 2.0 se emplea por primera vez por TIM O´REILLY en 2004.

línea entre el titular de la página web y los usuarios de esta, aportando una falta de dinamismo a la interacción de contenidos[288].

En la actualidad, la situación resulta manifiestamente diferente. Los servicios que la Web 2.0 puede ofrecer al usuario, además de resultar muy variados, convierten a este en partícipe activo de dicho universo, permitiéndole colaborar, opinar, editar contenido en tiempo real, además de continuar considerándose un consumidor de información.

En el contexto descrito, las redes sociales se erigen como la herramienta de mayor éxito de la Web 2.0; si bien la gran irrupción de estas plataformas podemos situarla aproximadamente en el año 2008, la primera red social nace en el año 1995[289]. Desde entonces, la popularidad de estos espacios virtuales ha crecido exponencialmente. Mientras que el nacimiento de redes sociales que todavía en la actualidad revisten popularidad podemos datarlo como sigue: en el año 2002 nace la red social MySpace, en 2005 Yahoo!360º, o por ejemplo, en el año 2007 Facebook[290], desde 2020 el número de estos servicios resulta muy elevado y aumenta diariamente[291]. Estos espacios virtuales, principalmente orientados al ocio, instan al usuario a compartir aspectos relacionados con la vida privada como vídeos, imágenes, escuchar música, compartir opiniones etc. En la actualidad, resulta posible encontrar pareja, trabajo, nuevas amistades e incluso trabajar en grupo desde distintas zonas del planeta por medio de estas plataformas. Efectivamente, el objetivo de las redes sociales reside en conseguir que sus miembros utilicen el medio *online* para convocar actos y acciones que influyan en el mundo *offline*[292].

---

[288] Véase al respecto AGUSTINOY GUILAYN, A., Y MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales*, Barcelona, Boch editor, 2021, p. 19.

[289] No obstante, la primera Red social nace en el año 1995 bajo la denominación de *Classmates*. La finalidad de dicha plataforma reside en poner en contacto a personas de un mismo colegio una vez este ha finalizado. DAVARA FERNÁNDEZ DE MARCOS, L., "Régimen jurídico de las redes sociales", en CAZURRO BARAHONA, V., (Coordinador), *Derecho digital, Perspectiva interdisciplinar*, Barcelona, Boch editor, 2017, p. 204.

[290] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), p. 35.

[291] A día de hoy, existen aproximadamente más de 40 redes sociales. IEBS SCHOOL. "Las redes sociales más utilizadas: cifras y estadísticas", de 9 de diciembre de 2020. Obtenido de: https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/#:~:text=Lideran%20el%20ranking%20de%20redes,49%25%20a%20un%2054%25). (última consulta 5 de mayo de 2021).

[292] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), p. 39

Así, la importancia de las redes sociales, resulta proporcional al número de millones de perfiles de usuarios que estas poseen. Nadie discute en la actualidad su fuerte penetración en el modo de socializar de las personas; en ese sentido, el 88% de la población española es usuaria de alguna red social[293]. Su gran atractivo reside en la posibilidad que estas ofrecen a las personas de cualquier parte del mundo para conocerse, compartir información y contenido a tiempo real, interaccionar con amigos y familiares que residen en distintos países, etc. A causa de estos nuevos comportamientos, se ha entablado una comunicación desinhibida de todo tipo información personal a una escala sin precedentes. Desde luego, la información es lo que mueve Internet, ya que, a mayor dinamismo por parte de los internautas, mayor riqueza poseerán los proveedores de servicios de la sociedad de la información. Sin embargo, este constante flujo de información a gran escala, constituye un reto para la protección jurídica de la vida privada de las personas. Efectivamente, nunca en la historia se ha intercambiado un volumen de datos tan elevado en tiempo real entre personas usuarias de estos servicios, lo que, inevitablemente ocasiona importantes riesgos para la privacidad e intimidad de los usuarios de los mismos, así como para los datos personales de estos.

El cambio de paradigma resulta más que destacable, en el sentido que, se ha evolucionado de proteger a las personas de las intromisiones que en su vida privada pueden llevar a cabo terceros a, incitadas por estas plataformas, ellas mismas desvelen cantidad ingente de información personal a efectos de socializar virtualmente. En nuevos hábitos, los *digital babies*, se presentan como una nueva generación que ha crecido inmersa en este nuevo mundo interconectado desde su niñez. En épocas anteriores, el universo del menor se encontraba condicionado por espacios de relación realmente reducidos como podían considerarse su domicilio, el colegio, el barrio, su ciudad o pueblo; sin embargo, a día de hoy el empleo de Internet y las redes sociales les concede un ámbito de relación a escala mundial, de un número prácticamente ilimitado de informaciones, conocimientos y nuevas experiencias[294]. Consecuentemente, esta generación de jóvenes, se siente cómoda navegando por la red de manera constante y compartiendo segundo a segundo detalles sobre su vida privada en las redes sociales. El

[293] IAB SPAIN., "Estudio de redes sociales 2022". Obtenido de https://iabspain.es/estudio/estudio-de-redes-sociales-2022/ (última consulta 4 de enero de 2023).
[294] PÉREZ LUÑO, A.E., "La protección de los datos personales del menor en Internet", *Anuario de la Facultad de derecho de Alcalá II*, 2009, núm. 2, p. 153.

nuevo contexto digital se presenta como una herramienta con innumerables ventajas, entre ellas, los jóvenes pueden ampliar sus fuentes de estudio, colaborar con mayor facilidad en la consecución de sus tareas escolares, etc[295].

Sin embargo, frente a las ventajas, también se presentan riesgos para la privacidad. El teléfono móvil se constituye como un nuevo espacio de ocio para los jóvenes internautas, que utilizan para publicar opiniones en Twitter, compartir fotografías en Instagram, realizar videos en TikTok o simplemente entretenerse con vídeos de YouTube, entre otros, desde cualquier lugar y a cualquier hora. Lo único que necesitan es una conexión a Internet, así como el terminal para poder socializar o entretenerse con amigos y amigas. En efecto, las redes sociales se configuran como una plataforma aparentemente gratuita, en el sentido que, no requiere de una contraprestación monetaria a cambio de la utilización del servicio. Ahora bien, los internautas generan un rastro económicamente rentable que constituye la fuente de riqueza de los proveedores de servicios de redes sociales. El excelso volumen de datos personales facilitado a través del uso habitual de estos servicios, revela los gustos, preferencias, hábitos, ideología… de las personas internautas sin gran esfuerzo[296].

Así las cosas, el verdadero negocio de los proveedores de redes sociales reside en el tratamiento de la información de los millones de personas usuarias en orden a facilitar a las empresas de publicidad, marketing y venta directa, entre otras; pues los datos personales compartidos por estos en sus plataformas, desvelan rasgos de la personalidad de los usuarios[297]. Dicha información se emplea por las empresas de publicidad,

---

[295] El uso adecuado de Internet trae consigo innumerables ventajas. Para GARCÍA MARTÍN permite una capacidad de expresión y de comunicación prácticamente ilimitada, se pueden practicar nuevos idiomas, familiarizarse con causas solidarias o entretenerse jugando a juegos *online*. GARCÍA MARTÍN, I., "Aspectos psicológicos de la influencia de Internet en el libre desarrollo de la personalidad del menor", *Menores e Internet*, Cizur menor, Aranzadi, 2013, p. 3. Ahora bien, a nuestro juicio, no todas las actividades mencionadas merecen el calificativo de ventajas. Efectivamente, la posibilidad de entablar una comunicación ilimitada, también puede considerarse un riesgo especialmente en el caso de menores internautas. Lo mismo ocurre con la práctica de juegos *online*. Por otra parte, cabría añadir como ventajas, la consideración de Internet como fuente prácticamente infinita de información y conocimiento para los menores de edad en el ámbito académico (siempre que se emplee responsablemente) o incluso las facilidades que esta herramienta brinda para el acceso a la cultura desde la comodidad del hogar.

[296]Así las cosas, en 2015 HEREDERO CAMPO auguraba que determinado sector aventuraba la versión 4.0 o Web predictiva; ahora, en 2023, la misma se ha convertido en una realidad. HEREDERO CAMPO, Mª T., "Evolución tecnológica y derecho al olvido digital, desde sus inicios a la actualidad", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información*, Granada, Comares, 2015, p. 71.

[297] El principal uso de profesionales y empresas en las redes sociales se orienta a la venta de productos y servicios. Aproximadamente un 75% de los profesionales venden por medio de redes sociales. IAB SPAIN., "Estudio de redes sociales 2020". Obtenido de: https://iabspain.es/sin-acceso/download-id/39688/ (última consulta 24 de marzo de 2021).

marketing y venta directa para ofrecer a las personas usuarias productos y servicios que puedan resultar de su interés dependiendo de la personalidad y gustos de cada una de ellas. Tales son los avances, que la doctrina ya menciona una evolución hacia la web 4.0 o semántica[298].

En relación con lo expuesto, nos encontramos en una nueva economía cuya base reside en la información. Los bienes, servicios e información ahora se consumen a través de la red, lo que ha conducido a un éxodo hacia Internet de la actividad humana en varias de sus facetas: política, entretenimiento, salud, ventas, etc. No podemos sino compartir las palabras de PÉREZ LUÑO cuando asegura que la intimidad en la sociedad de la información y del consumo, se ha tornado en muchas ocasiones una mercancía, cuyo valor se determina en virtud de las leyes de la oferta y de la demanda[299].

En el entorno descrito, mantener la privacidad de las personas resulta una tarea ardua y complicada, máxime si dichos internautas no alcanzan la mayoría de edad, pues, su falta de madurez les conduce, alentados por la red social, a compartir más información privada (propia e incluso de terceras personas) sin ningún tipo de control y sin verdadera conciencia de lo lesivas que pueden llegar a resultar dichas conductas para sus derechos fundamentales. Ciertamente, los menores de edad actúan con un manifiesto exceso de confianza en este ámbito al mostrarse demasiado colaboradores y proactivos con la publicación de información personal. Ello se debe, a que los jóvenes integran las redes sociales en su propio entorno personal[300], comportándose en las mismas con una sensación de anonimato e impunidad que los incita a adoptar un comportamiento que en el mundo analógico no se atreverían; sin embargo, las redes sociales no son la vía pública: pueden amplificar de manera incontrolable la información publicada, además de tratar, recopilar, estructurar, ceder etc. a terceros dicha información.

[298] HERNÁNDEZ, A., Y KÜSTER, I., "Brand impact on purchasing intention. An approach in virtual social networks channels", *Economics and bussines letters,* núm. 1(2), p. 1 a 9.
[299] PÉREZ LUÑO, A.E., "La protección de los datos personales del menor en Internet", *op. cit.*, p. 150.
[300] En efecto, las TIC constituyen un elemento natural en la vida de los menores de edad, en particular, de la generación *digital babie*. GETE-ALONSO Y CALERA, Mª.C., "Los derechos del menor y personas discapacitadas en el entorno digital", en MARTÍNEZ VÁZQUEZ DE CASTRO, L., (Director) y ESCRIBANO TORTAJADA, P., (Coordinadora), *Internet y los derechos de la personalidad*, *Internet y los derechos de la personalidad*, Valencia, Tirant lo Blanch, 2019, p. 277-278.

2. EL IMPACTO DE LAS REDES SOCIALES *ONLINE* EN LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL DEL MENOR

Los tratamientos de datos personales constituyen el elemento necesario de las redes sociales[301]. Los beneficios del proveedor provienen de la explotación de la información personal que los usuarios comparten diariamente. Por ello, resulta fundamental conocer el funcionamiento de estas plataformas para poder comprender el impacto que dicha dinámica puede suponer sobre los datos personales de las personas usuarias de dichos servicios, especialmente si estas son menores de edad. En ese sentido, solamente alcanzando cierto grado de conocimiento sobre el funcionamiento de estos servicios, podremos atisbar y limitar la potencial peligrosidad de los mismos, en especial para los más jóvenes.

2.1. Concepto, tipología y funcionamiento de redes sociales *online*

2.1.1. A vueltas con el concepto de red social

Se definen las redes sociales *online* como plataformas de comunicación en línea que facilitan a los usuarios de las mismas crear redes en las que se comparten intereses comunes[302]. De manera más detallada, las redes sociales se configuran como Servicios de la Sociedad de la Información que ponen a disposición de sus usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, creen y editen su propio contenido en línea, como publicar fotografías, vídeos, crónicas, comentarios, música etc., y en definitiva, generen una red virtual en la que existe una vinculación entre usuarios. Ahora bien, dicha vinculación puede alcanzar un grado máximo como consecuencia de los enlaces en cadena que se suceden con el fin de potenciar la incorporación de nuevos usuarios a la plataforma.

Esta última afirmación hunde sus raíces sobre la idea de que el número de conocidos crece exponencialmente con la cifra de invitaciones en cadena, precisando de pocos enlaces para que el conjunto de conocidos se convierta, a juicio de WATTS en toda la población del planeta[303]. Ejemplo práctico de ello constituye la clausurada red social

[301] MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, p. 95.
[302] Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, de 12 de junio de 2009, WP 163, p. 5.
[303] Esta idea se expuso por primera vez por FRIGYES KARINTHY y fue recogida en la obra de DUNCAN WATTS sobre *Six Degrees: the science of a connected Age*. Nueva York, W.W. Norton & Company, 2004.

española Tuenti[304]. El acceso a la mencionada plataforma, solamente podía efectuarse con invitación de una persona que ya fuera usuaria de Tuenti. Así, las primeras cinco invitaciones de acceso al servicio, se compartieron por los 5 socios fundadores de la misma, sin embargo, los usuarios de Tuenti crecieron exponencialmente hasta alcanzar los 8 millones de personas usuarias en toda España[305]. Se reafirma así la idea de que, se necesitan unos pocos enlaces para generar verdaderas redes de contactos interconectados todos ellos entre sí. En consecuencia, la información publicada resulta susceptible de alcanzar difusión máxima en el contexto descrito.

Sin embargo, las redes sociales no constituyen plataformas puestas a disposición de las personas de manera altruista para facilitar su interacción social. Estas generan gran parte de sus ingresos con la publicidad que las empresas anunciantes difunden en los perfiles web de los usuarios. La relación de causalidad entre ambas circunstancias resulta evidente en el sentido que todos los datos- muchos de ellos sensibles-, que los usuarios comparten en sus perfiles diariamente, ofrecen a la red social la posibilidad de lograr un mercado segmentado que a posteriori, se compartirá con empresas de publicidad, marketing o anunciantes. Así, estas últimas dirigen su publicidad de manera directa, específica y personalizada basada en los datos que la red social ha compartido con ellos sobre sus usuarios.

En el contexto descrito, el usuario asume un doble papel en su actividad en línea: por una parte, como creador de contenido, pues los propios usuarios ponen a disposición de la red social numerosos datos cualitativos y cuantitativos, propios y ajenos con la información que publican en sus perfiles relativa a la edad, sexo, localización, intereses y preferencias; y por otra, también asume la condición de consumidor, pues el verdadero negocio de la red social se asienta sobre la publicidad y marketing que terceras empresas anunciantes realizan en la plataforma, siempre basada en la información personal de los usuarios que, previamente las plataformas han compartido con estas empresas[306]. En

[304] La red social Tuenti fundada en 2006 y con dirección www.tuenti.es , se constituye como la primera red social española cuyo fin residía en fomentar la interacción social entre jóvenes. MARTOS DÍAZ, N., "Las políticas de privacidad, Redes sociales y protección de datos. El problema de la verificación de la edad", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores) *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, p. 147-148.

[305] *Idem.*

[306] Tal y como establecen AGUSTINOY GUILAYN y MONCLÚS RUIZ, el usuario de la Web 2.0 recibe el calificativo de "prosumidor", dado que, ya no solamente "consumen" contenidos *online*, sino que además

efecto, las redes sociales se posicionan como un espacio retroalimentado en el que la información personal de los millones de personas usuarias se presenta como un presupuesto indispensable para su negocio. A mayor número de interacciones en la red, mayor resultará el rastro de información disponible para su segmentación y posterior cesión de dichos datos a las empresas anunciantes. Una vez finalizados estos pasos, las empresas anunciantes disponen de los detalles personales suficientes para redirigir su publicidad a las personas usuarias de la red social[307].

Otro aspecto a valorar se halla en el incremento en el uso de redes sociales causado por la aparición de los teléfonos móviles *Smartphone,* pues estos dispositivos permiten la conexión en cualquier momento y en cualquier lugar. Tal y como se ha señalado, el teléfono móvil se convierte en una extensión del espacio de ocio, especialmente para los más jóvenes, a los que les resulta atractivo acceder a las redes sociales desde cualquier lugar y en cualquier momento para compartir su variada información. De acuerdo con ORTIZ LÓPEZ, la aparición de estos dispositivos y sus mencionadas características (ubicuidad e inmediatez), han incrementado las posibilidades de que las redes sociales impliquen riesgos adicionales para la privacidad de las personas[308]. Efectivamente, el acceso a estas plataformas puede resultar constante y ello ocasiona que la facilidad para desvelar información personal para su posterior tratamiento exhaustivo por la red social resulte todavía mayor.

Por todo lo expuesto, debemos apuntar que la definición tradicional de redes sociales como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes ha quedado manifiestamente obsoleta. Refuerza dicho argumento el hecho de que las redes sociales no actúan como una herramienta cuyo fin reside única y exclusivamente en proporcionar un soporte digital para socializar; sino algo mucho más complejo, considerándose un espacio

también contribuyen a su producción. AGUSTINOY GUILAYN, A., Y MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales, op. cit.*, p. 19.

[307] PLATERO ALCÓN coincide con el planteamiento expuesto cuando afirma que la actividad de las redes sociales no se identifica con facilitar el contacto con otros usuarios a título lucrativo, sino que reside en obtener un beneficio económico a través del desarrollo de una actividad publicitaria, traficando con los datos de sus usuarios. PLATERO ALCÓN, A., *El derecho al olvido el internet. La responsabilidad civil de los motores de búsqueda y las redes sociales: estudio doctrinal y jurisprudencial*, Madrid, Dykinson, 2021, p. 172.

[308] ORTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales,* Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, p 25.

retroalimentado en el que la información se posiciona como el elemento nuclear de su funcionamiento.

Por ello, entendemos que, tras aproximadamente una década desde la irrupción de estos espacios *online*, esta circunstancia debe reflejarse en la definición de estas plataformas. En efecto, la principal definición de la que se sirve la doctrina desde hace una década y recogida en la presente tesis doctoral- ante la ausencia de una definición actualizada- debe evolucionar incorporando esta nueva actividad que se desempeña en las redes sociales: la práctica de publicidad y mercadotecnia directas desde la recogida y tratamiento masivo de datos personales de usuarios de la red social.

Por otra parte, resulta de especial interés analizar los tipos de redes sociales al alcance de los usuarios actualmente. Así, podemos encontrar diversos tipos de redes sociales empleadas por diversas generaciones y para diferentes finalidades. Así, hallamos tres grandes grupos que, a pesar de compartir determinadas características, poseen elementos particulares que las diferencian.

El primer grupo de redes sociales, lo constituyen las redes sociales de comunicación o también conocidas como redes sociales generalistas o de ocio (Facebook, Instagram, TikTok, entre otras). En estos espacios, toda vez que los usuarios hayan creado su perfil personal, pueden publicar fotografías, vídeos, opiniones, preferencias, ideología de todo tipo propia y de terceras personas, comunicarse mediante mensajería instantánea o chat etc. Además, entre estas, destacan al considerase las más empleadas, las redes sociales que invitan al usuario a la construcción de un perfil[309].

El segundo grupo, lo conforman redes sociales especializadas. Estas, se centran en un eje temático concreto con la finalidad de predisponer la interacción entre colectivos que comparten determinados intereses (fotografía, viajes etc.). Como ejemplos de este tipo de plataformas podemos mencionar las redes sociales Pinterest, Twitter o Meetic, entre otras.

Finalmente, el último grupo de redes sociales lo conforman las redes sociales profesionales. En estas, las personas usuarias pueden buscar nuevas oportunidades de

[309] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales *online*, febrero de 2009, p. 42. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2009).

empleo, así como practicar *networking* con compañeros de trabajo o del sector mediante contactos comunes de confianza. Destaca en este grupo la plataforma LinkedIn con un modelo de financiación basado en la oferta de servicios *Premium* a las personas usuarias, además de la realización de campañas publicitarias personalizadas.

A pesar de la gran variedad de redes sociales descritas, la presente investigación se centra en las redes sociales de comunicación también conocidas como generalistas o de ocio por dos motivos principalmente; por una parte, los menores se encuentran especialmente presentes en este tipo de redes sociales; por otra parte, las redes generalistas o de ocio albergan un mayor nivel de riesgo que el resto de redes sociales, ya que, los usuarios no se limitan a exponer sus datos de contacto o información profesional, sino que habitúan a exponer de manera pública experiencias, vivencias, gustos e incluso ideología, lo que acarrea que el volumen de datos de carácter personal puestos a disposición del público resulte mayor que en los tipos de redes sociales restantes.

2.1.2. La experiencia del usuario de redes sociales y el tratamiento de sus datos personales. Un reto para el ordenamiento jurídico

El funcionamiento de las redes sociales se estructura en tres fases que pueden identificarse como sigue: un primer momento presidido por el registro en la plataforma, un segundo momento que se asocia con la utilización de la red social, por último, la baja de estos servicios o cancelación de la cuenta[310].

La comprensión de las vicisitudes de dichas fases resulta de trascendental relevancia, ya que los riesgos a los que los datos personales pueden exponerse con el manejo de redes sociales se antojan diversos, conforme el usuario se sitúe en una fase u otra. De este modo, las normas garantes del derecho a la protección de datos personales, han procurado proteger la información personal de los usuarios de redes sociales mediante el establecimiento de determinadas obligaciones jurídicas sobre tratamiento de datos personales que inciden en cada una de las mencionadas fases. No obstante, nos preguntamos si dichas obligaciones jurídicas se cumplen de manera efectiva por los proveedores de dichos servicios. Con el fin de proporcionar una respuesta que valore la suficiencia de garantías jurídicas en apartados posteriores, es preciso exponer las

[310] En ese sentido, véase la valiosa aportación de ORTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, *op. cit.*, p 26.

principales características de cada una de las tres fases implicadas en el funcionamiento de las redes sociales.

En una primera fase, la relación entre el usuario y el proveedor del servicio de la red social comienza en el momento del registro, paso también conocido como "darse de alta en la red social". Esta fase inicial, indispensable para convertirse en usuario del servicio, comienza con la solicitud de datos personales básicos como nombre, apellidos, dirección de correo electrónico, sexo y edad[311]. A estos datos personales, debemos añadir que también cabe la posibilidad de incluir una fotografía del futuro usuario para la construcción inicial del perfil. Queda de manifiesto que la relación entre usuario y proveedor nace con el tratamiento de datos personales desde el comienzo; puesto que estos datos identificativos se tratarán por la red social durante la consecución de la relación entre ambas partes. De hecho, a nuestro juicio, una de las claves que potencian la peligrosidad de las redes sociales para la información privada de las personas reside en que el usuario se identifica con sus verdaderos nombres y apellidos, vinculando la información que comparte en la red a su identidad[312].

En esta fase, previa a la utilización de la plataforma, constituye requisito indispensable la aceptación de las políticas de privacidad previamente diseñadas y redactadas por el proveedor de la red social. Sin ánimo de profundizar, pues no es objeto de estudio del presente epígrafe, el objetivo de estas políticas debiera consistir en informar al usuario del destino de los datos personales, pues no olvidemos que el usuario debe poseer en todo momento el control sobre su información personal. Por último, tal y como quedará de manifiesto más adelante, los riesgos de la presente fase se identifican con la ausencia de información incorporada en las políticas de privacidad, así como una incorrecta configuración de la privacidad del perfil por parte del usuario como consecuencia de dicha desinformación.

---

[311] La red social Facebook solicita los siguientes datos: nombre, apellidos, sexo, fecha de nacimiento y correo electrónico. Véase en la página de registro de la red social: https://es-es.facebook.com/ . Otras redes sociales como Instagram, solicitan el número de teléfono, nombre, apellidos y correo electrónico. Véase en la página de registro de Instagram: https://www.instagram.com/accounts/emailsignup/?hl=es (última consulta el 2 de noviembre de 2021).

[312] Antes bien, ello no apareja que deba fomentarse la participación por medio de un alias en estos espacios, ya que, la ocultación del verdadero interesado puede generar más riesgos en línea para los internautas. Piénsese así que, por ejemplo, para la represión de delitos cometidos *online*, puede dificultarse la búsqueda del autor de los hechos.

La segunda fase se configura como aquella en la que el usuario desarrolla su actividad en la plataforma compartiendo información personal en su perfil e interactuando con otros usuarios. Las redes sociales predisponen un entorno que anima a los usuarios a desvelar paulatinamente información personal y privada como sus vivencias, opiniones, imágenes, estado sentimental, familia, etc., estos, persuadidos por la dinámica que las redes sociales alientan, comparten constantemente este tipo de información. En el caso de menores de edad, sin resultar plenamente conscientes de que cuanta más información comparten, más se erosiona su privacidad. Por ello, las redes sociales impulsan al usuario a permanecer mayor tiempo empleando la plataforma, asegurándose que información personal de todo tipo.

La principal razón por la que las redes sociales precisan de información personal de las personas usuarias la hallamos en que el tratamiento de datos que la red social realiza no se limita únicamente a los datos aportados en la fase de registro expuesta anteriormente. En efecto, el volumen de información personal que las personas usuarias comparten constantemente se somete a tratamientos exhaustivos de información en orden a definir los gustos, preferencias, opiniones y, en definitiva, diseñar un perfil con los principales atributos de la personalidad de cada usuario a las empresas de publicidad y *marketig*. Y es que, la información publicada por las personas usuarias, unida al rastro que sus contactos y navegación dejan en la red social, genera una huella digital económicamente muy rentable para las plataformas de redes sociales, debido a que su principal fuente de ingresos proviene de las cesiones a terceros de los millones de datos que tratan. Tal y como afirma PLATERO ALCÓN, cuando un usuario se da de alta, su información personal se convierte automáticamente en un "negocio" para el proveedor de la red social[313].

Así las cosas, la red social se presenta como un servicio aparentemente gratuito para las personas usuarias del mismo, sin embargo, la información personal constituye la moneda de cambio durante el desarrollo de su actividad en la plataforma[314]. En este contexto, cuanta más información compartan los usuarios, mayor se estimará también la

[313] PLATERO ALCÓN, A., *El derecho al olvido en internet. La responsabilidad civil de los motores de búsqueda y las redes sociales: estudio doctrinal y jurisprudencial*, *op. cit.*, p. 178.
[314] La conducta descrita se identifica con *Pay for Privacy*, esto es, conceder al proveedor la posibilidad de rastrear y configurar perfiles de navegación o de editar determinada publicidad a cambio de ser usuario de la red social. Véase MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales, op. cit.*, p. 88.

rentabilidad que dichos usuarios pueden aportar al proveedor, en el sentido que, este dispondrá de mayor información para poner a disposición de las empresas que ofrecen publicidad dirigida a los usuarios de la red social, basada en la información que previamente han desvelado en sus perfiles[315].

En coherencia con lo expuesto, las herramientas de análisis empleadas inicialmente por las redes sociales para proporcionar dichos datos a terceras empresas ofertantes de publicidad, consistían en herramientas matemáticas sencillas; sin embargo, en la actualidad presentan cada vez de una mayor complejidad. Los algoritmos empleados por la red social para tratar la información, extraen un rendimiento verdaderamente valioso de las interacciones en la red (localización, sexo, nivel de vida, gustos, trabajo, familia…) esto es, permiten la puesta a disposición a terceras empresas de un perfil verdaderamente detallado de la personalidad de concretos usuarios para que estas conozcan exactamente qué productos o servicios ofertarles. Según dispone TRONCOSO REIGADA, toda la información compartida, señala pautas de consumo y permite personalizar la publicidad[316].

Con manifiesto acierto sostiene BARRIUSO RUIZ que no es altruismo lo que permite a estos servicios funcionar gratuitamente, y conformes con su afirmación, continúa señalando que la publicidad no constituye la única fuente de ingresos para estas plataformas. La información de los medios sociales sometida a algoritmos de análisis, que seleccionan y extraen contenidos con seguimiento de palabras clave, permiten

[315] Según disponen la AEPD e INTECO en el Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), pp. 45-46. La cadena de valor de las redes sociales se integra de los siguientes elementos: En primer lugar, los proveedores de Servicios de Internet, se tratan de las entidades encargadas de proveer a la red social de la tecnología necesaria (servidores, conectividad, ancho de banda, etc.). En segundo lugar, las plataformas colaborativas y las redes sociales, deben desarrollar y plantear una estrategia que debe considerar de antemano el público al que se dirigirá el servicio y el tipo de herramientas que pondrá a disposición de estos. En tercer lugar, las empresas de marketing y publicidad *online* constituyen el elemento de planificación del modelo de rentabilización económica de la red social, esto es, *determinarán las campañas publicitarias y las estrategias comerciales que la red social va a emplear para maximizar los beneficios de la monitorización de la plataforma a largo plazo de manera sostenible*. [la cursiva es nuestra]. Por último, los usuarios resultan el mayor activo económico para la plataforma. A mayor número de usuarios recurrentes, mayor resultará también el valor de la plataforma. En definitiva, todo el valor de la red social radica en el número de usuarios que esta posea registrados, su fidelización, el nivel de actualizaciones y la facilidad de implantar sistema de explotación económica de dicha información.

[316] TRONCOSO REIGADA, A., "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una", *Revista de los Estudios de Derecho y Ciencia de la UOC,* noviembre 2012, núm. 15, p. 64.

obtener de forma selectiva perfiles de gran significado[317]. Estas conductas, conllevan un verdadero riesgo para la privacidad de las personas, ya que, a mayor información compartida en la red, el riesgo de vulnerar la privacidad de las personas usuarias también aumentará exponencialmente. La técnica de tratamiento descrita y practicada por los proveedores de redes sociales no es baladí, tanto la personalidad como los hábitos e intimidad de los usuarios quedan totalmente descubiertos tras la aplicación de los algoritmos correspondientes. Así, la descontextualizada información que de manera inocente se publica paulatinamente en la red, se ordena, analiza y clasifica por las herramientas de medición, a efectos de generar un perfil lo más preciso posible sobre la persona usuaria. En consecuencia, queda expuesto el modo de ser, actuar, pensar e incluso pueden llegar a predecir las decisiones y comportamientos de las personas.

Con todo, los riesgos de esta fase se caracterizan, en primer lugar, por un desconocimiento absoluto por parte del usuario del alcance y utilización de la información publicada. En efecto, las personas que manejan estos servicios no toman conciencia de que los atributos y derechos que acompañan a su personalidad, aun no compartidos con la plataforma, pueden quedar al descubierto con gran facilidad por las potentes herramientas de medición. En segundo lugar, esta conducta consistente en desempeñar tratamientos masivos de todo tipo de información de los internautas, puede conllevar una posible utilización de la información para finalidades distintas a las descritas en las políticas de privacidad. En tercer lugar, recordemos que el propio usuario genera contenido, lo que puede implicar la vulneración de derechos fundamentales de otras personas. Por último, muchas redes sociales, ofrecen aplicaciones que no aclaran sus finalidades suficientemente, por lo que, pueden llegar a producirse tratamientos de datos por terceros no consentidos expresamente.

La tercera fase consiste en la cancelación de la cuenta, esto es, el final de la relación contractual entre proveedor y usuario. Ahora bien, este final no se caracteriza por su sencillez cuando supone eliminar, de manera efectiva, miles e incluso millones de datos personales que una persona ha compartido a diario en su perfil. Efectivamente, es evidente la dificultad para eliminar de manera real y efectiva la ingente cantidad de datos publicada en estas plataformas ya que, estos datos arrojan una huella digital compleja de eliminar por completo en Internet. Esta dificultad en la eliminación de la información, se

[317] BARRIUSO RUIZ, C., "Las Redes sociales y la protección de datos hoy", *op. cit.,* p. 304.

traduce en la práctica en la perpetua disponibilidad, sin el conocimiento del usuario, en muchas de las ocasiones, de información personal publicada mientras el contrato entre proveedor y este se encontraba vigente.

El principal riesgo de esta fase lo constituye, sobre todo, la gran dificultad e incluso en ocasiones imposibilidad de eliminar el gran volumen de datos personales que se encuentran en la red. Habría que señalar también, que dicha dificultad se acrecienta cuando los buscadores indexan estos datos, pues en esos casos, la información se encuentra expuesta a la totalidad del público de la red. Por otra parte, también debemos mencionar el óbice que supone cancelar o eliminar la cuenta en la plataforma *online*, mientras que para el registro no se precisan más que de unos escasos minutos. Esto es, los procedimientos para renunciar al servicio resultan complejos y distan notoriamente del procedimiento ágil para darse de alta. Por último, resulta controvertida la conducta de estos proveedores de servicios consistente en el almacenaje de los datos de navegación del usuario con objeto de ofrecer a este, con carácter posterior, publicidad contextualizada, a pesar de haber cancelado la cuenta en la red social.

En definitiva, todas las fases mencionadas se diseñan de un modo que pone en riesgo la información personal de las personas usuarias. El propio modo de operar de las redes sociales propicia en todo momento que las plataformas mantengan garantizado cada vez un mayor volumen de información personal al que someter a tratamiento.

Por todo lo expuesto, este nuevo mundo interconectado virtualmente, predispuesto por las redes sociales, se presenta como un desafío para la protección de los datos personales de las personas. Destacamos en este aspecto, cinco elementos acuñados por MARTÍNEZ MARTÍNEZ que evidencian dicho reto:

En primer lugar, las redes sociales se presentan al usuario como un ámbito relacional equivalente al que dispone en el mundo físico. Esta circunstancia, genera una falsa percepción de privacidad en el internauta. Antes bien, Internet se configura como una tecnología en la que la información fluye a tiempo real y de manera ubicua; en la vida *offline*, la amplificación de la información hasta dichos extremos deviene imposible.

En segundo lugar, las reglas que definen la relación contractual, no se acuerdan con el usuario. Darse de alta en una red social implica la aceptación de un contrato de

adhesión que se configura como un verdadero *take it or leave*[318]. Además, la prestación de dicho consentimiento conlleva eventualmente la aceptación de la política de privacidad diseñada por el proveedor de la red social. Mediante dicho consentimiento, se autoriza al proveedor a rastrear, configurar perfiles e incluso a monitorizar la actividad en línea de las personas usuarias para editar determinada publicidad por parte de empresas[319].

En tercer lugar, la información que se publica en el perfil, resulta de evidente carácter personal. El usuario narra en el perfil su vida *offline* en la plataforma, de manera auto bibliográfica y actualizada mediante la publicación de fotos, vídeos, localizaciones, opinión. Este apartado, enlaza con la siguiente circunstancia en el sentido que, el usuario ya no se considera un usuario pasivo, su conducta puede llegar a repercutir en los derechos de terceros. Mediante la publicación de fotografías, opiniones, vídeos, pude llegar a vulnerar derechos de otras personas. Se aprecian hábitos frecuentes como opinar y criticar a otras personas en redes sociales, etiquetar a estas en fotografías sin consentimiento, incluso en aquellas fotografías que pueden considerarse comprometedoras.

Por último, Internet no se desarrolla en un espacio público real y material. Los proveedores de servicios de la información de este tipo, poseen todo el conocimiento que paulatinamente genera cada usuario. Además, los riesgos para la privacidad pueden adquirir mayor alcance según la configuración del perfil, tal y como veremos posteriormente[320].

Como resultado de este nuevo fenómeno social, no compartimos la existencia de voces que afirman que las personas han de resignarse a no poseer privacidad o que si la conservan se debe a que alguien tolera dicha circunstancia[321]. Cierto es que, el propio concepto de red social invita a renunciar a parte de la privacidad. No obstante, debe advertirse jurídicamente que convertirse en usuario de las mismas no debe constituir

[318] La expresión *take it or leave* anglosajona, "lo tomas o lo dejas" en español, es empleada para hacer referencia a que el usuario no posee ningún tipo de capacidad para negociar las condiciones sobre las que se asentará la relación entre el proveedor de redes sociales y éste. La única opción posible reside en aceptar en bloque las cláusulas predispuestas por la red social en orden a convertirse en usuario de la misma.
[319] Véase en ese sentido la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre ¿Cómo usamos tu información?, (última fecha de consulta el 21 de septiembre de 2022), p. 17.
[320] MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales, op. cit.*, pp. 88-89.
[321]Dicha preocupante afirmación es realizada por el presidente y cofundador de *Sun Microsystems* en 1999. Véase TRONCOSO REIGADA, A., "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una". *op. cit.*, p. 64.

sinónimo de renunciar a la parcela de vida privada que todo usuario posee el derecho a conservar.

En este entorno, los datos de menores se hallan expuestos por dos motivos principales: se consideran los usuarios que más información personal comparten en la red social, además de constituirse como el colectivo que más las emplean; y en adición a lo señalado, en muchas ocasiones no son verdaderamente conscientes de lo debilitados que quedan sus derechos tendentes a proteger la privacidad y especialmente el derecho a la protección de sus datos personales.

2.2. Hábitos del usuario menor de edad en redes sociales. De las dificultades para la protección de su información personal

Las redes sociales componen un entorno verdaderamente atractivo para los jóvenes de hoy en día. Desde la irrupción de estas plataformas en 2008, su número de usuarios ha crecido exponencialmente. Concretamente, se estima que, las redes sociales contaban con 3,8 millones de usuarios en todo el mundo[322]. Dicho incremento y éxito en su empleo también se ha visto reflejado entre la población más joven que maneja estas plataformas principalmente para entretenerse y comunicarse.

En este sentido, deviene indispensable analizar minuciosamente los principales hábitos de uso de redes sociales por parte de los menores de edad, pues el modo en el que interactúan con estos espacios incide sobre su privacidad. Así las cosas, nueve de cada diez menores entre 11 a 20 años ya disponía de un teléfono móvil en el año 2009, fecha en la que podemos situar el verdadero *boom* en el empleo de redes sociales[323]. En lo que a redes sociales se refiere, un 92, 6% de los menores encuestados accedía a dichas

[322] "Informe anual sobre Aplicaciones y menores: un año atrapados detrás de las pantallas", *Qustodio*, Año 2020. Obtenido de https://qweb.cdn.prismic.io/qweb/10de139a-cb1c-488e-b0e9-f5becb01f32f_Informe+anual+de+Qustodio+2020+Informe+sobre+los+h%C3%A1bitos+digitales+de+los+menores_ES.pdf (última consulta el 4 de mayo de 2021).

[323] Encuesta de la FUNDACIÓN PFIZER sobre la Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Obtenido de https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf , El presente estudio se ha practicado sobre la recogida de una muestra nacional de 1.000 chicos y chicas (500 de cada sexo) de entre 11 a 20 años de edad, así como 1.000 progenitores de los menores encuestados. El objetivo del estudio reside en analizar los hábitos, usos y comportamientos que los jóvenes llevan a cabo en relación a las TIC, concretamente en redes sociales. Además, también se propone analizar cómo viven, valoran y entienden esta nueva forma de comunicarse digitalmente. (última consulta 7 de septiembre de 2021)

plataformas frente a un escaso 7,4% que no. No obstante, debemos enfatizar especialmente en que, el colectivo más joven (11 a 13 años) ya alcanzaba cifras de uso muy elevadas en 2009. Observamos que, los menores de edad, desde la misma irrupción de estas nuevas herramientas, se han visto inmersos en el manejo de las mismas.

Ahora bien, en 2021 la situación se presenta diferente, pues estos acceden principalmente a través de un *smartphone* de su propiedad. Véase que en España, en el año 2020 un 69,5% de menores de entre 10 y 15 años disponía de un *smartphone* para su uso personal, herramienta preferente por la que los menores de edad acceden a las redes sociales[324]. Puede apreciarse que, mientras que en 2009 el 99,8% de los menores accedían a las redes sociales mediante un ordenador, y generalmente de mesa, en la actualidad el teléfono móvil se convierte en el dispositivo de acceso predilecto[325].

No obstante, llama la atención la falta de sensibilidad por parte de los más jóvenes de los riesgos que el empleo de redes sociales puede conllevar. En ese sentido, puede afirmarse que principalmente manejan estos espacios virtuales para comunicarse[326]. Sin embargo, preocupa especialmente, la falta de advertencia por parte de los menores encuestados de los riesgos que el empleo de las redes sociales puede acarrear[327].

---

[324] Cabe destacar que, a medida que la edad aumenta, también incrementa respectivamente el porcentaje de menores con teléfono móvil; concretamente, mientras que un 22,1% de menores posee un *smartphone* con 10 años, dicha cifra aumenta a un 41,4% a los 11 años de edad; con 12 años la cifra ya alcanza el 68,8%; sin embargo, el gran incremento podemos situarlo a los 13 años, pues a dicha edad el 88,1% de los menores dispone de un teléfono móvil; las cifras en los 14 y 15 años se sitúan en 92,8% y 95,7% respectivamente. Los menores españoles, además de poseer un teléfono móvil personal, arrojan unas cifras de uso de Internet muy elevadas, dado que un 94,5% de menores utiliza esta herramienta. INSTITUTO NACIONAL DE ESTADÍSTICA. Encuesta sobre el Equipamiento y uso de Tecnologías Información y Comunicación en los Hogares, de 16 de noviembre de 2020, TIC_H-2020. Obtenido de: https://www.ine.es/prensa/tich_2020.pdf (última consulta 7 de septiembre de 2021).

[325] Encuesta de la FUNDACIÓN PFIZER sobre la Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Obtenido de: https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf , p. 47. (última consulta 7 de septiembre de 2021)

[326] En efecto, 8 de cada diez jóvenes poseía en 2009 un perfil en una red social con el fin de comunicarse y chatear con sus amigos; perfil que los menores completan con el mayor número de datos personales posible. El 90% de los menores encuestados comparte con la red social su género, el 80-90% su edad, aunque como veremos posteriormente, esta no siempre sea verdadera, el 75% comparte el dato relativo a la ciudad en la que reside, el 54% el centro de estudios y sus gustos o aficiones, el 16,7% su dirección postal, por último, un 13% su número de teléfono personal. Encuesta de la FUNDACIÓN PFIZER sobre la Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Obtenido de: https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf , p. 50. (última consulta 7 de septiembre de 2021).

[327] Así, sólo 37 de 1000 menores valoran las redes como un entorno negativo en el que pueden encontrarse abiertos a engaños y a una falta de privacidad. Además, solamente un 21,9% de los menores identifica como un peligro aportar demasiados datos personales. Podemos afirmar que, los menores de edad, con carácter general, no advierten las amenazas que estas plataformas suponen, véase que gran parte de los encuestados valora las redes sociales como algo muy positivo con una calificación de 4,01 sobre 5 puntos. Encuesta de la FUNDACIÓN PFIZER sobre la Juventud y las redes sociales en Internet. Informe de resultados

Sobre este último aspecto, corresponde a los progenitores apoyar a los menores a tomar conciencia de los riesgos que el manejo de estos espacios conlleva. Ahora bien, la brecha digital en este campo, resulta más que destacable[328]. Esta circunstancia influye sobre el control y advertencia de amenazas en el uso de redes sociales que realizan sus respectivos hijos o hijas[329].

Todavía cabe señalar, que únicamente un 11,2 % de los progenitores considera las redes sociales como un riesgo para la privacidad. Sin lugar a dudas esta cifra resulta preocupante en el sentido que, los adultos advierten en menor medida el riesgo que estas plataformas suponen para la privacidad de sus hijos e hijas (los menores que lo advertían alcanzaban un 21,9%). Es más, ante supuestos en los que los menores han visto su privacidad amenazada, han contestado en la encuesta que, el 67,9% de los progenitores y madres no tomó medidas para asistir al menor. Definitivamente, preocupa especialmente la falta de advertencia de los riesgos que estas herramientas suponen para la privacidad de las personas. En ese sentido, los progenitores parecen mostrarse más preocupados por los siguientes riesgos: el uso abusivo de estas plataformas y la respectiva pérdida de

---

de la encuesta, septiembre 2009. Obtenido de: https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf , p. 50. (última consulta 7 de septiembre de 2021). A propósito de lo expuesto, un estudio realizado en 2017 a adolescentes de Segovia entre 14 y 17 años avala dicha afirmación, ya que 3 de cada 4 adolescentes han sufrido algún tipo de experiencia negativa en redes sociales, pero ello no ha influido en su valoración del riesgo sobre las mismas. Efectivamente, según dispone el estudio, los menores tienden a disociar la percepción del riesgo de las experiencias vividas en las redes sociales. Consecuentemente, resulta realmente complicado que el menor tome conciencia de los riesgos a los que se encuentra expuesto si ni tan siquiera la propia experiencia sirve de referencia para tomar conciencia de ello. DE FRUTOS TORRES, B., y MARCOS SANTOS, M., "Disociación entre las experiencias negativas y la percepción de riesgo de las redes sociales en adolescentes", *El profesional de la información,* enero-febrero 2017, v. 26, núm. 1, p. 93.

[328] En el sentido que, mientras que un 92,6% de los menores encuestados por la Fundación Pfizer, participa activamente en redes sociales, un 62,2% de los progenitores no lo hace. ENCUESTA FUNDACIÓN PFIZER, La Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Obtenido de: https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf (última consulta 7 de septiembre de 2021).

[329] Los menores encuestados por la FUNDACIÓN PFIZER afirman navegar solos casi siempre (68,8%), no recibiendo nunca ningún control por parte de sus progenitores en su participación en redes sociales en un 52,7% de los casos. Refuerza dicha circunstancia el dato aportado por la encuesta realizada por la Comisión francesa de protección de datos personales (CNIL)a 6517 jóvenes entre 11 a 18 años entre el 10 de septiembre de 2020 y el 31 de enero de 2021, al afirmar que, el 70% de los menores encuestados posee un dispositivo desde el que acceder a redes sociales en su propia habitación. La propia agencia afirma que los jóvenes se encuentran "hiperconectados" a las redes sociales enfrentándose a menudo en solitario a estas. Informe de la Comisión francesa de protección de datos (CNIL) sobre las prácticas digitales de los jóvenes entre 11 a 18 años. Obtenido de: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf , pp. 8-9. (última consulta el 20 de octubre de 2021).

tiempo que ello conlleva para el menor, la posibilidad de que se entre en contacto con gente desconocida y peligrosa, así como que se trate de un entorno que permita al engaño.

En suma, a la luz del informe, curiosamente, tanto progenitores como menores no perciben las amenazas reales que las redes sociales suponen para la privacidad de las personas. Efectivamente, dicho riesgo queda relegado a segundo plano entre otros peligros que, sí advierten en mayor medida. Sin embargo, no debe pasar inadvertido el riesgo que estas constituyen para nuestra vida privada y particularmente para nuestros datos personales. Sin lugar a dudas, el estudio traído a colación nace en un contexto de una fecha próxima al descubrimiento de estos nuevos medios para comunicarse y socializar; en cambio estos servicios avanzan de manera vertiginosa convirtiéndose en cada vez más potencialmente peligrosos para la vida privada de las personas.

Antes bien, lo verdaderamente desconcertante, resulta la temprana edad con la que los menores toman contacto con Internet y se convierten en usuarios de redes sociales[330]. Indiscutiblemente, los menores son usuarios de este tipo de plataformas de forma masiva y desde edades muy tempranas, lo que repercute en mayor medida a que los derechos de la privacidad de estos y especialmente el derecho a la protección de los datos personales, se vulneren por los proveedores de redes sociales[331].

Así, influye decisivamente en ello la temprana edad de acceso a estos espacios virtuales, dado que, cuanto más jóvenes acceden a estos, mayores habitúan a tratarse los errores en materia de privacidad dada su manifiesta falta de madurez. Además, el teléfono móvil que portan con ellos en todo momento, se posiciona como un nuevo medio de acceso a las redes sociales, lo que potencia en parte la posibilidad de que su privacidad se desvele con más facilidad, principalmente porque, la tentación de compartir en todo momento su vida resulta elevada. En efecto, muchos de los aspectos de la vida de estos menores, se hallan condicionados por la tecnología, pues generan amistades, estudian,

[330] Así, el 70% de los preescolares (3-4 años) en Bélgica se encuentran conectados a algún dispositivo con Internet. PEREZ ESCODA, A., "Uso de *Smartphones* y redes sociales en alumnos/as de educación primaria". *Prisma social, revista de ciencias sociales,* marzo 2018, núm. 20. p. 20.

[331] En efecto, el 63% de los niños menores de 13 años posee una cuenta en una red social. Concretamente, el 58% de los jóvenes entre 11 a 14 años posee una cuenta en Instagram; Snapchat por su parte, cuenta con un porcentaje de menores de idéntica edad del 75% entre sus usuarios; seguidamente, Youtube se maneja por un 78% de menores entre 11 a 14 años; por último, TikTok se erige como la red social emergente entre la juventud, dado que esta aplicación ha pasado de manejarse por un 30% de usuarios entre 11 a 18 años a un 50% de los mismos entre los años 2020 a 2021. Véase al respecto el Informe de la Comisión francesa de protección de datos (CNIL) sobre las prácticas digitales de los jóvenes entre 11 a 18 años. Obtenido de: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf , pp. 2 a 5. (última consulta el 19 de octubre de 2021).

interactúan, etc., por medio de estas herramientas digitales, hasta tal punto que, no conciben una vida sin ellas. Su alto grado de participación en las mismas, al haber crecido desde edades muy tempranas empleándolas sin ningún control en la mayoría de los casos, ha ocasionado que estas generaciones hayan asimilado un concepto de privacidad más flexible.

Ahora bien, que los menores continúen en la actualidad empleando Internet y redes sociales desde edades tan tempranas alcanza un matiz de mayor preocupación al conocer que lo perpetran sin supervisión de sus progenitores. Desde luego, recibimos esta información con desasosiego. Que nuestra rutina se encuentra digitalizada se constituye como un hecho que podemos cuantificar, esto es, el 93% de la población española emplea Internet y un 88% posee un perfil en redes sociales[332]. Así mismo, casi la mitad de los usuarios de redes sociales se han planteado el abandono del empleo de las redes sociales por el temor a que se filtre información personal, sin embargo, aquellos que de verdad llevan a cabo dicho abandono no sobrepasan el 12%. De dicha circunstancia alcanzamos dos conclusiones. La primera de ellas es que, la privacidad parece preocupar a las personas cada vez menos, ya que anteponen permanecer en el sistema de manera visible a su vida privada. La segunda, es que los adultos no pueden proteger al menor de un riesgo que ellos mismos no valoran con la entidad suficiente.

En definitiva, no preocupa únicamente lo debilitados que pueden quedar los derechos inherentes a la privacidad, como el derecho a la protección de datos personales de los más jóvenes al inmiscuirse en el mundo digital sin supervisión adulta, sino también el riesgo que estos servicios suponen para el desarrollo de su personalidad, que se encuentra en tránsito hacia la madurez, sin que sus progenitores adviertan realmente dicha circunstancia.

En ese sentido, los menores acceden desde edades verdaderamente tempranas a las redes sociales (aproximadamente 11 años). Dicha edad, se sitúa en lo que se conoce como una niñez intermedia que, finaliza a los 12 años de edad para abrir paso a la adolescencia. Estas etapas, vienen presididas por el comienzo del desarrollo de la personalidad del menor de manera autónoma e independiente, en función del entorno

[332] IAB SPAIN., "Estudio de redes sociales 2022". Obtenido de https://iabspain.es/estudio/estudio-de-redes-sociales-2022/ (última consulta 4 de enero de 2023).

social y cultural que le rodea[333]. No obstante, actualmente, debemos considerar que los menores de edad también comienzan a formar su personalidad inmiscuidos en el empleo de las TIC y redes sociales que, además de innumerables beneficios[334], también traen consigo múltiples riesgos como se verá posteriormente. Evidentemente, el desarrollo de la personalidad del menor hacia su madurez, puede verse condicionado de manera negativa por el manejo de las redes sociales e Internet. Contribuyen decisivamente a ello factores como el acceso a contenidos inadecuados para la formación de su personalidad, una privacidad en riesgo, la posibilidad de resultar víctimas de ciberdelitos, etc.

Centrándonos de nuevo en la privacidad, tanto los menores como los progenitores no toman conciencia de las amenazas reales que las redes sociales suponen para su vida privada. Por una parte, la inmadurez del menor lo convierte en una persona vulnerable ante el empleo de estos servicios sin que él mismo perciba dicha circunstancia, y ello debe compensarse por sus progenitores como titulares de la patria potestad, así como por los poderes públicos como garantes de su interés superior junto con los anteriores (art. 39 CE). Por el contrario, en el contexto virtual descrito, una actuación correcta por parte de los progenitores en interés superior de sus hijos e hijas resulta difícil, pues no advierten los riesgos reales a los que se enfrentan la privacidad y los datos personales de sus descendientes. A nuestro modo de ver, ello reclama, en mayor medida, la intervención de los poderes públicos con el fin de configurar un sistema de protección de los jóvenes internautas cuando son usuarios de Internet y redes sociales. La protección descrita se torna necesaria debido a que el art. 5.1 LOPJM- único artículo con mención expresa a las TIC- invita a los más jóvenes a auto protegerse de los riesgos que el entorno digital conlleva, ahora bien, ha quedado evidenciado que los menores no pueden protegerse de aquellos riesgos que desconocen, lo que evidencia la necesidad de formar, con carácter urgente, a la población más joven en torno a la protección de su privacidad[335].

[333] FERNÁNDEZ CORONADO, A., y PÉREZ ÁLVAREZ, S., "La libre formación de la conciencia del menor a través de internet", *Menores e Internet*, Cizur menor, Aranzadi, 2013, pp. 7 a 9.
[334] Como, por ejemplo, proporcionar al menor la posibilidad de aprender, innovar y ser creativo, comunicarse y expresarse, colaborar y participar en la sociedad o tomar mayor conciencia del mundo que les rodea. Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones, Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones una "Estrategia europea en favor de una Internet más adecuada para los niños", del 2 de mayo de 2012, COM (2012) 196 final, p. 3.
[335] Véanse el apartado 5.4 del capítulo primero de la presente investigación sobre el art. 5.1 LOPJM.

2.3. Aproximación a los riesgos y amenazas para el menor derivados del acceso a redes sociales. Especial referencia a su privacidad

Los menores se han incorporado a las redes sociales sin alcanzar el grado de madurez suficiente para comprender las implicaciones jurídicas y riesgos que ello conlleva, en particular, para sus derechos fundamentales relacionados con la privacidad y especialmente con la protección de datos personales[336]. A esta realidad, cabe añadir que habitualmente navegan en solitario en la red y en estas plataformas; esto es, sin ningún tipo de supervisión adulta, incluso aunque no alcancen la edad legal preestablecida para su manejo.

Estas circunstancias fomentan que, por un lado, ellos mismos no adviertan los riesgos que el empleo de estas herramientas implica. Por otro lado, los progenitores no habitúan a supervisar su comportamiento en estos espacios, además de tampoco tomar conciencia real del debilitamiento que la privacidad de sus hijos e hijas sufre cuando navegan en solitario desde sus teléfonos móviles. RAMÓN FERNÁNDEZ comparte esta reflexión cuando afirma que no resulta posible un control del menor en su actividad en las redes sociales, ya que esta navegación no se realiza sólo a través del ordenador, sino de los teléfonos móviles que estos disponen, y además, desde una edad muy temprana[337]. A lo expuesto debemos añadir que la gran mayoría de los menores no ha recibido formación sobre las normas básicas de seguridad cuando emplean las redes sociales, lo que repercute en una manifiesta falta de cultura informática que puede incrementar situaciones de riesgo, muchas de ellas irreversibles. Por ello, nos preguntamos sobre los concretos riesgos que las redes sociales pueden suponer para los menores de edad, con especial referencia a aquellos que pueden debilitar sus derechos.

Así, creemos conveniente exponer primeramente aquellos riesgos más tradicionales y advertidos desde los comienzos de la irrupción de estas plataformas, para después, visibilizar nuevos riesgos que se perciben en menor medida hasta la fecha, sin

[336] Dicha preocupación ya se visibilizaba en la UE desde el año 2010. Véase a tal efecto el Dictamen del Supervisor Europeo de Protección de Datos sobre la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, de 16 de octubre de 2010. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_es.pdf (última consulta el 11 de febrero de 2013).

[337] RAMÓN FERNÁNDEZ, F., "Menores y redes sociales: cuestiones legales", *Revista sobre la infancia y la adolescencia*, abril 2015, núm. 8. p. 39.

perjuicio de que, estos poseerán un capítulo propio de análisis en la presente investigación.

Sentado cuanto antecede, las redes sociales provocan, con especial énfasis en el menor, una falsa sensación de que los datos personales permanecen en el círculo de control del usuario a pesar de publicarse en una plataforma *online*, que además puede encontrarse expuesta al mundo. Al hilo de lo formulado en apartados anteriores y en relación con lo declarado por MARTÍNEZ MARTINEZ, las redes sociales generan un clima de confianza con el usuario[338]. De este modo, este guía su comportamiento en la plataforma como si el mundo analógico se tratara, creándose una falsa percepción de privacidad y control sobre sus datos personales[339].

En el caso de usuarios menores de edad, acertadamente destaca CASTILLA BAREA que los menores navegan con una falsa sensación de seguridad y confianza ocasionada por la cotidianeidad en el uso de las TIC desde su mismo nacimiento[340]. En cambio, cuando una determinada información se comparte en la red social, escapa a toda posibilidad de control por parte del usuario, es decir, todo aquel contenido que se comparte, ya no puede someterse a seguimiento por el titular del mismo, de modo que, otras personas pueden continuar compartiendo dicho contenido, a su vez, entre otros usuarios[341].

En definitiva, los datos alcanzan gran difusión. Ante la situación descrita, los menores se consideran como las principales víctimas de esta falta de control y excesiva confianza alentada por la red social. No toman una real conciencia de que la información aportada, queda cautiva y susceptible de resultar manipulada o utilizada para fines

[338] MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales, op. cit.,* p. 88.

[339] En efecto, tal y como dispone BATUECAS CALETRÍO, los menores se configuran como un sector especialmente vulnerable y proclive a padecer los peligros que las redes sociales albergan debido a su falta de madurez, así como a la sensación de encontrarse en un entorno privado y de confianza. BATUECAS CALETRÍO, A., "El control de los padres sobre el uso que sus hijos hacen de las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, p. 139.

[340] CASTILLA BAREA, M., "La protección de los menores el internet (Comentario al artículo 84 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 3951-3952.

[341] Véase en ese sentido GARCÍA-ATANCE GARCÍA DE MORA, M.V., "Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación (TIC)", *Revista de Derecho político UNED,* septiembre-diciembre 2017, núm. 100, p. 1280 cuando afirma que, los datos pueden resultar fácilmente almacenados, copiados y circular de nuevo, perdiendo los originarios propietarios el control sobre éstos.

completamente distintos al previsto. Este clima de confianza potencia la pérdida de control sobre la información personal, se erigen como la antesala que sirve para potenciar los riesgos que las redes sociales traen consigo.

De este modo, la totalidad de la información compartida en ese contexto, ya no puede someterse a control por el usuario de la red social a pesar de que desde las célebres sentencias del TC 290/2000 y 292/2000, de 30 de noviembre, el contenido esencial del derecho a la protección de datos personales se identifique con garantizar dicho control al interesado *(habeas data)*. Adicionalmente, el comportamiento activo del usuario, como nuevo generador de contenido *online*, constituye un peligro para la privacidad de las personas, no solo para la suya propia, sino también para la de terceros. Nos referimos a que, no solamente la red social trata información personal, sino que, como veremos posteriormente, el propio usuario (incluso menor de edad) puede llegar a tratar datos personales de terceros cuando comparte fotografías, vídeos o información personal sobre éstas[342].

En tales circunstancias, en el momento de darse de alta en la red social, el usuario debe designar la configuración de privacidad de su perfil. Esto es, decidir el colectivo de personas que podrán acceder a dicha información. Tradicionalmente, se han presentado tres niveles de privacidad en gran parte de las redes sociales: sólo amigos, amigos de amigos y totalmente público[343]. No obstante, en la actualidad, sin perjuicio de que dicha circunstancia pueda influir en que la pérdida de datos resulte mayor, la posibilidad de capturar la pantalla de los terminales y así almacenar determinada información, fotografías, vídeos etc., provoca que incluso la información de un perfil privado pueda convertirse totalmente viral en cuestión de minutos. Es suficiente que un usuario (amigo) comparta, a su vez, dicha información con otros contactos de su círculo de amistades. Recordemos que la red social se configura como un espacio interconectado que aspira a unir a todas las personas usuarias del mismo.

[342] Efectivamente, de conformidad con MARTÍNEZ OTERO, el uso generalizado de redes sociales en Internet presenta nuevos desafíos al Derecho, y en especial en lo relativo a la protección de la intimidad, la propia imagen y los datos personales, tanto de los propios usuarios como de terceras personas. En ese sentido, continúa el autor disponiendo que, la euforia con la que los usuarios de redes sociales comparten todo tipo de información propia y ajena afecta a varios derechos fundamentales. MARTÍNEZ OTERO, J.M., "Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento", *Revista Española de Derecho Constitucional,* 2016, núm. 106, p. 122.

[343] Así se configuran redes sociales como Facebook, Instagram, TikTok, Twitter, etc.

Esta dinámica, desde luego, atenta contra la privacidad de las personas usuarias de las redes sociales al poder llegar a constituir una vulneración del derecho a la protección de datos personales (art. 18.4 CE); y especialmente contra la de aquellas que se encuentran en tránsito hacia su madurez como los menores de edad. Una incorrecta configuración del perfil con el riesgo a que la información circule por la totalidad de la red, pueden incidir de manera especialmente traumática y negativa en su desarrollo personal si no toman conciencia de lo peligroso que dicho comportamiento resulta para la privacidad propia y de los demás[344]. Adviértase que el perfil del usuario con su nombre y apellidos e incluso fotografía habitúa a indexarse en los motores de búsqueda en redes como Facebook o Instagram, proporcionando un grado de difusión máxima a dichos datos a pesar de configurar el perfil de modo privado[345].

En otro orden de consideraciones, resulta habitual que las fotografías, vídeos o información no conciernan únicamente al propio usuario de la red social o al menor. En ese sentido, se encuentra disponible una función que permite el etiquetado de terceras personas en fotografías compartidas por un usuario concreto. Antes bien, este sistema de etiquetado, genera un conflicto con la protección de los datos personales de esas terceras personas, ya que, compartir información concerniente a estas personas sin su consentimiento puede constituir un tratamiento ilícito de datos personales[346].

Compartir fotografías de o con terceras personas puede poner en riesgo, a su vez, otros derechos fundamentales relacionados con la privacidad como la intimidad personal

---

[344] Un informe realizado por el OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN en 2011 revela que, el 77% de los menores de edad internautas configura su perfil como público, esto es, la totalidad de la red social, e incluso los motores de búsqueda pueden acceder y mostrar dicha información a la totalidad del universo internauta. Libro blanco de los Contenidos Digitales, de 2008. Obtenido de: https://www.ontsi.red.es/sites/ontsi/files/1233569673805.pdf (última consulta 24 de mayo de 2021).

[345] La propia AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS dispone en la Declaración sobre buscadores de Internet, de 1 de diciembre de 2007. Obtenido de: https://www.facua.org/es/documentos/declaracionsobrebuscadoresdeinternet.pdf (última consulta el 12 de septiembre de 2022), que este comportamiento, consiste en la captura de información disponible en Internet que realizan los motores de búsqueda y de la indexación que ofrecen a los usuarios para facilitar un acceso selectivo a la misma. Por ejemplo, la información publicada en la red social Twitter, aparece en los motores de búsqueda al público. De idéntico modo, el nombre y apellidos de una persona usuaria de Facebook aparecen en Google (motor de búsqueda), si bien el resto de información del perfil, aparecerá dependiendo del grado de privacidad configurado por el usuario. En definitiva, los potentes algoritmos de estos buscadores, rastrean la información disponible en la red, y la estructuran con el fin de ofrecer al usuario dicha información de manera ordenada.

[346] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), p. 75.

o familiar, la propia imagen y el honor (art. 18.1 CE). Así, los menores pueden publicar en su perfil social fotografías, vídeos, críticas sobre otras personas que pueden lesionar el honor o intimidad personal y familiar de otras personas u otros menores. Destacamos algunos casos en los que se ha publicado información comprometedora, vídeos que dañan el honor o la intimidad de otras personas, e incluso existen conductas directamente encaminadas a hacer daño[347]. El verdadero problema reside en que, la red social proporciona un alcance incontrolable y amplificado al extremo a esa violación del honor y a la intimidad.

Por otra parte, al estudiar el funcionamiento de las redes sociales, ha quedado de manifiesto que el verdadero negocio de estos espacios, se encuentra en los tratamientos de grandes bancos de datos personales previamente proporcionados por los millones de personas usuarias que estas poseen.

La información personal que se comparte en la red por las personas, se somete a potentes herramientas de análisis, medición e inferencia que, poseen la capacidad de relacionar información aparentemente no relacionada entre sí. En otras palabras, la labor técnica de dichas herramientas resulta especialmente compleja, en el sentido que, los usuarios van compartiendo información en distintos contextos, momentos, formatos a lo largo de su vida como usuarios de la plataforma. A dicha información, se le aplica por la red social potentes algoritmos que, poseen la capacidad de filtrar, analizar y contextualizar toda esa cantidad de información segmentada. De conformidad con ROIG, la tecnología posibilita extraer datos personales cada vez con más precisión y complejidad, de contextos desestructurados y sin capacidad aparente de identificar a nadie[348]. De dicho análisis, las redes sociales facilitan la construcción perfiles de

[347] En ese sentido, destacamos la sentencia de la Audiencia Provincial de Valencia 372/2019, de 27 de septiembre de 2019, (rec. 329/2019) en la que, la Audiencia Provincial de Valencia confirma la condena del Juzgado de primera instancia impuesta a los progenitores de unas menores y un club de fútbol con motivo de la difusión a través de *Whatsapp* de la fotografía de una joven desnuda tomada por sus compañeras en las duchas tras jugar un partido de fútbol. En ese sentido, la madre de la menor de 13 años fotografiada, interpuso demanda de protección civil del derecho al honor, a la intimidad y a la propia imagen con motivo de la captura y difusión de dicha fotografía. Alega el Tribunal de primera instancia que, efectivamente, la única finalidad de la fotografía residió en captar la imagen de la joven en las duchas para difundirla entre otras personas, con el fin de atentar contra su intimidad y su imagen. Así las cosas, también responsabiliza al club de fútbol por no tomar las medidas pertinentes en aras de evitar este tipo de comportamientos. Por otra parte, la AEPD ha sancionado a particulares por la publicación y difusión de imágenes vejatorias en Whatsapp y redes sociales, sirva como ejemplo, el Procedimiento Sancionador PS/00327/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00327-2021.pdf (última consulta el 5 de enero de 2023).

[348] ROIG, A., "E-privacidad y redes sociales", *op. cit.*, p. 47.

personalidad de todas y cada una de las personas usuarias, perfiles que desvelan claramente el nivel de vida, gustos, preferencias, personalidad, tipo de decisiones, etc., del usuario. En efecto, se desvela a las empresas anunciantes, con todo detalle, los productos que deben ofrecer a cada usuario, motivo por el que, el art. 22 del RGPD siente las garantías a las que deberán someterse este tipo de tratamientos de datos personales.

Esta nuevo modelo de marketing, tan habitual a día de hoy, recibe el nombre de comercialización de comportamiento, es decir, existe una selección de la publicidad a mostrar a cada persona basada en la observación y análisis del usuario a lo largo del tiempo en la plataforma y en la red[349]. Efectivamente, las redes sociales pretenden aumentar sus ingresos mediante el análisis del comportamiento de los usuarios, identificando subsegmentos de mercado a partir de las necesidades y preferencias personalizadas de estos, así como mediante la creación de mercados *online* internos en los que los usuarios pueden llevar a cabo transacciones económicas. Por último, dichos aumentos de los ingresos también los propicia la explotación publicitaria y promocional de los perfiles de usuarios mediante acuerdos comerciales con marcas y empresas externas (*branding*)[350].

De extenderse el control digital constante sobre el modo de actuar de las personas usuarias al ámbito analógico, las personas advertirían con mayor facilidad la vulneración de la privacidad[351]. Sin embargo, los proveedores de redes sociales han desarrollado una herramienta que somete a las personas a ese control exhaustivo sin que estas sean conscientes del alcance y consecuencias de dicho comportamiento para sus datos personales. Huelga decir que los menores de edad no pueden llegar a comprender el complejo tratamiento al que su información personal se somete. En cierto modo, la población adulta también desconoce las implicaciones que dicho comportamiento acarrea para su información personal. Ahora bien, sin perjuicio de que incidiremos sobre ello más adelante, denunciamos que, no se informa con la transparencia y rigor suficiente de dicha

[349] Dictamen 5/2009, Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, p. 10.
[350] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), pp. 56-57.
[351] Supongamos así que, analógicamente, una persona controlara constantemente los comportamientos de un consumidor en orden a averiguar sus pautas de consumo.

circunstancia a las personas usuarias con el fin de mantener un negocio multimillonario para la industria digital.

A los riesgos descritos, debemos añadir que la disponibilidad de desmesurado volumen de datos personales en la red ha propiciado la aparición de un nuevo problema íntimamente ligado con la privacidad de las personas: la huella digital, inicialmente perpetua que los datos personales generan en la web. En efecto, la información publicada por la persona usuaria, permanece disponible y con carácter permanente en la red social o en la web. Este rasgo característico de la información digital, ha de limitarse con especial cuidado en aquellos casos en los que el menor de edad publica una elevada cantidad de información durante su adolescencia que, en edad adulta desea eliminar.

En ese sentido, la adolescencia se configura como una etapa marcada por la realización de conductas carentes de reflexión. Sin embargo, mientras que las conductas residen en la memoria de algunas de las personas en el mundo analógico, la red concede a dichos comportamientos rastro y difusión perpetuos. Esta realidad, todavía no se ha considerado con la entidad que debiera por las personas usuarias de Internet y redes sociales. Es más, el grado de inmadurez de los más jóvenes, propicia que estos no adviertan que algunas acciones que realizan virtualmente, dejan un rastro que puede acarrearles problemas al llegar a la edad adulta[352].

No obstante, esperamos que, con el tiempo, la conciencia sobre esta circunstancia crezca considerablemente, especialmente entre la generación *digital babie* que vive en mayor medida su adolescencia en redes sociales e Internet. El derecho a la supresión conocido como "derecho al olvido digital" (art. 17 RGPD y 93-94 LOPDGDD) propone otorgar una respuesta a este creciente problema: eliminar la información de la red siempre que el usuario lo solicite. Sobre esta controversia, tal y como ha quedado de manifiesto en apartados precedentes de esta investigación, el TJUE ha emitido sendas sentencias

[352] En ese sentido, la 30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad celebrado en Estrasburgo los días 15 a 17 de octubre de 2008 sobre la Protección de la privacidad en los servicios de redes sociales, p. 2. visibiliza la práctica, cada vez, más habitual que algunas empresas acometen para la búsqueda de nuevos candidatos y candidatas a un puesto de trabajo. Así, un tercio de los responsables de recursos humanos, admite emplear datos de servicios de redes sociales en su trabajo para comprobar y/o completar detalles de los candidatos a un puesto de trabajo. Resolución sobre la intimidad de los niños en línea, adoptada en la 30ª Conferencia Internacional de Autoridades de protección de datos y privacidad, propuesta por el Comisario de Protección de datos de Canadá, adoptada en Estrasburgo, octubre de 2008. Obtenido de https://edps.europa.eu/sites/default/files/publication/08-10-17_strasbourg_children_online_es.pdf (última consulta el 8 de marzo de 2022)

creando jurisprudencialmente el derecho citado[353]. Sin embargo, desde su creación hasta su positivización en el RGPD y posterior adaptación a la LOPDGDD, su aplicación no ha resultado pacífica. Ahora bien, más adelante, valoraremos este nuevo derecho, pues nos mostramos escépticos ante la posibilidad real y efectiva de poder eliminar el alud de información previamente compartida en redes sociales.

Por otra parte, sin perjuicio de que no guarda relación con el objeto de estudio en la presente tesis doctoral, los últimos años han demostrado que los peligros a los que se puede enfrentar el menor como usuario de las redes sociales, no residen únicamente en que su privacidad y datos personales puedan vulnerarse fácilmente. Las redes sociales se han convertido en la herramienta cómplice para que los jóvenes resulten víctimas de diversos delitos que pueden surgir en línea, muchos de ellos tipificados penalmente.

Los comportamientos que se expondrán a continuación, con la salvedad del *sexting*, carecían de tipificación penal específica en nuestro ordenamiento jurídico, sin embargo, se ha procedido a su incorporación paulatina en nuestra normativa penal concerniente a ciberdelitos[354]. En efecto, los menores de edad pueden resultar víctimas de acoso escolar por medio de estas plataformas *online*, lo que se conoce como de *ciberbullying*[355]; por otra parte, las redes sociales también pueden favorecer el *childgrooming*, consistente en el acoso de un adulto hacia un menor por medio de las TIC[356]. Respecto al *sexting*, cada vez resulta más frecuente el envío de mensajes e

[353] Nos referimos así a la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, Asunto C-131/12, cuyo análisis acometeremos con posterioridad.

[354] Véanse los arts. 173.1 y 183 ter respectivamente de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Boletín Oficial del Estado, de 24 de noviembre de 1995, núm. 281.

[355] El objetivo de esta conducta se halla en ridiculizar y humillar a la víctima haciéndole daño de manera intencionada y repetida en el tiempo por medio de las TIC. Acostumbran a constituir manifestaciones habituales de este comportamiento, hechos como colgar fotografías comprometidas de la víctima en Internet, tanto si resultan reales como si constituyen montajes, publicar en la red datos sensibles que puedan avergonzar o ridiculizar a la víctima en aras de lograr su desprestigio, crear falsos perfiles con nombre y apellidos del menor para atribuirle determinados comportamientos, colgar comentarios ofensivos en chats, foros, perfiles, incluso compartir rumores a través de la red sobre cuestiones personales de la víctima.. En definitiva, todos los comportamientos persiguen un fin común: desprestigiar al menor en las redes. A lo señalado debemos añadir que, la conducta descrita puede afectar seriamente a su desarrollo personal, ya que, los muros del hogar ya no constituyen un espacio de protección para el menor, puesto que Internet no conoce de muros. GARCÍA-ATANCE GARCÍA DE MORA, M.V., "Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación (TIC)", *op. cit.*, p. 1. Así las cosas, las TIC ocasionan que los límites temporales y físicos que marcaban el acoso en la escuela, sufran un traspaso. A lo expuesto se debe añadir que, la audiencia que puede acceder al contenido lesivo, puede resultar muy amplia e incluso ilimitada. En particular, la información se expande con gran rapidez y comodidad por la red y, además, el contenido digital acosando a la víctima puede quedar almacenado de manera permanente en múltiples dispositivos de personas receptoras de dicha información.

[356] Las redes sociales, se emplean en este entorno para favorecer un acercamiento del adulto hacia el menor, con el fin de ganarse su confianza y así, entablar una relación física sexual con éste. Realmente, la persona

imágenes de contenido erótico en el seno de una conversación *online* que finalmente se difunden al público. En orden a lo expuesto, esta conducta no constituye un delito, principalmente porque el contenido erótico o sexual se comparte de manera consciente y voluntaria por estos jóvenes. No obstante, el riesgo de esta conducta se acentúa con la viralidad que dicha información puede alcanzar en caso de que la persona receptora de dicho contenido decida difundirla en redes sociales o Internet.

Más allá de la problemática legal, debemos mencionar la aparición de una realidad cada vez más creciente como la adicción y dependencia que las redes sociales comienzan a generar entre la población más joven. En verdad, el diseño y funcionamiento de las redes sociales fomenta que este tipo de patologías puedan aparecer con mayor facilidad entre la población adolescente y preadolescente[357]. En tal sentido, a mayor tiempo transcurrido por los menores en las redes sociales, no solo incrementará el riesgo de ser víctimas de transgresiones en su privacidad; sino que también padecerá un incremento de sufrir un mayor aislamiento social (analógico) e incluso una bajada en las calificaciones escolares[358]. En sintonía con lo expuesto, la encuesta realizada por la Comisión francesa de protección de datos (CNIL) citada en reiteradas ocasiones del presente trabajo, señala que un 30% de los jóvenes usuarios de redes sociales permanece despierto durante la noche en orden a permanecer conectado a las redes[359]. En ese sentido, como Taiwán, han

adulta emplea las TIC para camuflar su verdadera edad y generar una paulatina confianza con los menores que elige como víctimas. Una vez que dicha confianza queda entablada haciéndose pasar por otra persona menor, engaña a la víctima para conseguir imágenes eróticas que posteriormente empleará como mecanismo de extorsión a efectos de conseguir más relaciones sexuales con el menor coaccionado.

[357] El sistema *pull to refresh* mencionado anteriormente, pronto se consideró una de las características más adictivas de estos espacios. LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*, Barcelona, Ed: Planeta, 2019, p. 149.

[358] Encuesta del OBSERVATORIO ESPAÑOL DE LAS DROGAS Y DE LAS ADICCIONES sobre Uso de Drogas en Enseñanzas Secundarias en España (ESTUDES 2018-2019). Obtenido de: https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/sistemaInformacion/pdf/ESTUDES_2018-19_Informe.pdf (última consulta el 12 de septiembre de 2022), recoge desde el año 2014 preguntas relativas a detectar el uso compulsivo de Internet (CIUS) junto con otras substancias adictivas como tabaco, alcohol, cannabis etc. En años como 2017, el indicador evidenció la existencia de un uso compulsivo de las TIC entre los jóvenes de secundaria (una cifra superior a 28 de 56 indicadores). Encuesta del OBSERVATORIO ESPAÑOL DE LAS DROGAS Y DE LAS ADICCIONES sobre Uso de Drogas en Enseñanzas Secundarias en España (ESTUDES 2017-2018). Obtenido de: https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/sistemaInformacion/pdf/ESTUDES_2018_Informe.pdf (última consulta el 1 de septiembre de 2022).

[359] Informe de la Comisión francesa de protección de datos (CNIL) sobre las prácticas digitales de los jóvenes entre 11 a 18 años. Obtenido de: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf , p.9. (última consulta el 20 de octubre de 2021).

aprobado normativas que prevén multar a los progenitores que permitan a sus hijos menores de 18 años emplear el móvil en exceso[360].

Finalmente, las redes sociales e Internet también han facilitado que los menores accedan a contenido inadecuado para su edad. Así, resulta poco dificultoso acceder a páginas web o perfiles de redes sociales con contenido nocivo para el menor como pueden tratarse, perfiles o páginas web xenófobas, racistas, violentas, difamatorias, pornográficas, o incluso páginas pro-anorexia y pro-bulimia[361]. Desde luego que la posibilidad de acceder a dichos contenidos de manera tan sencilla, pone en peligro el comportamiento futuro de los jóvenes, pues los menores tienden a aprender de manera imitativa, y ello puede derivar en interiorizar comportamientos que realmente aportan unas pautas erróneas sobre el comportamiento que deberían emprender[362].

3. LA NORMATIVA APLICABLE A LAS REDES SOCIALES *ONLINE:* LA AUSENCIA DE UN MARCO JURÍDICO ESPECÍFICO DE REFERENCIA

Actualmente no existe una normativa *ad hoc* que constituya un marco regulador para las redes sociales. Efectivamente, a pesar de que la irrupción de las redes sociales podemos datarla en el año 2008 y con especial intensidad a partir del año 2011, a día de hoy el ordenamiento jurídico internacional continúa sin establecer los estándares internacionales jurídicamente vinculantes que presidan la normativa sobre redes sociales. En el ámbito nacional, por su parte, la situación no dista de la internacional.

---

[360] DÁVARA FERNÁNDEZ DE MARCOS, L., "Los menores en el Reglamento General de Protección de Datos: cuestiones de Interés (comentario al artículo 8 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, p. 960.

[361] Sobre estas últimas, cabe destacar que, las adolescentes resultan más propensas a sufrir las enfermedades como la anorexia y la bulimia, pues ellas se ven más influenciadas por la información en Internet acerca de artistas, modelos, actrices etc., lo que la mayoría de veces desemboca en una idea errónea del cuerpo ideal, induciendo a estas a perder peso y generando en ellas un trastorno alimenticio. Así, de una búsqueda en google aparecen alrededor de 500.000 páginas pro anorexia y pro bulimia, además el 75% de personas que consultan estos contenidos son menores de edad. En definitiva, la salud mental de los más jóvenes también puede verse afectada por el contenido que estos visualicen en redes sociales y páginas web. LOZANO SÁNCHEZ, Z.B., "La familia y las redes sociales en los trastornos alimenticios en adolescentes de la época contemporánea", *Revista Científica In Crescendo*, 2012, núm. 2 Vol. 3, p. 307 a 308.

[362] En ese sentido el Considerando 62 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE de servicios digitales, Diario Oficial de la Unión Europea, L 277/1, de 27 de octubre de 2022, visibiliza la circunstancia expuesta cuando impone a las plataformas digitales actuar de forma fiable contra contenidos perjudiciales para destinatarios vulnerables como menores. Así, parece que el legislador europeo comienza a tomar conciencia de estos nuevos riesgos para los más jóvenes que, sin duda, ponen en riesgo su desarrollo. De igual modo el Considerando 57 (bis), reconoce que estos servicios pueden causar un comportamiento adictivo en los jóvenes tal y como acabamos de exponer en líneas precedentes.

La ausencia de una normativa específica aplicable la actividad de las redes sociales, ha desembocado en la aplicación concurrente de diversos ámbitos normativos a estas plataformas. Es decir, el marco regulatorio de las redes sociales se encuentra presidido por la normativa sobre protección de datos personales, junto con normativas trasversales como la concerniente a servicios de la sociedad de la información y comercio electrónico y, por último, la normativa sobre propiedad intelectual, aunque en este último ámbito no nos detendremos, pues no se encuentra relacionado con el objeto sometido a estudio en la presente investigación.

En realidad, la normativa de mayor impacto para los derechos fundamentales de las personas usuarias de redes sociales, es la normativa sobre protección de datos de carácter personal contenida en el RGPD y la LOPDGDD estudiadas en el capítulo segundo. Sentado cuanto antecede, hasta la aprobación de los mencionados textos las redes sociales carecían de visibilidad y acomodo en sus respectivos articulados. En efecto, transcurrida una década desde la irrupción de las redes sociales, las normativas implicadas en su regulación, con especial énfasis la relativa a la protección de datos personales, procuran acomodarse a la nueva era digital[363]. Antes bien, cualquiera de las normativas señaladas, se dirige a cualquier responsable del tratamiento y no específicamente a proveedores de redes sociales.

Por otra parte, ha quedado claro que el impacto jurídico de las redes sociales no reside exclusivamente en la protección de datos personales, por el contrario, también resultan aplicables de forma transversal otras regulaciones trasversales en estas plataformas. Así, la actividad que prestan los proveedores de redes sociales recaerá en el ámbito de aplicación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[364] (en adelante, LSSIE), como prestadores de servicios digitales, además de publicitadores de productos en estas plataformas en los términos que estudiaremos más adelante. Por otra parte, no debe pasar inadvertida la aplicabilidad de las disposiciones de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la

[363] Sirvan como ejemplo el art. 94 LOPDGDD sobre el Derecho al olvido en redes sociales, el art. 95 de idéntica norma sobre el Derecho a la portabilidad en redes sociales.
[364] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Boletín Oficial del Estado, de 12 de julio de 2002 núm. 166.

protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[365], y de la que la LSSIE trae causa.

3.1. A propósito de los responsables del tratamiento en redes sociales *online*. Sobre los problemas que plantean los hábitos del usuario (su participación activa) en redes sociales

Con respecto a la aplicación de la normativa sobre protección de datos personales a los prestadores de servicios de redes sociales, deben matizarse dos cuestiones. En primer lugar, es pacífico afirmar para la doctrina, que a las empresas proveedoras de redes sociales debe aplicárseles la normativa sobre protección de datos de carácter personal[366]. En relación con ello, merece especial mención el Dictamen 5/2009, de Grupo de Trabajo 29 citado previamente, ya que en dicho documento radica la justificación sobre la aplicabilidad de la normativa de protección de datos de carácter personal a las redes sociales. Habida cuenta que, la principal actividad de las redes sociales radica en los tratamientos de datos masivos que estas realizan, puede intuirse, que los tratamientos que estas practican quedan al amparo de la normativa sobre protección de datos personales, esto es, del RGPD y la LOPDGDD.

En coherencia con lo expuesto, consideramos que las redes sociales se integran en el ámbito de aplicación de la normativa sobre protección de datos personales, entre otras. En ese sentido, el art. 2.1 del RGPD dispone que, dicho Reglamento resultará de aplicación a los tratamientos de datos personales total o parcialmente automatizados de datos personales, así como al tratamiento no automatizado de los mismos contenidos o destinados a incluirse en un fichero. Cabe así preguntarse dos cuestiones en relación al ámbito de aplicación: la primera, sobre la determinación de "dato personal"; la segunda, cuando se considera que se practica un "tratamiento" de datos personales. De este modo, al amparo del RGPD, el dato personal se corresponde con toda información sobre una persona física identificada o identificable, más concretamente, constituye una persona física identificable, toda persona cuya identidad pueda determinarse, directa o

[365] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, citada previamente. Ahora bien, la UE trabaja en un nuevo reglamento que regulará la materia. Véase la Propuesta de Reglamento de la Comisión Europea sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), de 1 de octubre de 2017, COM (2017) 10 final.

[366] Véase a tal efecto la obra colectiva *Derecho y Redes sociales*, RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010.

indirectamente, en particular mediante un identificador, como por ejemplo, un nombre, un número de identificación, datos de localización o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural, o social de dicha persona física (art. 4.1 RGPD)[367]. Por otra parte, un tratamiento de datos personales se define como el conjunto de operaciones realizadas sobre datos personales que incluyen procedimientos manuales o automatizados. Estas operaciones, consisten en la obtención, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión, cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales (art. 4.2 RGPD).

Las citadas definiciones conducen a estimar que las redes sociales se integran en el ámbito de aplicación de la normativa sobre protección de datos personales. Ello se debe a que, los datos que estas recaban, conciernen a información sobre personas físicas identificadas o identificables, recordemos que las personas usuarias al darse de alta se identifican con datos sobre su persona como el nombre, apellidos, dirección postal, etc., que quedan a disposición de la red social. A ello añadimos que también organizan, estructuran y conservan, entre otras, la información personal que las personas usuarias ponen a su disposición al registrarse, pero también la que con el habitual empleo de la red social genera (huella digital). Adicionalmente, debe tomarse en consideración que estas plataformas o sus colaboradores someten a exhaustivos algoritmos la información para la elaboración de perfiles, conformados a partir de la información que los usuarios involuntariamente comparten en sus perfiles, aparentemente de manera desligada a la identificación de los mismos. No obstante, las redes sociales pueden relacionar dicha información sin necesidad de grandes esfuerzos. En efecto, los datos personales que los usuarios publican en sus perfiles, se convierten en verdaderas identidades digitales que facilitan un conocimiento rápido de los datos de contacto, preferencias y hábitos de

[367] Para más información sobre dato identificable, véase también ROMEO CASABONA, C.M., por persona identificable ha de entenderse aquella que no resulta conocida (no se encuentra identificada), pero puede resultar susceptible de llegar a resultar identificada (identificable). Esto es, no aparece identificada al no mediar una vinculación explícita entre los datos y la persona; no obstante, la vinculación de dichos datos puede ocurrir por medio de diversos procedimientos fácilmente realizables. CASABONA ROMEO, C.M., "Datos personales (Comentario al artículo 4.1 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 585.

consumo[368]. No solo eso, también poseen la tecnología para identificar personas en una imagen, según ha declarado la *European Network and Information Security Agency* (en adelante ENISA) ya en 2007[369].

Comparte este razonamiento el Grupo de Trabajo 29 cuando afirma que los proveedores de redes sociales resultan responsables del tratamiento de datos, debido a que proporcionan los medios que permiten tratar los datos de las personas usuarias. Así mismo, ofrecen servicios básicos vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas). Más aun, determinan la manera en la que los datos de los usuarios pueden emplearse con fines publicitarios o comerciales, incluida la publicidad proporcionada a terceros[370]. En el ámbito nacional, la Agencia Española de Protección de Datos (en adelante, AEPD) acoge igualmente la interpretación basada en el Dictamen del Grupo de Trabajo 29 en su Informe Jurídico 0197/2013[371], afirmando que las redes sociales poseen la condición de responsables del fichero. Por tanto, los proveedores de redes sociales reciben la consideración de "responsable del tratamiento", de conformidad con el art. 4 del RGPD, como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Sin embargo, debemos señalar nuevamente que el usuario se posiciona como un participante activo de la red social, que crea, comenta, comparte información propia y de terceras personas. La circunstancia descrita ha suscitado mayores dudas en cuanto a la aplicabilidad de la normativa sobre protección de datos personales a este comportamiento. Adviértase que las legislaciones de forma natural se encuentran dirigidas a regular el tratamiento de datos por parte de las empresas y las

[368] Estudio de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022), p. 82.
[369] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, *Security Issues and Recommendations for Online Social Networks*, Position paper, núm. 1, de octubre 2007, p. 23.
[370] Dictamen 5/2009, Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, p. 5.
[371] Informe Jurídico 0197/2013 de la AEPD, Gabinete jurídico, Madrid. En dicho informe la AEPD responde a la consulta planteada por un club deportivo sobre la posibilidad de publicar material audiovisual relativo a menores en su perfil de red social. Concretamente, el club deportivo propone a menores la subida de dicho material a la plataforma *Youtube* a través de sus canales privados, enlaces que, posteriormente habrán de compartirse en la página *Facebook* del Club. Como consecuencia, el club desea conocer sobre quién recaerían las eventuales responsabilidades en relación a la protección de datos de carácter personal.

administraciones, de modo que, la normativa no contempla la posibilidad de que las propias personas usuarias, eventualmente, traten datos personales de otras.

Sentado lo anterior, los tratamientos de datos personales practicados por personas usuarias, quedan en la mayoría de los casos, excluidos del ámbito de aplicación de la normativa sobre protección de datos de carácter personal. Esta exclusión se establece en el art. 2.2.c) del RGPD cuando afirma que el RGPD no resultará de aplicación a los tratamientos de datos personales efectuados por una persona física en el ejercicio de sus actividades personales o domésticas. Ahora bien, la irrupción de esta nueva revolucionaria forma de socializar *online*, ha evidenciado la necesidad de reinterpretar dicha excepción doméstica. Ello se debe principalmente a que, si bien las personas usuarias acostumbran a considerarse "afectadas o parte interesada" para el RGPD y LOPDGGD, en ocasiones, su faceta activa puede acarrear la toma de decisiones sobre la información que tratan, que se identifica con un tratamiento de datos personales sometido a obligaciones legales derivadas de dicho tratamiento. Así, por ejemplo, cabe preguntarse si las personas usuarias son responsables del tratamiento cuando etiquetan o comparten una fotografía, con o de terceras personas, o desvelan datos personales de las mismas en sus perfiles.

En este contexto, resulta fundamental traer a colación el célebre caso *Lindqvist*, ya que en el mismo, se desarrolla el establecimiento de aquellos criterios que convierten un tratamiento de datos personales realizado por una persona usuaria, en un tratamiento sometido a la normativa sobre protección de datos de carácter personal[372]. De este modo, el TJUE concluyó que la información personal de terceras personas compartida en una página web diseñada y elaborada por una persona particular, constituye un tratamiento de datos personales no resultando aplicable, en estos casos, la excepción de vida privada acuñada en la normativa sobre protección de datos personales. Así las cosas, siguiendo

[372] Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, *Bodil Lindqvist*, Asunto C- 101/01. La Sra. Lindqvist, a finales del año 1998, creó con su ordenador personal varias páginas web con el objetivo de que los feligreses de la parroquia que se preparaban para la confirmación pudiera obtener de manera sencilla información que pudiera resultarles de utilidad. No obstante, dichas páginas web, además de contener información personal sobre la propia Sra. Lindqvist, también albergaban información de dieciocho de sus compañeros y compañeras de parroquia, incluyendo sus nombres de pila, y en ocasiones nombres completos. Además, la catequista acostumbraba a compartir en la web las funciones que desempeñaban sus compañeros, así como sus aficiones. En esta circunstancia, en varias ocasiones la Sra. Lindqvist llegó a compartir la situación familiar de alguna de estas personas, incluso su número de teléfono.

las acertadas manifestaciones de MARTÍNEZ MARTÍNEZ, la publicación de una fotografía, un vídeo o un texto escrito en una red social sobre terceras personas, no difiere del caso *Lindqvist*[373].

Sin embargo, hemos adelantado en apartados previos que las redes sociales, como norma general, se erigen como espacios en los que el usuario configura el círculo de personas con las que desea compartir la información publicada. Es decir, el alcance que dicha información puede adquirir en caso de que el usuario restrinja el número de personas que pueden acceder a la información publicada en su perfil, no resulta inicialmente tan amplio como cuando la información se publica en una página web abierta al público en general. De todos modos, a nuestro juicio, a pesar de comprender dichas afirmaciones, no es menos cierto que los dispositivos móviles actuales permiten capturar imágenes y vídeo para su posterior difusión. Por lo que, en cierto sentido, mantener el perfil restringido no constituye una mayor garantía de la protección de la información personal. A la mencionada circunstancia debemos añadir, que las redes sociales configuran por defecto los perfiles con el nivel más bajo de privacidad, recayendo sobre el usuario la responsabilidad de modificarlo.

De vuelta a la cuestión que nos concierne, finalmente, la incertidumbre en torno a los comportamientos del usuario de redes sociales que pueden recaer en el ámbito de aplicación de la normativa sobre protección de datos, reciben una respuesta tanto por la AEPD como por el Grupo de Trabajo del Artículo 29. Así, la AEPD se pronuncia en su Informe 0615/2008[374], afirmando que, la publicación de fotografías de determinadas personas no queda incluida ni amparada por la excepción doméstica cuando no existen límites de acceso a las mismas. Ello se debe a que, la excepción opera cuando el tratamiento se identifique con una actividad puramente personal o familiar, equiparable a la que podría realizarse sin la utilización de Internet. En consecuencia, el tratamiento de datos de carácter personal excederá del ámbito doméstico cuando el público que puede

[373] MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma", RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y redes sociales, op. cit.*, p. 98.
[374] Véase el Informe 0615/2008 de la AEPD, Gabinete jurídico, Madrid. El Informe, nace como el resultado de una doble consulta planteada al mencionado organismo: por una parte, es preguntado sobre la consideración de las imágenes como dato personal; por otra parte, sobre la aplicabilidad de la excepción doméstica a la publicación de fotografías en páginas web de determinados particulares en las que se percibe a sus hijos realizando actividades extraescolares. En este sentido, el Informe afirma el carácter de dato personal de la imagen, así como el establecimiento de las pautas que dilucidan la aplicabilidad de la normativa sobre protección de datos a dicho comportamiento expuestas en el texto de la presente investigación.

acceder a dicha información resulta ilimitado, hecho que ocurre cuando dicha información se comparte en la red social cuya configuración de la privacidad no se encuentra restringida. A mayor abundamiento, como señala el informe, ha tenido lugar una cesión o comunicación de datos de carácter personal como, poner a disposición del proveedor de la web información personal sobre terceras personas. Así, la comunicación descrita, requiere del consentimiento del interesado. En sintonía con lo expuesto, reitera la AEPD su interpretación a través de la Resolución del Procedimiento Sancionador 479/2008, afirmando que la captación y reproducción de imágenes de transeúntes en la vía pública y su publicación en YouTube, accesible a cualquier usuario de Internet, requiere del consentimiento de sus titulares[375].

Posteriormente, se pronunció el Grupo de Trabajo del Artículo 29 en su informe citado 5/2009, articulando una serie de criterios, en orden a clarificar que algunos de los comportamientos de particulares exceden del ámbito de la excepción doméstica. El propio documento, sienta que la excepción doméstica puede no alcanzar determinadas situaciones en las que puede desenvolverse un usuario de redes sociales y puede entonces considerarse que el mismo ha asumido algunas de las responsabilidades de un responsable del tratamiento datos. Dichas situaciones se identifican con un total de cuatro supuestos dispuestos por el organismo.

La primera de las situaciones mencionadas, tiene lugar cuando el usuario de la red social emplea la plataforma con el fin de a colaborar para una asociación o una empresa. En este supuesto, se considera que el usuario actúa con fines comerciales, políticos o sociales para la empresa o asociación, por lo que, la exención doméstica no resultará de aplicación en la descrita circunstancia. En este caso, huelga decir que el usuario asume plena responsabilidad en lo que al tratamiento de datos se refiere, por lo que quedará sometido a las obligaciones que la normativa impone. Así, necesitará el consentimiento de las personas interesadas para compartir la información concerniente a estas en su perfil[376].

[375] Resolución 01800/2008 de la AEPD por la que se resuelve el Procedimiento Sancionador 479/2008 sobre la difusión de vídeos en la plataforma Youtube.

[376] Ejemplo de ello, puede constituir una persona que, colabora con una empresa para publicitar sus productos y decide publicar una imagen con otras personas en su perfil. En dicha circunstancia, necesita del consentimiento de las personas que aparecen en dicha imagen, independientemente del grado de configuración de la privacidad del perfil.

La segunda situación que permite considerar a una persona física como responsable de un tratamiento de datos personales, está condicionada por del número de contactos elegidos por el usuario para el acceso a su perfil. Esto es, algunos usuarios pueden sumar un gran número de contactos y no llegar a conocer a muchos de estos. Por ello, un elevado número de contactos puede resultar indicativo de que no se aplica la excepción doméstica y, en consecuencia, el usuario recibirá la consideración de responsable del tratamiento de datos personales. Sobre este aspecto, consideramos oportuno profundizar por la relevancia que reviste en relación a los menores de edad el comportamiento descrito. Estos jóvenes, habitualmente aspiran a alcanzar grandes volúmenes de contactos o seguidores en sus perfiles, lo que les conduce habitualmente a aceptar el acceso a sus perfiles de personas que realmente no conocen. La consecuencia de este comportamiento reviste especial gravedad desde la perspectiva jurídica, habida cuenta que, a la luz del razonamiento del Grupo del Artículo 29 recientemente expuesto en su Informe 5/2009, podrá atribuirse al menor la responsabilidad del tratamiento de datos que realiza sin resultar verdaderamente conscientes de las implicaciones que ello conlleva. En consecuencia, consideramos que legalmente se debe imponer a los proveedores de redes sociales notificar a los usuarios menores de edad la superación de determinado número de contactos, en orden a rebajar las probabilidades de que se llegue a considerar a este como responsable del tratamiento.

La tercera circunstancia que excluye la aplicación de la excepción doméstica, consiste en configurar el perfil de tal modo que todos los miembros que pertenecen a la red social pueden acceder a un perfil concreto o cuando los datos resultan susceptibles de indexación por los motores de búsqueda (como ocurre con la red social Twitter). Adviértase que, en estos contextos, se amplía el acceso a la información más allá de los amigos elegidos, lo que conduce a asumir las obligaciones legales de un responsable de tratamiento de datos personales. Ciertamente, no restringen suficientemente el número de contactos que podrán acceder a la información de su perfil, de modo que, aquellos menores cuyo perfil se configure de modo público, esto es, permitan un acceso a todos los usuarios de la red social, pueden convertirse en verdaderos responsables del tratamiento de datos[377]. Consecuentemente deben solicitar el consentimiento de terceras

[377] Dictamen 5/2009 Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, p.6.

personas cuya información publiquen[378]. Así las cosas, los menores no conocen esta circunstancia, por lo que, vulneran la protección de datos personales de otras personas al no recabar el consentimiento de las mismas. Tal vez el perfil de los menores de edad debiera configurarse siempre por defecto del modo más restrictivo posible a efectos de evitar esta circunstancia especialmente lesiva para la privacidad de los usuarios de redes sociales.

Por último, la excepción doméstica también se ve limitada por la necesidad de garantizar los derechos de los terceros, especialmente por lo que se refiere a los datos sensibles que pueden resultar desvelados en redes sociales.

En suma, de acuerdo con TRONCOSO REIGADA, con carácter general, las actuaciones que los usuarios desarrollan en redes sociales, reciben el amparo de la exención doméstica que la normativa dispone. No obstante, un determinado número de esos comportamientos, entre los que destacan los señalados por el Grupo de Trabajo 29, pueden no verse protegidos por dicha excepción, imponiendo al usuario las obligaciones de un responsable del tratamiento de datos personales[379]. De acuerdo con estas manifestaciones se muestra igualmente PÉREZ DÍAZ cuando afirma que, en los casos en los que los perfiles de redes sociales posean carácter público, la exención doméstica no resulta aplicable[380]. En adición, convenimos con MEGÍAS QUIRÓS que procederá analizar y ponderar en cada caso concreto la eventual responsabilidad[381]. Efectivamente, la AEPD también se ha acogido a las consideraciones expuestas, pues ha impuesto sanciones a particulares por la difusión de vídeos en grupos de personas conformados en la red social Whatsapp sin el consentimiento del interesado[382].

---

[378] Conforme con dicha afirmación se muestra MARTÍNEZ OTERO, J.M., "Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento", *op. cit.*, pp. 135-140.

[379] TRONCOSO REIGADA, A., "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una", *op. cit.*, p. 68. No se trata esta de la primera vez que autor expone dichas conclusiones, dado que, en su obra de 2010, *La protección de datos personales. En busca del equilibrio*, *op. cit.*, p.1697. ya avanzaba las mismas.

[380] PÉREZ DÍAZ, R., "Los menores de edad en la nueva Ley de Protección de Datos Personales", en FERNÁNDEZ VILLAZÓN, L.A., (Coordinador), *Derecho y Nuevas Tecnologías*, Cizur Menor, Aranzadi, 2020, pp. 161-162.

[381] MEGÍAS QUIRÓS, J.J., "Actividades personales y domésticas excluidas del ámbito de aplicación (comentario al artículo 2.2.c) RGPD y al artículo 2.2.a) LOPDGDD)" en TRONCOSO REIGADA, A., (Coordinador), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, pp. 365-368.

[382] Véase el Procedimiento Sancionador de la AEPD PS/000539/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00539-2021.pdf (última consulta el 5 de enero de 2023) por el que

A la luz de lo expresado, un determinado número de menores de edad recibe la consideración de responsable de los tratamientos de datos que realizan. Así sucederá cuando posean un elevado número de contactos o la configuración de su perfil no se encuentre restringida y se muestre accesible a la totalidad de los usuarios de la plataforma. En estos casos, asumen las obligaciones de un responsable de tratamiento, como si de una empresa o administración pública se tratara[383]. A nuestro parecer, esta situación reviste gravedad, pues los menores de edad, y especialmente los *digital babies*, se sienten cómodos compartiendo detalles privados propios, pero también de terceras personas, sin resultar verdaderamente conscientes de esta circunstancia dada su falta de madurez, lo que deriva en vulneraciones de derechos fundamentales de terceras personas. Esta función permitida en redes sociales, en su caso, debería constituir objeto de revisión y resultar restringida desde el diseño y por defecto cuando el usuario es menor de edad a fin de garantizar la seguridad del derecho fundamental a la protección de datos de carácter personal.

Por último, de acuerdo con ORTIZ LÓPEZ, consideramos que los creadores de aplicaciones que se integran como servicios adicionales en las redes sociales, de igual modo que las empresas anunciantes de estas plataformas, también pueden estimarse eventualmente responsables del tratamiento si la red social facilita información sobre sus personas usuarias a los mismos[384]. No obstante, sobre la señalada la responsabilidad de estos actores implicados en las redes sociales, volveremos más adelante.

3.2. La determinación jurídica de la legislación aplicable ante la ubicuidad de las redes sociales: un debate superado

La determinación de la legislación aplicable sobre protección de datos personales a prestadores de servicios digitales ubicados en terceros Estados no pertenecientes a la UE, se ha desarrollado de manera controvertida en el seno de la UE como quedará de manifiesto. Ello se debe, principalmente, al desafío que supone la determinación de la

sanciona a un particular con una multa de 2.000 € por la difusión sin el consentimiento del interesado, de un vídeo en el que este sufre una agresión por un grupo de *Whatsapp* conformado por 12 personas.

[383] Adviértase que la AEPD ha llegado a apercibir a una persona por grabar sin consentimiento a un grupo de escolares durante una visita al zoológico y compartir, posteriormente, las imágenes en un perfil público de la red social Facebook. Véase la Resolución 2261/2011, de la AEPD. Obtenido de https://www.aepd.es/es/informes-y-resoluciones/resoluciones (última consulta el 12 de septiembre de 2022).

[384] ORTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, *op. cit.*, p. 31.

aplicabilidad de la normativa ante el carácter global de la prestación de dichos servicios. Esto es, cuando se trata de Internet, y en concreto, de las redes sociales, la prestación de dichos servicios no conoce de barreras físicas que puedan arrojar claridad sobre la determinación del ámbito territorial de las normativas cuyo objeto reside en la protección de datos de carácter personal. Principalmente porque el responsable puede encontrarse en un Estado no europeo, y el interesado, en cambio, considerarse una persona residente en la UE.

Por otra parte, la determinación de la legislación aplicable resulta indispensable con el objetivo de conocer las obligaciones del responsable a las que los tratamientos de datos deberán someterse. Sobre este aspecto, la consideración del régimen legal europeo como excesivamente exigente ha propiciado que muchas empresas proveedoras de servicios de la sociedad de la información ubicadas en Estados terceros hayan procurado no someterse al ámbito de aplicación territorial de dicha normativa. De modo que, la regulación actual sobre el ámbito de aplicación de la normativa sobre protección de datos personales, se constituye como fruto de varios conflictos que la UE ha debido enfrentar hasta la definitiva aprobación del RGPD.

Partiendo de dichas consideraciones, el derogado art. 4 de la Directiva 95/46/CE, establecía que constituiría régimen aplicable al tratamiento el del Estado miembro en el que se encontrara el establecimiento del responsable del tratamiento en el marco de cuyas actividades tuviera lugar el tratamiento. Así, muchos proveedores de estos servicios, eludieron la aplicación de la normativa europea, alegando que no poseían establecimientos principales en la UE. Como consecuencia, la sentencia *Google Spain*, de 13 de mayo de 2014, citada en el capítulo segundo del presente estudio, resulta de particular interés respecto al conflicto planteado[385]. En dicha sentencia, el TJUE afirma que el art. 4 de la Directiva 95/64/CE se cumple cuando el gestor de un motor de búsqueda cuenta en España con una sucursal o filial destinada a la promoción y la venta de espacios

[385] Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.* La presente sentencia trae causa de una petición de decisión prejudicial presentada en el marco del litigio entre Google Spain, S.L., y Google Inc., por un lado, y la Agencia Española de Protección de Datos y el Sr. Costeja González por otro, en relación con una resoluciónen la que la AEPD estimaba la reclamación del Sr. Consteja contra ambas sociedades en la que ordenaba a estas, adoptar las medidas necesarias en orden a retirar los datos personales del Sr. Costeja de sus índices.

publicitarios en el buscador cuya actividad se dirija a los habitantes de España[386]. En este sentido, la sentencia resulta de gran transcendencia práctica en el caso de los motores de búsqueda y redes sociales, pues a todas luces, aquellos proveedores de servicios de la sociedad de la información con filiales en la UE, deberán respetar la normativa europea a tal efecto a pesar de que la matriz no pertenezca a la UE.

Sin embargo, la solución adoptada por el TJUE en la sentencia de 13 de mayo de 2014, precisaba de mayor matización para aquellos casos en los que las empresas prestadoras de dichos servicios no se encontraran establecidas en la UE, esto es, que no poseyeran ningún tipo de presencia en este espacio[387]. En este sentido, ha constituido una práctica habitual que las empresas que se emplacen en Estados donde el nivel de protección de los datos personales resulta notoriamente inferior al proporcionado por la UE, argumenten la falta de aplicación de la normativa europea a sus tratamientos de datos[388]. No obstante, Internet facilita la captación y tratamiento de datos personales independientemente de la localización geográfica de los implicados, de modo que, mediante el registro en servicios ofrecidos en páginas web o mediante la instalación de *cookies* en los equipos de los usuarios, estas empresas tratan datos personales de interesados europeos, con un menor nivel de garantías del que se debiera. Con el fin de conceder una solución, la Directiva 95/46/CE, imponía la aplicación de la normativa europea a aquellas empresas prestadoras de servicios situadas en un Estado tercero, cuando los medios a los que recurriera para el tratamiento de datos personales, se encontrasen en un Estado miembro.

Ahora bien, dicha solución se dirigía principalmente para los casos en los que se instala una *cookie* en el ordenador, o se coloca un archivo de texto en el dispositivo, entre otros. Ello se debe a que, la colocación de un archivo en un ordenador que se encuentra

[386] Para mayor detalle, véase PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? A propósito de la STJUE de 13 de mayo de 2014 (Google Spain, S.L. y Google Inc./ Agencia Española de Protección de datos [AEPD] Y Mario Costeja González, C-131/12", *Indret, revista para análisis del derecho*, 2015, núm. 1, p. 14 y ss.

[387] De acuerdo con la acertada afirmación de DE MIGUEL ASENSIO, las actividades que estas empresas llevan a cabo, poseen millones de usuarios en la UE a los que dirigen sus servicios, ofreciéndoles, además, espacios publicitarios específicamente dirigidos a anunciantes interesados en comercializar sus productos o servicios en países de la UE. DE MIGUEL ASENSIO, P.A., *Estudios y Comentarios Legislativos (Civitas). Derecho Privado de Internet*, Cizur Menor, Editorial Aranzadi, 2015, p. 73.

[388] En ese sentido, con acierto señala HEREDERO CAMPO que los argumentos territoriales se han empleado de forma sistemática por las empresas prestadoras de servicios en línea. HEREDERO CAMPO, Mª T., "Evolución tecnológica y derecho al olvido digital, desde sus inicios a la actualidad", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 78.

en la UE conlleva el empleo de medios que radican en la UE. Pero para las situaciones en las que el sitio web se limita a obtener datos personales mediante formularios en los que los usuarios facilitan cierta información, resulta más controvertido valorar en qué medida dicho comportamiento se considera utilizar medios situados en el territorio de un Estado miembro. En consonancia con lo expuesto, el Dictamen 1/2008 sobre cuestiones de protección de datos en relación con buscadores[389], dispone que los centros de datos situados en el territorio de un Estado miembro pueden utilizarse para el almacenamiento y el tratamiento a distancia de datos personales por empresas no situadas en la UE, en cuyo caso considera que se emplean medios situados en el territorio de un Estado miembro[390].

Con la finalidad de resolver la problemática sobre la jurisdicción y ley aplicable a empresas no establecidas en la UE, pero que ofrecen servicios en el territorio de comunitario, como pueden considerarse las redes sociales, el RGPD sienta en su art. 3 una solución con un planteamiento más específico que dista considerablemente del deseo mostrado por las empresas prestadoras de estos servicios, como quedará de manifiesto.

Así, las Directrices 3/2018, del CEPD, relativas al ámbito territorial del RGPD, de 12 de noviembre de 2019[391], aportan un análisis a efectos de clarificar el nuevo ámbito territorial diseñado en el RGPD cuya importancia ha de destacarse en el presente estudio debido al impacto que este nuevo planteamiento posee sobre los proveedores de redes sociales. Es así que, el RGPD instaura dos criterios con el objetivo de determinar la aplicabilidad de la normativa europea. El primero, se corresponde con el criterio del establecimiento regulado en el art. 3.1. El segundo, en cambio, se conoce como el criterio

[389] Dictamen 1/2008 Grupo de Trabajo del Artículo 29, sobre cuestiones de protección de datos en relación con buscadores, de 4 de abril de 2008, WP 148. pp. 10-13.

[390] Sobre el criterio de los medios empleados, se han alzado voces críticas como la del responsable mundial de Privacidad de Google FLEISHER, quien sostiene que el criterio de los medios resulta inviable para la determinación del régimen y jurisdicción aplicables. Además, también matiza que, para los casos de sistemas de almacenamiento en la nube, por ejemplo, la determinación de la legislación aplicable en virtud de los medios empleados por el prestador de servicios, pude conducir a la aplicación de la normativa europea a personas residentes fuera de la UE. Más aún, propone el sometimiento a la normativa del país de origen del prestador de servicios en que se encuentren las operaciones principales; criterio que, desde luego, resulta inadmisible a nuestro juicio, dado que, de aceptar dicho planteamiento, la ubicuidad en la prestación de estos servicios desvirtuaría las sendas garantías que la normativa europea sobre protección de datos impone en aras de proteger los derechos fundamentales en el ámbito europeo. FLEISHER, P., "¿Qué legislación en materia de privacidad debería aplicarse en Internet a nivel mundial?", en PIÑAR MAÑAS, J.L., (Director), *Redes sociales y privacidad del menor* Madrid, Reus, 2011, pp. 314-317.

[391] Directrices 3/2018, del Comité Europeo de Protección de Datos, relativas al ámbito territorial del RGPD (artículo 3), de 12 de noviembre de 2019.

de destinatario acuñado por el CEPD en las mencionadas Directrices. Así las cosas, el RGPD mantendrá su aplicabilidad cuando se dé cumplimiento a uno de los dos criterios expuestos. No obstante, conviene profundizar más en las diversas variables que pueden sucederse en la aplicación de los criterios expuestos. Esto es, con el fin de determinar la aplicabilidad del criterio del establecimiento, el CEPD expone tres variables que deberán analizarse.

La primera de ellas determina que el RGPD resultará de aplicación cuando el "establecimiento" que acomete el tratamiento se encuentre en la UE independientemente de que el tratamiento se lleve a cabo en seno comunitario o no. Sobre esta afirmación, debemos subrayar que el concepto establecimiento ha de entenderse de manera amplia a la luz del Considerando 22, que dispone que, la forma jurídica que revistan dichos establecimientos, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto. De manera evidente, este nuevo criterio despeja las dudas e incertidumbre suscitadas cuya resolución tuvieron lugar a través de la sentencia del TJUE de 13 de mayo de 2014 recientemente expuesta[392]. Es más, el propio CEPD afirma que, este criterio reviste validez para las empresas que se dedican a ofrecer servicios exclusivamente a través de Internet.

Por otra parte, dispone el art. 3.1 del RGPD que el mismo gozará de aplicabilidad cuando el tratamiento de datos personales "se realice en el contexto de las actividades de un establecimiento". En realidad, no es necesario que el tratamiento se practique por el propio establecimiento sito en la UE, sino al contrario, las actividades de tratamiento de datos de un responsable establecido fuera de la UE, pueden resultar ligadas a las actividades de un establecimiento local situado en la UE, a pesar de que este segundo no participe en modo alguno en el tratamiento de datos en sí. De esta forma, el análisis de cada caso demuestra habitualmente que se encuentra presente un vínculo indisociable entre las actividades de un establecimiento de la UE y el tratamiento de datos realizado por un responsable ubicado fuera de la UE. Indiscutiblemente, esta situación se identifica con la ocurrida en la sentencia del TJUE de 13 de mayo de 2014, en tanto en cuanto,

[392] Así se ha manifestado posteriormente de nuevo el TJUE en las Sentencias, de 1 de octubre de 2015, *Weltimmo/NAIH*, Asunto C-230/14; Sentencia del Tribunal de Justicia de la Unión Europea, de 28 de julio de 2016, *Verein für Konsumenteninformation/Amazon EU Sarl*, Asunto C-191/15 (en concreto el apartado 76); y Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de junio de 2018, *Wirtschaftsakademie Schleswig-Holstein*, Asunto C-210/16.

Google Spain operaba en el contexto de las actividades de *Google Inc*. situada en Estados Unidos a pesar de que no trataba los datos personales.

La última variable, contemplada en el art. 3.1 se refiere a la aplicabilidad del RGPD al tratamiento de datos personales en el contexto de las actividades de un establecimiento en la UE, "independientemente de que el tratamiento ocurra en la UE". En suma, consiste en que la presencia del establecimiento se trate de la que marca la aplicabilidad de la normativa europea, no resultando determinante en estos casos que, los tratamientos de datos personales se lleven a cabo fuera de la UE.

Debemos mencionar, además, que la ausencia de un establecimiento en la UE, no implica necesariamente que las actividades de tratamiento realizadas por un responsable establecido en un tercer país queden excluidas del ámbito de aplicación del RGPD, tal y como dispone el CEPD en las Directrices 3/2018, de 12 de noviembre de 2019. Antes bien, al contrario, el art. 3.2 del RGPD dispone que el mismo puede resultar aplicable en función de las actividades de tratamiento del responsable. De este modo, el RGPD se reputará aplicable cuando el responsable situado fuera de la UE lleve a cabo dos actividades dirigidas a residentes en la UE[393]. En primer lugar, según señala el Considerando 23, cuando estas se encuentren relacionadas con la oferta de bienes y servicios a interesados de la UE, independientemente, además de si se requiere un pago para la prestación del mismo. En segundo lugar, tal y como dispone el Considerando 24, cuando su actividad se relacione con la observación del comportamiento de los interesados, en la medida que dicho comportamiento ocurra en la UE.

Con todo, a nuestro juicio, el segundo apartado ha dotado de mayor refuerzo y garantía a los internautas en la UE, dificultando la alegación de la no aplicabilidad del RGPD a los proveedores de redes sociales. Adviértase que, a pesar de que estas compañías, no dispongan de un establecimiento que radique en la UE, deberán cumplir las premisas del RGPD cuando observen el comportamiento de los usuarios, conducta

[393] Ahora bien, el término residencia no debe inducir a equívocos. El RGPD resulta aplicable a cualquier ciudadano localizado en la UE, no debiendo poseer este la condición de nacional europeo o residente legal. Dicho razonamiento, además de desprenderse del considerando 14 del RGPD, ha sido ratificado por el CEPD en las Directrices 3/2018, relativas al ámito territorial del RGPD (artículo 3), de 12 de noviembre de 2019, p. 16.

que desarrollan entre sus servicios, o presten servicios a residentes en la UE, circunstancia que también concurre tal y como afirma el CEPD[394].

Definitivamente, debemos señalar que el RGPD constituye un avance considerable de la posición jurídica y las garantías de las personas ante la naturaleza global de Internet y las redes sociales, al configurarse como plataformas cuyos servicios no se circunscriben a un solo territorio. De igual modo, la nueva regulación supone el cese de prácticas por parte de empresas internacionales consistentes en negar la aplicabilidad del derecho de la UE, provocando la indefensión de millones de interesados respecto a los derechos fundamentales que el ordenamiento europeo les garantiza.

4. LA PRESTACIÓN DEL CONSENTIMIENTO DEL MENOR DE EDAD COMO BASE LEGAL DE LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES EN REDES SOCIALES

El contexto generado por las redes sociales en línea respecto a la privacidad de las personas usuarias, en concreto, en relación a los datos personales de estas, convierte en imperante la necesidad de garantizar al usuario suficiente poder de control sobre su información personal. Sin embargo, tomamos conciencia de que el concepto de red social puede resultar incompatible con esta facultad, pues el usuario de estas plataformas, lamentablemente, pierde parte de dicho control al darse de alta en las redes sociales. El modo de funcionar de estos espacios en la prestación de su servicio constituye la razón principal de dicha dificultad en el control de la información personal por parte de los usuarios cuando esta se comparte en la red. Antes bien, como se desprende del RGPD, el derecho a la protección de datos personales consiste, en esencia, en la capacidad del sujeto de disponer y ejercer un poder de control sobre sus datos personales (*habeas data*). Así, en orden a garantizar legalmente dicho poder de control sobre los propios datos personales, el sujeto debe disponer de una serie de facultades que le permitan hacer efectivo su derecho, incluso cuando es usuario de redes sociales.

Dichas facultades, cristalizan en nuestro ordenamiento jurídico en principios y derechos que el RGPD y la LOPDGDD acogen en su articulado. No obstante, dichas

[394] Véanse las Directrices 3/2018, del Comité Europeo de Protección de Datos relativas al ámbito territorial del RGPD (artículo 3), de 12 de noviembre de 2019, p.18.

facultades se traducen en obligaciones y deberes, que los prestadores de servicios *online* deberán cumplir en la consecución de la prestación de sus servicios[395].

Así, según disponen el RGPD y la LOPDGDD, el tratamiento de datos debe ser lícito (art. 5.1.a) RGPD), considerándose el consentimiento del afectado como una de las bases jurídicas de legitimación del tratamiento de datos personales. En tales circunstancias, cuando el responsable del tratamiento inicia sus actividades, debe detenerse a valorar cuál resultará la base legal que legitime el tratamiento que prevé realizar (art. 6 RGPD y LOPDGDD)[396]. Antes bien, el responsable del tratamiento debe evaluar, con carácter previo, si el consentimiento cumplirá con todos los requisitos para que este se repute válido. De lo contrario, el control que el usuario pueda ejercer sobre su información personal no será efectivo y el consentimiento recabado inválido como base jurídica que legitime el tratamiento de datos personales. En caso de encontrarse en dicha circunstancia, el tratamiento habrá de practicarse en virtud de una base legal diferente al consentimiento (art. 6 RGPD), y en caso de que ninguna de ellas resulte satisfactoria para la finalidad del tratamiento propuesto, el responsable habrá de abstenerse de practicar el tratamiento con los fines declarados[397].

[395] En efecto, cobran virtualidad en ese sentido, principios como la licitud, lealtad y transparencia (art. 5.1.a) RGPD), la limitación de la finalidad (art. 5.1.b) RGPD), la minimización de datos (art. 5.1.c) RGPD), la exactitud de los datos (art. 5.1.d) RGPD), la limitación del plazo de conservación (art. 5.1.e) RGPD), la integridad y confidencialidad (art. 5.1.f) RGPD) y, por último, una responsabilidad proactiva en todas las fases del tratamiento (art. 5.2 RGPD). A estos principios se añaden, los tradicionales derechos ARCO (Acceso, rectificación y oposición) y los que el RGPD incorpora novedosamente como el derecho a la portabilidad, derecho de oponerse a decisiones individuales automatizadas y el derecho a la supresión de los datos. Para más detalle, véase TRONCOSO REIGADA A., "Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)", en TRONCOSO REIGADA, A., (Coordinador), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, p. 852.

[396] En virtud del art. 6 RGPD, las bases jurídicas para el tratamiento de datos personales se identifican con un total de seis, a saber: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

[397] Sobre este particular, el cambio de paradigma sentado por el RGPD resulta destacable en cuanto que, bajo la vigencia de la Directiva 95/46/CE el consentimiento se posicionaba como la única causa autorizante del tratamiento de datos personales. Véase al respecto la valiosa aportación del Considerando 40 del RGPD.

En este contexto, los proveedores de redes sociales acostumbran a justificar los múltiples fines de tratamiento de datos personales que practican en diferentes bases legales previstas en el RGPD. En cambio, merece especial análisis la base legal referente a la prestación del consentimiento dadas las dificultades que entraña su prestación con garantías suficientes en el ámbito *online*.

Ciertamente, la correcta configuración del consentimiento deviene indispensable al fin de garantizar la protección de la información personal[398]. Pese a ello, tomamos conciencia del reto que dicha afirmación supone, principalmente porque una de las características más destacadas de las redes sociales reside en la pérdida del control de la información personal compartida que sufre el usuario al darse de alta y publicar información en la plataforma.

En el particular caso de que los titulares del derecho a la protección de datos de carácter personal no alcancen la mayoría de edad, la correcta configuración de dichas facultades, y con especial cautela la del consentimiento expreso e informado, debe acometerse con diligencia por tres motivos principales. El primero de ellos radica en que, las normas específicas dirigidas a la protección jurídica de la minoría de edad no contemplan la adaptación de sus postulados al derecho fundamental a la protección de datos personales, mientras que sí regulan en su articulado los derechos al honor, intimidad personal y familiar y propia imagen. El segundo, trae causa del primero, en el sentido que la correcta protección del menor en el ámbito TIC y concretamente en redes sociales, ha de configurarse en las normas sobre protección de datos personales y las garantías que estas regulan. Esto es, las facultades de las que disponen las personas en orden a garantizar el control sobre sus datos personales, deberán salvaguardar el interés superior del menor como personas especialmente presentes en las redes sociales. Por último, los menores han demostrado que no toman conciencia de la potencial lesividad que las conductas desarrolladas en la red social ocasionan en su información personal, es más, en especial los más jóvenes, no valoran que los datos compartidos en la red social conducen a una falta de control de su información personal. En el contexto descrito, la configuración del *habeas data* del menor en relación a la información personal que le concierne y que

[398] En efecto, conformes con GIL MEMBRADO, la idea el consentimiento se encuentra íntimamente ligada a la del control sobre la información personal. GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, p. 113.

comparte voluntariamente, pero de manera inconsciente, constituye un verdadero reto para el ordenamiento jurídico.

4.1. Luces y sombras en torno al consentimiento *online* del tratamiento de datos personales

Tal y como establece el art. 4.11 RGPD, el consentimiento debe reputarse libre, específico, informado, inequívoco y expreso. De su lectura se deduce que se ha de informar al usuario, con carácter previo a la prestación de su consentimiento, para que este manifieste un consentimiento válido e informado. Esto es, habrá de proporcionarse al usuario un conocimiento claro sobre quién tratará dicha información, con qué finalidades y qué derechos le asisten en defensa de esta, principalmente[399]. En adición a las características expuestas, el consentimiento debe recabarse de manera previa a que el tratamiento se produzca y para cada una de las finalidades de tratamiento en caso de resultar varias, además ha de poder garantizarse su retirada en cualquier momento.

Sentado cuanto antecede, en el ámbito de las redes sociales, el consentimiento se presta en el momento en el que el usuario se da de alta en la plataforma. Esto es, en el registro cuando procede a cumplimentar los campos sobre su información personal. En ese momento, se advierte al usuario de que la aceptación conlleva, asimismo, la prestación del consentimiento a la política de privacidad de la compañía prestadora del servicio de la red social. Así, el usuario presta el consentimiento al tratamiento de sus datos personales, se entiende que, previa lectura de dicha política de privacidad, que formalmente cumple con el requisito de informar a los usuarios sobre las vicisitudes del tratamiento que se realizará sobre su información personal.

Así las cosas, las políticas de privacidad se configuran como un instrumento jurídico cuyo fin reside en garantizar al titular el control sobre su información personal, facilitando a este la información sobre quién, cómo, dónde y para qué se tratarán sus datos, además de los derechos que le asisten[400]. En esencia, se busca que el usuario emita

[399] Efectivamente, tal y como señala EGUSQUIZA BALMASEDA, la válida prestación del consentimiento requiere que el titular de los datos tenga un conocimieto cabal de qué se consiente, para qué y quién será el destinatario de la cesión de uso o derecho que implica aquella. EGUSQUIZA BALMASEDA, Mª.A., *Protección de Datos: Intimidad y Salud*, Cizur Menor, Aranzadi, 2009, p. 67.

[400] ARIAS POU, M., "Transparencia e información que deberá facilitarse cuando los datos personas se obtengan del interesado. El derecho a la información desde el diseño (comentario al artículo 13 RGPD y al artículo 11.1 y 2 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General*

un consentimiento formado conscientemente. De este modo, solo cuando el usuario es informado correctamente de dichos extremos del tratamiento podrá decidir a conciencia sobre la prestación del consentimiento al mismo.

Por otra parte, debemos detenernos en el estudio de los sujetos que deben prestar el consentimiento válido para el tratamiento de datos personales. Sobre este aspecto, debemos subrayar nuevamente que el consentimiento constituye una manifestación esencial del derecho fundamental a la protección de datos personales, por lo que el consentimiento habrá de otorgarse por los titulares de este. No obstante, dicha afirmación ha de matizarse para el caso en el que dichos titulares sean menores de edad. En tal sentido, la actual normativa sobre protección de datos personales sienta en sus arts. 8 RGPD y 7 LOPDGDD, que el mayor de 14 años podrá prestar consentimiento por sí mismo al tratamiento de sus datos personales[401]. Por el contrario, la prestación del consentimiento cuando el menor no alcance la edad de 14 años, recaerá sobre sus representantes legales como personas que han de velar por su bienestar y protección prestándoles asistencia a tal efecto (art. 154 CC)[402]. Efectivamente, tal y como ha quedado expuesto en apartados precedentes de la presente investigación, el menor podrá consentir por sí mismo el tratamiento a su información personal toda vez que haya alcanzado la edad de 14 años, presumiéndose así su madurez como suficiente para ejercitar por sí mismo el control sobre su información personal[403].

Con todo, de conformidad con PÉREZ LUÑO, para el tratamiento de datos personales del menor, especialmente sensibles por las condiciones de su titular, el consentimiento adquiere especial protagonismo al fin de garantizar el poder de control del que estos o sus representantes legales deben ejercer sobre la múltiple información

de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, Madrid, Civitas, 2021, p. 1358.

[401] Recordemos sobre este extremo que el art. 8 del RGPD establece la edad mínima para prestar un consentimiento válido en 16 años, pero autoriza a los Estados miembros a decantarse por una edad comprendida entre los 13 y 16 años. Así, España fijó la edad en 14 años.

[402] SERRANO PÉREZ, Mª.M., "El consentimiento de los menores de edad para el tratamiento de datos personales (comentario art. 7 LOPDGDD)" en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, pp. 991-1001.

[403] HERRÁN ORTÍZ, A.I., "Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?", *Revista R.V.A.P.* 2010, núm. 87-88, p. 553. Conformes con dicha aseveración se muestran a su vez, el ya citado GRIMALT SELVERA, P., "Los menores e internet: capacidad versus protección de la vida privada" en CUENCA CASAS, M., ANGUITA VILLANUEVA, J. A., ORTEGA DOMÉNECH, J., (Coordinadores), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa*, *op. cit.*, p. 188 y REYES MENÉNDEZ, D., "El acceso del menor a las redes sociales y el problema de su autentificación: la necesidad de una respuesta tecnológica", *Diario La Ley*, 2018, núm. 9335, p. 4.

personal publicada en las redes sociales por estos jóvenes[404]. Más aún, de la correcta configuración del consentimiento depende en gran medida la protección jurídica del menor ante los múltiples riesgos que las redes sociales conllevan para su desarrollo o tránsito hacia la madurez.

Sin embargo, hasta la entrada en vigor de la LOPDGDD, recuérdese de nuevo, que el establecimiento de la edad en 14 años de edad, ha resultado polémico. En ese sentido, determinado sector doctrinal entre el que destaca HERRÁN ORTÍZ, sostienen que, el criterio cronológico instaurado no cohonesta con el resto del ordenamiento civil en cuanto a la valoración de la madurez del menor para el ejercicio autónomo de derechos de su titularidad[405]. A nuestro juicio, se debe tener presente que si bien podemos compartir las afirmaciones expuestas, no se debe olvidar que los métodos *offline* que pueden contribuir a comprobar con mayor rigor la madurez del menor, no sirven para valorar la madurez de este cuando desea darse de alta en una plataforma social virtualmente debido a la falta de contacto físico con este[406]. Efectivamente, compartimos el parecer de GIL MEMBRADO cuando dispone que, en redes sociales constituiría una tarea compleja sujetar la actuación del menor al criterio de madurez, ya que en dicho contexto devendrá imposible valorarla[407]. Con todo, a nuestro juicio, el criterio cronológico resulta el acertado en el contexto de redes sociales.

Sin perjuicio de ello, los proveedores de redes sociales no deben olvidar, que a pesar de que el usuario alcance 14 años de edad, continúa considerándose como una persona menor de edad y especialmente vulnerable hasta que alcance la mayoría de edad. Por todo ello, además de tomar conciencia de que las vicisitudes sobre el consentimiento

[404] PEREZ LUÑO, A.E, "Principios de la protección de datos: consentimiento del afectado. El consentimiento de los menores (1ª parte)", en TRONCOSO REIGADA, A., (Coordinador), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*, Cizur Menor, Editorial Aranzadi, 2010, pp. 484.

[405] *Idem.*

[406] Efectivamente, sobre este extremo debemos incidir nuevamente en que ambos criterios de determinación de la capacidad del menor (madurez que demuestre el menor o cronológico) presentan ventajas e inconvenientes tal y como dispone BATUECAS CALETRÍO. Por una parte, un sistema que depende directamente de la madurez que el menor pueda demostrar, se encuentra en mayor sintonía con otras normas que sientan la capacidad del menor como, por ejemplo, la LOPJM; pero a su vez, presenta un principal inconveniente en el ámbito digital: la inseguridad jurídica que genera valorar la misma en dicho contexto. Por el contrario, un sistema cronológico, aporta la seguridad jurídica necesaria en el ámbito *online*, pero no cohonesta con las restantes normas de determinación de la capacidad. BATUECAS CALETRÍO, A., "El control de los padres sobre el uso que sus hijos hacen de las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información*, *op. cit.*, p. 155.

[407] GIL MEMBRADO, C., "Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales", *La Ley Derecho de Familia*, 2017, núm. 13, p. 7.

de menores deben regularse con especial rigor dadas las condiciones especiales de estos, también deben adaptar sus espacios a la edad del usuario registrado a fin de proteger a este como usuario especialmente vulnerable, independientemente de que posea capacidad para consentir por sí mismo el tratamiento de datos personales.

4.1.1 Los principios de licitud y transparencia en los tratamientos de datos de menores de edad: las confusas y complejas políticas de privacidad de las redes sociales

El tratamiento de datos personales de usuarios de redes sociales debe practicarse de modo lícito, leal y transparente al abrigo del art. 5.1.a) RGPD independientemente de la base legal que legitime las finalidades de tratamiento. Sin embargo, constituye tarea reservada del presente epígrafe conceder un análisis detallado sobre la licitud y transparencia del tratamiento cuando el consentimiento se configura como la base legal que justifica el mismo. En ese sentido, el propio art. 4.11 RGPD impone el deber de recabar un consentimiento del interesado que se considere informado, entre otras obligaciones.

Concretamente, el RGPD impone a los responsables del tratamiento la obligación de informar de manera leal y transparente a los interesados sobre la finalidad o finalidades del tratamiento y el destino de sus datos de carácter personal (arts. 12 y 13 RGPD). Así las cosas, los proveedores de redes sociales deben informar a los potenciales usuarios, con el mayor detalle posible, sobre quién procederá al tratamiento de su información personal, con qué finalidades, si estos datos resultarán transferidos a terceras personas o entidades, así como los derechos que les asisten en defensa de su derecho fundamental a la protección de datos personales. En esencia, se trata de garantizar que el usuario conozca con la mayor exactitud posible, cuál será el destino de sus datos personales, para así, conservar el poder de control cuyo derecho a ejercer sobre los mismos conserva[408]. No debe sorprender el hecho de que, para que dicho control pueda ejercitarse correctamente, la información proporcionada por los proveedores de redes sociales deba arrojar una imagen clara y transparente sobre las finalidades y el destino de los datos personales que tratan. Sin embargo, la realidad resulta muy lejana a dicha afirmación, pues con destacado acierto a nuestro juicio, dispone GIL MEMBRADO que las políticas de privacidad no

[408] Concretamente, el art. 13 RGPD impone informar al interesado sobre varios aspectos para garantizar que el usuario conoce el destino de su información personal. En redes sociales, cobran especial relevancia aquellos que se exponen posteriormente en el enunciado del texto.

consiguen que el usuario comprenda cómo se utilizará la información que compartirá en la red[409].

Sobre este aspecto, el Informe sobre políticas de privacidad publicado por la AEPD en el año 2018, aporta una suerte de consideraciones de necesaria mención en el presente estudio[410]. Ciertamente, el organismo desempeña la labor de revisar las políticas de privacidad y formularios de recogida de diversas empresas *online*, con el fin de aportar recomendaciones para su mejora y adaptación a la normativa vigente. Como se verá, muchas de las observaciones realizadas en dicho documento, podrían contribuir a mejorar las políticas de privacidad de los proveedores de redes sociales, que tal y como ha quedado claro, también se encuentran obligados a informar a las personas interesadas sobre el tratamiento de sus datos personales previo a darse de alta en los servicios que estas ofertan al considerarse responsables del tratamiento.

Así, dispone el organismo que, conforme al art. 13 del RGPD, para que el consentimiento se considere informado, se precisa comunicar al interesado, al menos, los elementos cruciales que este precepto señala para que el interesado pueda valorar y formarse su juicio[411]. Sin embargo, las políticas de privacidad de las redes sociales, acostumbran a redactarse de un modo que entorpecen la transmisión de esa información de vital relevancia para los datos personales del usuario en orden a emitir un consentimiento que pueda reputarse válido. Además, con frecuencia, también omiten informaciones de carácter preceptivo exigidos por el art. 13 RGPD[412].

Como quedará de manifiesto en el presente trabajo, en el ámbito de las redes sociales, sin perjuicio de que todos los elementos enumerados han de informarse, deben

[409] GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 111.

[410] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022)

[411] La identidad del responsable del tratamiento; el fin de cada una de las operaciones de tratamiento para las que el consentimiento se solicita; qué tipo de datos se prevé recoger y utilizar; la existencia del derecho a retirar el consentimiento en cualquier momento; el destinatario o categorías de destinatarios de los datos personales; la información sobre el uso de los datos para decisiones automatizadas cuando resulte pertinente, incluida la elaboración de perfiles; y la información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas. (Art. 13 RGPD).

[412] Se muestra conforme con la afirmación PLATERO ALCÓN cuando afirma que, en ocasiones, en las políticas de privacidad de las redes sociales no aparece con detalle toda la información al respecto. PLATERO ALCÓN, A., *El derecho al olvido en internet. La responsabilidad civil de los motores de búsqueda y las redes sociales: estudio doctrinal y jurisprudencial, op. cit.*, p. 173.

transmitirse con especial cuidado los siguientes aspectos: el fin de cada una de las operaciones de tratamiento, en el sentido que, los proveedores de redes sociales acostumbran a tratar la información con diversos fines, debiendo detallar expresamente todos y cada uno de ellos; la existencia y puesta a disposición del usuario de la posibilidad de retirar el consentimiento en cualquier momento; los destinatarios o categorías de destinatarios con los que la información habrá de compartirse, debiéndose su relevancia a que los destinatarios de los datos tratados por la red social pueden alcanzar una cifra verdaderamente elevada a razón de la venta y marketing *online* que en sus plataformas se practica; por último, la información sobre adopción de decisiones individuales automatizadas y elaboración de perfiles, conducta que las redes sociales practican desde hace varios años y de la que no informan con claridad, como se verá.

A partir de las consideraciones realizadas por la AEPD en el documento citado, hemos considerado oportuno analizar la Política de privacidad de la red social Instagram[413], una de las plataformas más populares entre los jóvenes internautas. Intentaremos determinar si la misma se acomoda a las premisas y recomendaciones de la AEPD, en cuanto a su deber de informar[414]; así como a los requisitos para la emisión de un consentimiento informado válido, al amparo de la normativa vigente. De este examen se desprende que la política de privacidad de dichas plataformas, reviste aparente legalidad, esto es, menciona prácticamente todos los aspectos que al menos deben publicitarse con objeto de emitir un consentimiento informado por la persona interesada-futuro usuario. No obstante, se han podido detectar determinadas carencias en la política de privacidad que deberían subsanarse, especialmente cuando la persona interesada que desea acceder al servicio no alcanza la mayoría de edad.

Así las cosas, a la luz del art. 12 RGPD, la transmisión de la información que el art. 13 RGPD enumera, ha de practicarse de manera concisa, transparente y en un lenguaje claro y sencillo al fin de facilitar tanto la transmisión de la información, como la comprensión por parte los interesados de la información contenida en las políticas de privacidad. No obstante, como denuncia la AEPD, muchas de las políticas de privacidad

[413] La red social Instagram comparte política de privacidad con Facebook por pertenecer ambas al "Grupo Meta".
[414] A ello cabe añadir que las plataformas sociales Facebook, Instagram y WhatsApp son las que más usuarios poseen (todas ellas pertenecientes al mismo grupo). Informe anual sobre Aplicaciones y menores: un año atrapados detrás de las pantallas, *Qustodio*, Año 2020. Obtenido de https://qweb.cdn.prismic.io/qweb/10de139a-cb1c-488e-b0e9-f5becb01f32f_Informe+anual+de+Qustodio+2020+Informe+sobre+los+h%C3%A1bitos+digitales+de+los+menores_ES.pdf (última consulta el 4 de mayo de 2021).

analizadas carecen de concisión, pues se redactan en apartados extensos que disuaden al interesado de su lectura. En efecto, mientras que la política de privacidad de Instagram y Facebook (Grupo Meta), vigente hasta el 26 de julio de 2022 ya excedía de una longitud que no disuadiera de su lectura al encontrarse provista de 11 páginas en su versión descargable, tras la modificación de la misma en la fecha señalada, su longitud se ha extendido a 128 páginas. Evidentemente, la sola extensión del texto, disuade al usuario de su lectura, lo que conduce a este a no ejercitar de manera adecuada y concienzuda el derecho de control sobre la información personal.

Otro de los puntos controvertidos, se refiere a la falta de claridad, transparencia y sencillez del lenguaje utilizado. De acuerdo con MARTÍNEZ MARTÍNEZ, los proveedores de redes sociales, emplean un lenguaje aparentemente amable en sus políticas de datos para trasladar la información sobre el tratamiento de los datos personales[415]. Aunque ello no constituye sinónimo de claridad, transparencia y sencillez, a nuestro juicio. Sirva como ejemplo que la política de privacidad de Instagram emplea un lenguaje sencillo y amable en algunos de sus apartados, pero en muchas ocasiones, no aporta información clara de obligado acceso como, por ejemplo, e la identidad de otros responsables que también tratarán sus datos además de la propia red social. En efecto, la red social asegura que comparte la información sobre cada usuario con el fin de ayudar a anunciantes y otros socios, pero no detalla la identidad de estos[416].

La plataforma acostumbra a utilizar en exceso términos como “nuestros socios”, “anunciantes” o “colaboradores”, todos ellos sencillos, pero generalistas e indeterminados. De acuerdo con esta aseveración se muestra la AEPD cuando expresa en su documento que muchas de las políticas de privacidad de aseguradoras analizadas, señalan que “se podrá comunicar sus datos personales a las siguientes entidades aseguradoras, coaseguradoras y reaseguradoras y administraciones públicas”; pero aduce el organismo oficial que no se detalla a qué aseguradoras, coaseguradoras o

[415] MARTINEZ MARTINEZ, R., “Protección de datos personales y Redes sociales: un cambio de paradigma” en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales*, *op. cit.*, p. 94.

[416] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre ¿Cómo usamos tu información?, (última fecha de consulta el 21 de septiembre de 2022), p. 17.

reaseguradoras se refiere[417]. Lo mismo ocurre en el caso de Instagram y Facebook cuando la política de privacidad del grupo ejemplifica algunas de las categorías de socios y anunciantes pero no identifica a cada uno de estos[418]. Esta falta de mención, constituye un incumplimiento legal, pues informar sobre los destinatarios de la información resulta obligatorio para el responsable del tratamiento, al amparo del art. 13 RGPD. En cambio, se inclinan por el empleo de fórmulas basadas en un lenguaje ambiguo y poco claro, para ocultar sus tratamientos.

Así, nos preguntamos sobre la identidad exacta de esos socios que conocen la información personal que les proporcionan las plataformas Instagram y Facebook y de cuya identidad los usuarios no reciben información. En efecto, el usuario no posee la capacidad de controlar quiénes tratan su información personal en el contexto descrito, lo que conduce al incumplimiento del art. 5.1.a) RGPD que propugna la necesidad de informar de manera leal y transparente del destino de los datos personales. Además, el Grupo de Trabajo 29 afirma en su documento sobre las Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 28 de noviembre de 2017[419], que para los casos en los que los datos personales se transfieran a otros responsables que desean basarse en el consentimiento original, deberán nombrarse estas organizaciones en las políticas de privacidad. Dicha circunstancia no se cumple en el caso de estas redes sociales por lo que, incumplen la obligación de informar de manera leal y transparente del destino de la información personal[420].

En otras ocasiones, la política de privacidad abusa de tecnicismos que exceden del conocimiento medio de las personas usuarias. En relación con lo expuesto, mientras que la AEPD aconseja no emplear este tipo de palabras en las políticas de privacidad, la política de privacidad de Instagram y Facebook emplea variedad conceptos técnicos como, *plugins*, API, Píxel de Meta, etc. Esta práctica dificulta considerablemente al

[417] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022), p. 22.
[418] Véase al respecto la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#annotation-36 . Apartado ¿Cómo compartimos información con Socios, proveedores, prestadores de servicios y terceros?, (última fecha de consulta el 21 de septiembre de 2022), p. 35.
[419] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259, modificadas por las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión 1.1, de 4 de mayo de 2020 por el CEPD.
[420] Ello conduce a incumplir el principio de lealtad y transparencia en el sentido que, no se informa de los destinatarios de dicha información. (art. 5.1.a) RGPD).

interesado conocer qué tipo de información sobre su persona se recopila exactamente y qué tratamientos se practicarán sobre la misma[421].

En ese sentido, la transmisión de la información debe realizarse de un modo inteligible (art.12.1 RGPD). Esto es, no solamente mediante el empleo de un lenguaje aparentemente amable y sencillo, sino también comprensible para un usuario medio. Ello implica que las políticas de privacidad deban redactarse de tal modo que, permitan al usuario conocer con el mayor grado de exactitud posible el verdadero destino de su información personal para poder decidir sobre la prestación de su consentimiento. Efectivamente, la terminología empleada por el proveedor de la red social se expresa en términos sencillos cuando afirma que para mejorar la experiencia del usuario comparte datos con anunciantes, colegas de profesión o socios, pero resulta evidente la falta de claridad de la información. Sobre este particular, además, subrayar que la inteligibilidad de la información variará dependiendo del usuario al que se dirija, de modo que, el responsable del tratamiento debe realizar un esfuerzo añadido en conseguir que sus políticas de privacidad se comprendan por los usuarios más jóvenes (art. 12 RGPD).

Otro aspecto sobre el que corresponde informar de manera comprensible al interesado es el relativo a la finalidad o finalidades de cada uno de los tratamientos que se practicarán sobre los datos personales recabados, ya que solamente ante el conocimiento de dicha información podrá consentir a conciencia cada una de las finalidades aducidas. Destacar que, entre las finalidades de las redes sociales, la tradicional finalidad de tratar datos a efectos de poner a disposición de las personas usuarias una herramienta para socializar y crear comunidades de personas ya no constituye su único cometido. En efecto, entre sus fines secundarios, destacamos el empleo de los datos personales aportados por los usuarios, tanto los proporcionados al darse de alta, como los que comparte durante el uso de la red social para la comercialización directa de productos a estas e incluso información compartida con terceros responsables por el usuario. Para ello, los proveedores de redes sociales facilitan a terceras empresas los datos que las personas usuarias comparten en sus perfiles, además de elaborar perfiles a efectos de conceder al usuario unos servicios personalizados.

[421] Véase la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre ¿Cómo usamos tu información (última fecha de consulta el 21 de septiembre de 2022), p. 31.

Sin embargo, justifican dicha recogida por la personalización de la experiencia para el usuario, terminología que consideramos vaga e imprecisa dada la magnitud y alcance de los tratamientos realizados por la red social. Sobre este punto, el Grupo de Trabajo del Artículo 29 ha dispuesto en sus Directrices sobre el principio de la transparencia en virtud del RGPD, que constituyen prácticas deficientes, contrarias a un lenguaje claro y sencillo, enunciados tales como "podremos utilizar sus datos personales para ofrecerle servicios personalizados", ya que, de acuerdo con su opinión, el enunciado expuesto no aclara qué implica dicha personalización[422].

Es cierto que con la última actualización de la política de privacidad, se percibe una ligera mejoría en cuanto a procurar una explicación sobre qué información emplea la plataforma para la muestra de anuncios y otro contenido publicitario o comercial personalizado, pero en última instancia, los usuarios tampoco reciben una información que detalle exactamente cómo consiguen dicha personalización, y lo que reviste todavía mayor importancia, las consecuencias que acarrea para su información personal.

Con todo, en cumplimiento del Considerando 60 RGPD, los fines secundarios deben reflejarse con claridad, además de figurar de manera determinada y específica en las políticas de privacidad de estos proveedores de servicios[423]. Cuando nos referimos a informar de manera clara a las personas usuarias, no nos referimos únicamente a que las palabras empleadas revistan sencillez, sino a que debe explicarse al usuario la lógica aplicada en las operaciones de tratamiento. Sobre este aspecto, la AEPD ha manifestado, a modo de ejemplo, que informar a la persona usuaria de que se elaboran perfiles con su información personal, no resulta suficiente, exigiendo dicha actuación un esfuerzo añadido, consistente en explicar al interesado la importancia de esta actividad y las consecuencias que este tratamiento posee para su información personal[424].

En sintonía con lo expuesto, la nueva política de privacidad de Instagram y Facebook, deja entrever que se elaboran perfiles y se emplean algoritmos cuando afirma que para decidir qué anuncios y contenido comercial se muestra a cada usuario, la plataforma emplea las "asunciones que realizamos sobre ti". Ahora bien, el usuario medio

[422] Directrices del Grupo de Trabajo del Artículo 29 sobre la transparencia en virtud del Reglamento (UE) 2016/679, de 11 de abril de 2018, WP 260, p. 10.
[423] En efecto, el Considerando 60 RGPD dispone que los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento, así como de sus fines.
[424] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022), p. 27.

no deducirá de dicha expresión, que el proveedor de la red social se refiere a que elaborará perfiles con la información recabada. A mayor abundamiento, a pesar de que el art. 13.2.f) RGPD obligue al responsable, tampoco informan de la lógica subyacente en dichos tratamientos, ni tan siquiera en un hipervínculo cuyo cometido resida en ampliar la información sobre la personalización de los servicios[425].

De la lectura de la política de privacidad de Instagram y Facebook, no se deduce la gran cantidad de información personal recabada que comparten con millones de terceras entidades para finalidades diversas. De este modo, la información carece de total y absoluta transparencia. Ciertamente, no se llega a informar al usuario sobre la complejidad de las operaciones constantes que estas realizan con la información personal de los usuarios; en consecuencia, no pueden ejercitar un control eficaz sobre su información personal. Este comportamiento colisiona, a su vez, con el principio de limitación de la finalidad (art. 5.1.b) RGPD), por cuanto que este principio obliga a los responsables del tratamiento a exponer los fines determinados, explícitos y legítimos para los que tratarán dicha información. Sin embargo, la realidad demuestra cómo las redes sociales abogan por la vaguedad en la determinación de las finalidades de tratamiento, pudiendo ello conllevar la práctica de tratamientos no previstos inicialmente.

Esta circunstancia resulta especialmente grave, dado que, de conformidad con TRONCOSO REIGADA, los fines del tratamiento han de determinarse de manera previa a la recogida, debiendo quedar estos identificados de manera precisa y completa, además de resultar específicos, esto es, la determinación de la finalidad prohíbe los tratamientos para finalidades vagas e inconcretas[426]. En efecto, no se debe permitir que las políticas de privacidad informen de las finalidades de manera vaga o redactadas de modo ambiguo, pues favorecen la posible práctica de tratamientos inicialmente no previstos sin que el

[425] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre Cómo mostramos anuncios y otro contenido comercial pp. 17-18 (última fecha de consulta el 21 de septiembre de 2022)

[426] TRONCOSO REIGADA, A., "Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)", *op. cit.*, pp. 861-862. En ese sentido se manifiesta también DEL CASTILLO VÁZQUEZ cuando señala que no se admite el consentimiento otorgado para un fin tan vago o general que, en la práctica, suponga un riesgo para los derechos y libertades de las personas físicas por dar cobertura a un universo de posibilidades para usos imprevistos de los datos, con los que no contaba el interesado. DEL CASTILLO VÁZQUEZ, I.C., "Consentimiento (Comentario al art. 4.11 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, p. 687.

usuario advierta dicha circunstancia, lo que a su vez dificulta que este pueda ejercitar un control sobre su información personal tratada con fines diferentes a los consentidos.

Por otro lado, la normativa sobre protección de datos personales prevé que los proveedores de redes sociales, traten los datos personales de conformidad alguna de las bases legales que justifiquen dicho tratamiento para considerar el tratamiento lícito (art. 6 RGPD) y por ello, el art. 13.1.c) RGPD impone a los responsables del tratamiento informar sobre la base legal aplicable a cada una de las finalidades de tratamiento alegadas. De este modo, Instagram y Facebook prevén diversas finalidades de tratamiento en cada una de las bases legales que la normativa europea obliga. Sin embargo, entendemos conveniente realizar una serie de consideraciones a este respecto. En primer lugar, tanto Facebook como Instagram alegan en su políticas de privacidad compartida, que acometen el tratamiento de datos personales en orden a prestar sus servicios contractuales sobre las siguientes finalidades, a saber: proporcionar, personalizar y mejorar sus productos; fomentar la seguridad, la integridad y la protección; comunicarse con el cliente; para la realización de tareas de investigación e innovación en aras del bienestar social; por último, para ofrecer servicios de medición y análisis a empresas. No obstante, a nuestro juicio, de su lectura no queda claro qué tratamientos se incluyen como esenciales para la prestación del servicio de la red social y cuáles para otros fines.

Principalmente, la finalidad de las redes sociales debería consistir en proporcionar un espacio para fomentar la interacción de las personas usuarias, conducta que, no se refleja en dicha enumeración. Expresiones ambiguas como “proporcionar, personalizar y mejorar nuestros productos de Facebook” no aclaran qué tratamientos de datos resultan necesarios para ello. En ese sentido, véase que para que los usuarios socialicen, la “personalización” no es necesaria para la correcta prestación de dicho servicio. Es más, originariamente, la publicidad, anuncios y mercadotecnia no tenían cabida en las mismas, por lo que, en efecto, lo que evidencia que este servicio no resulta indispensable.

En la línea con lo expuesto, la versión descargable de la política de privacidad, que redirige en excesivas ocasiones a otros documentos para completar la información, solo aclara qué bases jurídicas han de aplicarse a cada una de las finalidades del tratamiento en uno de los muchos hipervínculos disponibles. En efecto, la política de privacidad enumera las bases legales sobre las que descansan los tratamientos de datos personales que practican, pero en ningún caso vincula específicamente la base legal aplicable a cada una de las finalidades para las que tratan los datos, contraviniendo el art.

13.1.c) RGPD que impone dicho deber[427]. En consecuencia, el usuario no conoce de manera clara, sencilla, ni rápida qué finalidades debe consentir, cuáles resultan imprescindibles para la prestación del servicio, o, en definitiva, cuáles constituyen parte del interés legítimo del prestador del servicio, entre otras. Todo ello conduce al potencial usuario-interesado a aceptar sin elementos de valoración la política de privacidad, ante la complejidad de conocer el verdadero destino de su información personal, además de imposibilitar el conocimiento por parte de este de qué derechos le asisten dependiendo de las bases legales aplicadas a cada una de las finalidades.

Con todo, denunciamos que la política de privacidad del Grupo Meta, además de presentar determinadas carencias, contraviene el art. 5.1.a) RGPD, pues estas determinan que los consentimientos recabados por diversas redes sociales puedan no reputarse válidos cuando la base legal que justifica el tratamiento es el consentimiento. Entre las carencias destaca, por una parte, que la lectura completa de las mismas resulta ardua y complicada; por otra parte, a la extensa longitud del documento sobre la política de privacidad, debe agregarse que el empleo de pluralidad de hipervínculos a otras informaciones que la AEPD califica de positivo[428], debe realizarse de un modo que facilite el conocimiento al usuario de la información indispensable sobre el tratamiento de datos, no lo contrario. Consideramos que la fórmula empleada por los proveedores de redes sociales provoca en el usuario el deseo de desistir de su lectura al obligar a este a acceder en más de una veintena de hipervínculos durante la lectura de la política de privacidad. A la conducta expuesta se debe añadir que se omiten o relegan a un segundo nivel informaciones que deberían colocarse en el primero. En efecto, el CEPD afirma que la sinergia entre las distintas páginas debe configurarse de tal modo que no contribuya a aumentar la confusión, sino a reducirla[429]. Más aún, de la lectura sin hipervínculos que se

[427] En ese sentido, la autoridad irlandesa de protección de datos (*Data Protection Commission of Ireland*) ha sancionado al Grupo Meta por no informar de manera transparente a los usuarios sobre la base legal aplicable a la finalidad del tratamiento que persigue ofrecer a los usuarios publicidad comportamental. Así, sobre esta cuestión el CEPD emitió su decisión vinculante de disputa el pasado diciembre de 2022, *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)*, adopted on 5 december 2022. Obtenido de: https://edpb.europa.eu/system/files/202301/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf (última consulta el 30 de enero de 2023).

[428] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022), p. 31.

[429] Directrices 4/2019, del Comité Europeo de Protección de Datos sobre protección de datos desde el diseño y por defecto, de 20 de octubre de 2020, p. 16.

ha realizado con el fin de comprobar la comprensión de estas políticas de privacidad, gran parte de la información no ofrece una imagen clara sobre los tratamientos a realizar ni es comprendida en su totalidad por el interesado.

Estrechamente relacionado con lo expuesto, de la lectura en conjunto de las políticas de privacidad de estos espacios, no se desprende una idea clara sobre los tratamientos de datos personales del futuro usuario al prestar el consentimiento, es decir, no se informa de modo transparente de los fines para los que los datos habrán de tratarse ni los destinatarios de los mismos. En estas circunstancias, resulta complejo garantizar un poder de control, en el sentido que, no existe manera de conocer qué entidades llegan a tratar información personal que se comparte en la plataforma (destino), ni cuáles resultarán los tratamientos practicados (finalidad o finalidades). Así pues, el contenido esencial del derecho fundamental a la protección de datos personales queda desvirtuado al consentir el tratamiento de datos personales a estas plataformas electrónicas.

Sentado cuanto antecede, en el ámbito de las redes sociales, el consentimiento de los usuarios no se encuentra correctamente informado. Es así que, este hecho puede derivar en la invalidez de los consentimientos prestados por los futuros usuarios de la red social y en definitiva encontrarnos ante tratamientos que contravienen el principio de licitud del tratamiento consagrado en el art. 6. RGPD. En efecto, en el ámbito de las redes sociales, el consentimiento no se constituye como una base legal válida que legitime el tratamiento de datos personales de los usuarios. Concretamente, el consentimiento no puede considerarse informado (art. 4.11 RGPD) dado que, la información aportada por los proveedores de redes sociales carece de concisión y transparencia, además de no emplear un lenguaje claro ni sencillo para el usuario (art. 5.1.a) RGPD y art. 12 RGPD) lo que conduce a su vez, a un tratamiento desleal[430]. Por otra parte, tampoco se informa de todos los extremos que mínimamente habrán de informarse al interesado en virtud del art. 13 RGPD. Por último, la falta de transparencia en las políticas de privacidad provoca el incumplimiento del principio de limitación de la finalidad (art. 5.1.b) RGPD), por cuanto que no se informa de los fines concretos, determinados y explícitos de tratamiento,

[430] Véase que incluso faltan a la verdad en sus políticas de privacidad, pues mientras afirman en esta que no vende la información personal de los usuarios y nunca procederán de tal modo, a posteriori reconocen en ese mismo texto que proporcionan a los anunciantes informes sobre la cantidad y el tipo de personas que visualizan sus anuncios e interactúan con ellos. Véase la política de privacidad del Grupo Meta en vigor a partir del 26 de julio de 2022, disponible en la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre ¿Cómo usamos tu información (última fecha de consulta el 21 de septiembre de 2022), p. 31.

constituyéndose la vaguedad e imprecisión en su redacción como la principal causante de ello.

En este sentido, podemos establecer, con cautela, un paralelismo con sectores económicos como la banca, en los que la falta de información ha implicado la nulidad de la contratación acaecida[431]. Nos referimos a la contratación por medio de condiciones generales propugnada por el sector bancario, en el que muchas de las cláusulas se anularon en virtud de la falta de información que explicara la entidad económica real de la contratación a los usuarios[432]. Nos preguntamos, si cabría establecer esta misma conclusión en el tratamiento de datos personales, que descansa sobre la base de un consentimiento erróneamente formado ante la ausencia de información que aclare los diversos extremos sobre el tratamiento.

Estas afirmaciones adquieren mayor rotundidad en el caso de menores de edad, por su limitada capacidad para comprender muchas de las informaciones contenidas en la política de privacidad de las redes sociales, de modo que, su *habeas data* queda notoriamente debilitado e incluso inexistente. Cabe mencionar, además, que el Considerando 58 del RGPD y el art.12.1 RGPD velan por el refuerzo de la posición del menor en este campo obligando a los responsables del tratamiento a emplear un lenguaje claro y sencillo que resulte fácil de entender a efectos de garantizar una protección específica del menor. Reiteramos que, lenguaje fácil y sencillo no debe confundirse con proporcionar una comprensión real sobre el tratamiento de datos que se prevé realizar sobre la información personal. Para los casos de usuarios menores de edad debería obligarse legalmente a los proveedores de servicios de redes sociales a la redacción de políticas de privacidad adaptadas al público menor de edad en orden a cumplir con las premisas expuestas por la normativa[433]. Lamentablemente, la política de privacidad empleada por estas plataformas resulta idéntica para personas mayores y menores de edad, lo que, sin duda, conduce a afirmar que estas plataformas no se adaptan al

[431] Sobre la relevancia de la transparencia en el sector financiero, véase TOMÁS MARTÍNEZ, G., y GÓMEZ URQUIJO, L., "La protección al cliente bancario en el nuevo marco de la gobernanza financiera europea. Breve comentario a la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios", *Diario La Ley*, 2012, núm. 7842, versión en línea sin paginación.

[432] Sentencia del Tribunal Supremo 241/2013, de 9 de mayo de 2013, ponente Excmo. Sr. Rafael Gimeno-Bayón Cobos, (Ref. Aranzadi RJ 2013/3088).

[433] Véase GIRÓN REGUERA, E., "La protección de datos de los menores de edad en internet", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 4277.

cumplimiento de la normativa sobre protección de datos personales, y además de tampoco observa el interés superior del menor.

Sobre esta obligación en relación a las políticas de privacidad destinadas a los menores de edad, queda mucho camino por recorrer. Ello se debe principalmente a que los menores no son conscientes del verdadero destino y finalidad de sus datos personales, así como quién controlará el acceso a la información que revelan ni, en definitiva, las implicaciones que ello conlleva para sus derechos de la personalidad[434]. En esta circunstancia, los propios proveedores de redes sociales no facilitan que el menor comprenda los extremos detallados, es más, contribuyen a generar confusión sobre los aspectos más relevantes para que el consentimiento se forme correctamente[435].

En definitiva, deberá obligarse legalmente a los prestadores de estos servicios a informar de manera clara y sencilla de la lógica aplicada de los tratamientos que realizan y los derechos que asisten al usuario. De lo contrario, de conformidad con TRONCOSO REIGADA, existe una apariencia de consentimiento, pero el incumplimiento del principio de información determina la ausencia de un consentimiento informado[436]. Nos unimos así a las voces que reclaman mayor transparencia, claridad y sencillez en la redacción de las políticas de privacidad. Destacan entre estas, las palabras de ORTIZ LÓPEZ cuando afirma que, la redacción de políticas de privacidad claras y transparentes es precisa para garantizar al usuario elementos de control sobre su información personal[437]. Sin embargo, lamentamos que la doctrina no realice aportaciones más concretas suficientes al fin de solventar los problemas de transparencia de las políticas de privacidad. Sin perjuicio de lo afirmado, se presentan algunas de las soluciones planteadas como sigue.

---

[434] Véase SANTAMARÍA RAMOS, J.F., "Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (Comentario al artículo 95 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 4302.

[435] Sobre este particular, cabe mencionar que el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE de servicios digitales, impone a las plataformas digitales en su art. 14.3 un esfuerzo especial a efectos de garantizar una mejor comprensión por parte de los jóvenes de las condiciones de sus servicios. En efecto, aboga por reforzar la transparencia en este ámbito. Sin duda, medida que consideramos necesaria.

[436] TRONCOSO REIGADA, A., "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una". *op. cit.*, p. 74.

[437] ORTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales, op. cit.*, p. 35.

En relación a la concisión, tomando en consideración el Considerando 166 RGPD y el art. 12.7 RGPD, la doctrina propone la incorporación de iconos en las políticas de privacidad con la finalidad de resumir la información legal a efectos de recabar un consentimiento informado[438]. Concretamente, el sistema procura eliminar la complejidad y cansancio presentes en la lectura de estos documentos, pues afirman sus creadores que un 97% de los usuarios no dedica más de 30 segundos a la lectura de estos textos; desde luego, un tiempo manifiestamente insuficiente para interiorizar y comprender la información a efectos de emitir un consentimiento informado. Es más, según disponen sus promotores, la lectura de todas las condiciones legales de los servicios, aplicaciones y productos requiere la necesidad de dedicar más de un mes a su lectura.

Con todo, el objetivo del sistema *Consent Commons* se encuentra en facilitar de un vistazo la información que se debe mostrar al titular de los datos personales. De este modo, el sistema propuesto incluye una serie de iconos diseñados desde la observancia de las Guías de Privacidad de las Agencias españolas de protección de datos citadas en el presente apartado. En última instancia, el usuario de estos servicios ha de comprender de manera sencilla y transparente, además de rápida a través de las grafías, las diversas vicisitudes del tratamiento expuestas en la política de privacidad.

No obstante, si bien la iniciativa resulta loable, consideramos que el propósito de informar al usuario con mayor transparencia y de la manera más rápida posible, dada la falta de paciencia en la lectura de estas políticas de privacidad por parte de estos, puede verse frustrado. En efecto, de manera previa a la implementación de este sistema, debería instruirse de manera generalizada a la ciudadanía en el significado de todas y cada una de las grafías empleadas para cada extremo a informar, dado que, de lo contrario, el usuario tampoco recibiría la información preceptiva a efectos de emitir un consentimiento informado. Nótese que, las propias grafías, sin aclaración sobre su significado, no transmiten la información preceptiva a efectos de emitir un consentimiento suficientemente informado.

[438] Para mayor detalle sobre el sistema "Consent Commons" creado por LLANEZA, P., véase su página web: https://consentcommons.com/el-sistema/ (última consulta el 28 de septiembre de 2021). Este sistema, se encuentra disponible para aquellas empresas que deseen incorporar el mismo en sus políticas de privacidad.

De conformidad con VILASAU SOLANA, el empleo de este método, debería producirse siempre de modo complementario a la información escrita plasmada en la política de privacidad y nunca de manera sustitutiva. Ya que, de adoptarse de modo similar al etiquetado de productos alimenticios, muchas informaciones vitales para el titular de los datos personales, quedarían sin transmitir a causa de la simplificación de información que las grafías conllevan[439]. A nuestro juicio, constituye este el mayor inconveniente de la propuesta realizada en el sentido que, los usuarios pueden consentir el tratamiento desconociendo totalmente el significado de las grafías y, en consecuencia, desinformados.

Tomamos conciencia de lo difícil que pude resultar lograr un equilibrio entre informar de manera concisa pero clara y detallada a su vez. De ahí que, a nuestro juicio, los proveedores de redes sociales deberán combinar diversas técnicas que procuren el señalado objetivo. En ese sentido, puede resultar de utilidad a la hora de redactar las políticas de privacidad, incorporar el modelo de información por capas o niveles propuesto por las Agencias de Protección de datos personales española, vasca y catalana a efectos de aportar claridad a la información dispuesta[440].

Este modelo, propone la presentación de la información desde un enfoque multinivel a efectos de proporcionar concisión y comprensión en la forma de presentarla. En concreto, el sistema propuesto consistente en presentar, por un lado, una información básica resumida en un primer nivel sobre los aspectos cuya mención resulta obligatoria en virtud del RGPD. Por otro lado, remitir la información adicional a un segundo nivel, donde se concretarán detalladamente las informaciones restantes.

Consideramos que, de implementar adecuadamente el método propuesto por las autoridades de control señaladas, la información podría resultar más accesible y concisa para el usuario facilitando su lectura y comprensión. No obstante, la labor deberá desarrollarse de manera meticulosa, pues el empleo del modelo de información por capas, no resulta suficiente con el fin de cumplir la obligación de transparencia, sino que, los

[439] VILASAU SOLANA, M., "Las exigencias de información en el RGPD y la LO 3/2018, de protección de datos y garantía de los derechos digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?", en GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (editoras), *Protección de Datos. Un enfoque nacional y comparado*, Valencia, Tirant lo Blanch, 2019, p. 230.

[440]. Guía de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; AGENCIA CATALANA DE PROTECCIÓN DE DATOS; AGENCIA VASCA DE PROTECCIÓN DE DATOS para el cumplimiento del deber de informar. Obtenido de: https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/modeloclausulainformativa-es.pdf (última consulta el 10 de mayo de 2021), pp. 7 y ss.

contenidos concretos que habrán de exponerse en cada nivel también precisan de una revisión exhaustiva por parte de los proveedores de redes sociales. Por una parte, en un primer nivel deberá informarse de aquellas cuestiones que de manera básica el art. 13 RGPD obliga, relegando a un segundo nivel solamente informaciones complementarias. En efecto, los proveedores de redes sociales no deberán emplear este método con el fin de omitir informaciones que deberían colocarse en un primer nivel. Por otra parte, con el fin de considerar la transmisión de dicha información acorde a la concisión, transparencia y sencillez que el art. 12 RGPD impone, los contenidos de ambos niveles deben explicarse con claridad, esto es, aportando una imagen clara al usuario sobre el destino de su información personal en un lenguaje inteligible para este.

En esencia, de lo que se trata es se conozca el destino y finalidades de tratamiento, es decir, que el usuario conozca de manera real, efectiva y exacta la información requerida para la emisión de un consentimiento informado válido. Véase que ese conocimiento previo deviene imprescindible a la hora de valorar la idoneidad de la prestación del consentimiento para los fines y destino propuesto. Por el contrario, la falta de información, así como la vaguedad e imprecisión por parte de los proveedores de redes sociales en la transmisión de dicha información provocan desconfianza en el usuario a la hora de prestar el consentimiento.

Lejos de concluir con los problemas sobre esta fase del consentimiento informado, en el proceso de alta, el usuario debe decidir el grado de privacidad de su perfil. En caso de configurarlo de modo público, la totalidad de red podrá acceder a la información que se comparta en el mismo; por el contrario, existen funciones para restringir el acceso de terceras personas al mismo. Ahora bien, los proveedores de redes sociales activan por defecto, el mayor grado de publicidad del perfil, relegando a un momento posterior la responsabilidad del usuario el cambio a una configuración más restrictiva de este. Ello colisiona con el Considerando 78 y el art. 25 del RGPD que propugnan la protección de los datos personales desde el diseño y por defecto, en el sentido que, el diseño de esta funcionalidad no se ha meditado suficientemente en aras de proteger los datos personales de los usuarios de redes sociales.

En este sentido, de acuerdo con el Grupo de Trabajo del Artículo 29, los perfiles de menores deberían configurarse, por defecto, con el mayor grado de privacidad

posible[441]. En esa línea se manifiesta también la Comisión Europea al advertir que, solamente el 56% de los menores entre 11 a 12 años dice saber modificar los parámetros de confidencialidad en línea, para lo que propone que se predefinan previamente los parámetros de confidencialidad de usuarios menores de edad[442].

A pesar de no constituir una medida que por sí misma pueda garantizar en su totalidad la protección de la información personal de los más jóvenes, sí que puede contribuir a reducir los tratamientos de datos ilícitos. Ello se debe, principalmente, a que no todo usuario de la red contará con acceso a las informaciones, lo que mitiga el riesgo de que la información circule en la red, pero no lo excluye[443].

En ese sentido, el Reglamento europeo 2022/2065 por el que se aprueba un mercado único de servicios digitales, acoge la medida expuesta en su Considerando 89, cuando aboga por adaptar el diseño e interfaz de las plataformas digitales en los casos en los que el usuario no alcance la mayoría de edad al fin de proteger su interés superior. Así, creemos que, la medida debe recibir una valoración positiva, pero como se verá posteriormente, su implementación no goza de sencillez.

Por último, apreciamos un problema, en relación a la participación activa del usuario que, creemos conveniente visibilizar en el presente epígrafe. Según ha quedado expuesto en el presente trabajo de investigación, el usuario puede convertirse, a su vez, en responsable del tratamiento de datos personales en determinadas circunstancias que ya se han visibilizado en el presente estudio. Sin embargo, ninguna política de privacidad advierte de la eventual consideración del usuario como responsable del tratamiento en determinadas circunstancias. Así, consideramos que los proveedores de redes sociales deberían informar al usuario sobre esta posibilidad en sus políticas de privacidad. El razonamiento expuesto, se desprende del ya citado informe 5/2009 del Grupo de Trabajo 29, cuando aconseja a los proveedores de redes sociales recuerden a los usuarios que compartir en línea información relativa a otras personas puede perjudicar a su derecho a la intimidad y a la protección de datos personales. No obstante, las políticas de privacidad no advierten, que en determinadas circunstancias la publicación de información sin

[441] Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, pp. 13-14.
[442] Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones una "Estrategia europea en favor de una Internet más adecuada para los niños", del 2 de mayo de 2012, COM (2012) 196 final, pp. 6 y 12.
[443] Recordemos en este punto que la información puede resultar objeto de captura por un usuario que sí se encuentra en el círculo de amigos y ser este quien, con carácter posterior, difunde la información.

consentimiento necesario, puede suponer un incumplimiento de las obligaciones del responsable de un tratamiento. A nuestro juicio, dicha advertencia debe visibilizarse en las políticas de datos, para que los usuarios conozcan las eventuales implicaciones a la hora de compartir información de terceras personas en las plataformas sociales[444]. En el caso de que, sean menores de edad quienes desean darse de alta, esta función debería impedirse, ante la falta de madurez manifiesta para asumir las obligaciones de un verdadero responsable de tratamiento de datos personales.

Para ello, a nuestro juicio, pueden resultar de especial interés las siguientes medidas: por una parte, no permitir a jóvenes usuarios configurar el perfil de modo público tal y como se ha afirmado hace escasas líneas, ya que de esta manera el tratamiento queda al abrigo de su actividad doméstica, y en consecuencia, no asume la obligación de un responsable del tratamiento. Por otra parte, podría resultar útil informar a los usuarios menores de edad de la importancia de no aceptar peticiones de amistad de usuarios desconocidos, dado que un número elevado de contactos podría conllevar, igualmente, la asunción de las obligaciones legales del responsable del tratamiento.

Sin perjuicio de que, el menor pueda no considerarse responsable del tratamiento al no cumplir las premisas para ello recientemente detalladas, creemos conveniente incidir en que, el etiquetado de terceras personas en fotografías, constituye un tratamiento de datos personales tal y como dispone ENISA. En su informe "Temas de seguridad y recomendaciones para redes sociales *online*"[445], sienta que se requerirá del consentimiento de la persona afectada para su publicación y etiquetado. Esta circunstancia, debe contemplarse en las políticas de privacidad para una mayor información de los usuarios.

[444] Tómese en cuenta que cada vez con mayor asiduidad, personas particulares pueden considerarse responsables del tratamiento sujetos a las obligaciones legales que un responsable ha de garantizar. A modo de ejemplo, los *Influencers*, esto es, personas que se dedican a mostrar sus hábitos en redes sociales, además de publicitar productos de determinadas marcas, asumen dicha responsabilidad con el normal desempeño de su actividad laboral. En consecuencia, en caso de tratar datos de terceras personas, como subir fotografías con ellas, deberán recabar el consentimiento preceptivo de estas. Pero no solo eso, eventualmente también deberían garantizar el resto de premisas y derechos que los titulares del derecho a la protección de datos presentan, como, por ejemplo, el derecho de oposición o rectificación.

[445] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, *Security Issues and Recommendations for Online Social Networks*, Position paper, núm. 1, de octubre 2007, p. 21.

4.1.2. La configuración online de la prestación del consentimiento vs. la normativa sobre protección de datos personales

El art. 4.11 RGPD establece que se entiende por consentimiento del interesado, toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Antes bien, se debe analizar si el sistema de prestación del consentimiento en línea implementado por los proveedores de redes sociales respeta la normativa vigente.

Así, la AEPD insiste en que se debe informar al usuario de manera previa a la recogida de datos sobre el tratamiento que se practicará respecto de su información personal[446]. Cierto es que dicha se cumple por los proveedores de redes sociales, pero creemos necesario matizar algunas cuestiones. Al amparo del art. 12 RGPD, dicha información ha de resultar de fácil acceso. Sin embargo, las páginas de registro de estas plataformas disponen en su pie de página un hipervínculo a las políticas de privacidad, en el que el tamaño de la fuente y el color empleados para identificarlas no persuaden al usuario a abrir dichos hipervínculos y proceder a su lectura. Conviene subrayar sobre este punto que el Grupo de Trabajo del Artículo 29 rechaza la colocación o las combinaciones de colores que propician que un texto o enlace revistan menor visibilidad u ocasionen una dificultad a la hora de encontrar información en una página web, ya que, estos comportamientos, reputan dicho modo de disponer la información de difícil acceso[447].

A nuestro juicio, debería constituir una obligación para estos proveedores, que entre sus pasos para registrarse en la plataforma se desplegara de manera automática la política de privacidad. Creemos que resulta más conveniente de este modo, pues de otra manera, el usuario puede darse de alta incluso sin reparar en la existencia de la política de privacidad[448]. En efecto, de conformidad con ARIAS POU, el responsable del tratamiento debe "facilitar" la información, lo que necesariamente conlleva una acción

[446] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022), p. 5.
[447] Directrices del Grupo de Trabajo del Artículo 29 sobre la transparencia en virtud del Reglamento (UE) 2016/679, de 11 de abril de 2018, WP 260, p. 9.
[448] En ese sentido, resulta ilustrativo un estudio realizado a 190 jóvenes, disponible en DURÁN SEGURA, M., Y MEJÍAS PELIGRO, J.F., "Conocimientos y comportamientos de los usuarios de la red social Facebook relacionados con la privacidad", *Ámbitos: revista internacional de comunicación*, 2014, núm. 26, p. 556, en el que los autores afirman que el 64% de los jóvenes entre 20 y 35 años encuestados, nunca se ha leído la política de privacidad de la compañía.

del responsable por la que activamente pone a disposición la información sobre el tratamiento al usuario[449]. En ese sentido, cuestionamos si la puesta a disposición de un modo tan residual del hipervínculo en el formulario de registro cumple con dicha acción de "facilitar" la información activamente. Estos comportamientos no predisponen ni garantizan en suficiente medida el poder de control sobre los datos personales. Véase que concurre una gran dificultad en conseguir que los menores lean las políticas de privacidad, auspiciada por este *modus operandi* de las redes sociales[450].

A la presente preocupación, debemos agregar que el consentimiento no puede obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio[451]. Sin duda alguna, esta obligación que impone el art. 7.2 RGPD supone un escollo importante para muchas de las redes sociales, que como en el caso de Instagram y Facebook, la acción que sirve para aceptar los términos legales o "condiciones" ser la misma que para aceptar la política de privacidad de la plataforma. En definitiva, la aceptación global de los términos y condiciones generales no puede considerarse como una clara acción afirmativa destinada a prestar el consentimiento al uso de datos personales tal y como dispone el Grupo de Trabajo del Artículo 29 en las Directrices sobre el consentimiento en el sentido del Reglamento de la Unión Europea[452].

Coincidimos con DEL CASTILLO VÁZQUEZ cuando afirma que las finalidades que reciban acomodo en un consentimiento único otorgado de forma genérica para un conjunto de actividades de tratamiento y que se mezclen con otros mensajes como las condiciones de uso, no gozarán de la legitimación requerida, aparejando este

[449] ARIAS POU, M., "Transparencia e información que deberá facilitarse cuando los datos personas se obtengan del interesado. El derecho a la información desde el diseño (comentario al artículo 13 RGPD y al artículo 11.1 y 2 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.,* p. 1374.

[450] Solamente un 6% de los menores lee las políticas de privacidad. GARCÍA-ATANCE GARCÍA DE MORA, M.V., "Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación (TIC)", *op. cit.,* p. 1279.

[451] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259 modificadas por las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020, p. 18.

[452] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259 modificadas por las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020, p. 18.

comportamiento, que los tratamientos practicados en las circunstancias expuestas se reputen ilícitos[453].

A lo expuesto cabe añadir que la AEPD dispone que debe recabarse un consentimiento para cada una de las finalidades del responsable[454]. En efecto, tal y como afirma GIL MEMBRADO, no cabe configurar un consentimiento de modo indiscriminado que abarque todo tipo de fines[455]. En cambio, los proveedores de redes sociales recaban un consentimiento calificado por el organismo oficial como, "en bloque", lo que, sin duda debe reputarse como una conducta no recomendada, al no adaptarse a la normativa vigente (art. 6.1.a) RGPD). Efectivamente, las redes sociales ponen a disposición del usuario una única casilla para consentir el tratamiento de datos personales cuando de la lectura de sus políticas de privacidad se deducen, al menos, cinco finalidades distintas[456]. Para que dicho tratamiento pueda considerarse lícito, las redes sociales deben recabar el consentimiento por separado para cada una de las finalidades descritas, de lo contrario, se reputará como un consentimiento prestado sin libertad[457]. Recordemos igualmente que también deben informar sobre la base legal aplicable a cada una de las finalidades, pues, de lo contrario, el usuario no conoce cuáles de todas las finalidades consiente.

Es cierto que al regir la libertad de forma sobre este aspecto, se admite como forma válida de prestar el consentimiento la marcación de una casilla en una página web o red social, tal y como ha establecido la propia AEPD[458]. Dicha opción se ha sostenido, con carácter posterior, por el Considerando 32 del RGPD cuando establece que el

---

[453] DEL CASTILLO VÁZQUEZ, I.C., "Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (comentario al artículo 7 RGPD y al artículo 6 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, p. 950.

[454] Informe de la AEPD sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022), p. 30.

[455] GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 115.

[456] En ese sentido, la AEPD ha apercibido a determinadas empresas por no diferenciar el consentimiento para cada una de las finalidades del tratamiento. Véase el Procedimiento Sancionador 00388/2020. Obtenido de: https://www.aepd.es/es/documento/ps-00388-2020.pdf (última consulta el 5 de enero de 2022).

[457] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259, p. 11.

[458] Informe 0300/2009 de la AEPD, Gabinete jurídico, Madrid. En dicho Informe, la AEPD afimra que la marcación de la casilla "acepto" por parte del usuario implica la prestación del consentimiento al tratamiento de sus datos personales.

consentimiento debe proporcionarse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos carácter personal que le conciernen, y en ese sentido, el silencio, las casillas ya marcadas o la inacción no constituyen consentimiento. De igual modo, apunta que el consentimiento ha de otorgarse para todas las actividades de tratamiento realizadas con el mismo fin o los mismos fines. Para el caso de que el tratamiento albergue varios fines, debe prestarse un consentimiento para cada uno de ellos.

Sin embargo, las casillas que se han de marcar para una correcta prestación del consentimiento deberían configurarse de tal modo que, cada una de las finalidades fuera provista de su respectiva casilla. De lo contrario, la conducta señalada se corresponde con la prestación de un consentimiento que no se ha otorgado de manera específica e inequívoca e inevitablemente conduce a un incumplimiento normativo, pues los proveedores de redes sociales practican un tratamiento ilícito de datos personales[459].

Adviértase que la red social no permite culminar el registro en caso de no aceptar en bloque la totalidad de la política de privacidad. Es cierto que, con carácter posterior, permite retirar el consentimiento sobre las finalidades que el usuario no desee consentir; no obstante, a nuestro juicio, no es habitual que los usuarios cambien dicha configuración una vez dados de alta. La red social aprovecha esta circunstancia a efectos de garantizarse el consentimiento de la totalidad de las finalidades[460].

En efecto, el mecanismo diseñado por los proveedores de estos servicios, no garantiza la prestación del mismo de manera libre y específica a pesar de que el Considerando 43 del RGPD y el art. 7.4 RGPD advierten expresamente de la falta de

[459] En efecto, con manifiesto acierto afirma DEL CASTILLO VÁZQUEZ que el acceso a los servicios de redes sociales no puede condicionarse a la prestación de un consentimiento para recibir publicidad comportamental, pues el usuario ha de poder prestar su consentimiento de manera libre y específica para recibir este tipo de publicidad, independientemente de su deseo de ser usuario de la red social. DEL CASTILLO VÁZQUEZ, I.C., "Consentimiento (Comentario al art. 4.11 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. op. cit.*, 2021, p. 688.

[460] A mayor abundamiento, la propia política de privacidad del Grupo Meta advierte que la prestación de sus servicios puede verse afectada en caso de no consentir el tratamiento de datos. Véase la política de privacidad del Grupo Meta en vigor a partir del 26 de julio de 2022 disponible en la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , (última fecha de consulta el 21 de septiembre de 2022).

libertad en la prestación del consentimiento cuando el mismo no permite autorizar por separado las distintas operaciones de tratamiento de datos personales. De conformidad con DEL CASTILLO VÁZQUEZ, no habrá libertad en la prestación del consentimiento si el responsable del tratamiento decide practicar varias finalidades, pero no recaba el consentimiento para cada una de ellas[461]. La conducta correcta consistiría en permitir el registro aceptando solamente aquellas finalidades que el usuario desee, en virtud del poder de control que este posee, pero no forzándole a aceptar finalidades que a posteriori puede desactivar[462].

Por otra parte, el consentimiento debe poder retirarse en cualquier momento sin que el interesado sufra perjuicio alguno. Sobre este punto, el Grupo de Trabajo del Artículo 29 afirma que cuando el consentimiento se obtiene por medios electrónicos mediante una única acción del ratón, los interesados deben poder retirar su consentimiento de una manera análogamente sencilla[463]. En cambio, las redes sociales Instagram y Facebook dificultan considerablemente el proceso[464]. En concreto, mientras que para prestar el consentimiento no se precisan más que unos segundos, la retirada del mismo se demora al tener que dirigirse a la configuración del perfil, cuyo diseño resulta más complejo para proporcionar una retirada rápida de este. Incluso se conocen situaciones en las que, determinadas redes sociales como *FaceApp*, han establecido una irrevocabilidad del consentimiento, obligando a los usuarios de la misma a aceptar el acceso a un gran abanico de datos personales de sus dispositivos, además de a la utilización de los mismos de forma, perpetua, irrevocable, sin compensación y en todos los formatos y canales de medios conocidos o desarrollados posteriormente[465].

---

[461] DEL CASTILLO VÁZQUEZ, I.C., "Consentimiento (Comentario al art. 4.11 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. op. cit*., 2021. p. 689.

[462] En ese sentido, GIL MEMBRADO señala a modo de ejemplo, que únicamente se reputará como consentimiento libre y específico para recibir publicidad comportamental aquel que el individuo otorgue con independencia del acceso a la red social. GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 116. Ahora bien, deseamos añadir que, en el presente contexto, los proveedores de redes sociales desean asegurarse que los interesados aceptarán el tratamiento para la finalidad descrita, para lo que han diseñado un mecanismo que impide emplear el servicio sin la prestación de un previo consentimiento.

[463] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259, p. 24.

[464] Ello contraviene el art. 7.3 RGPD que dispone que será tan fácil retirar el consentimiento como darlo.

[465] La aplicación FaceApp, en auge en el año 2019, es una plataforma que permitía a los usuarios de la misma, previa aportación de una fotografía, conocer cuál sería su aspecto físico al envejecer tras la aplicación de algoritmos e IA a la imagen compartida. GARCIA GARNICA, M.C., "Datos personales y menores de edad", en GONZÁLEZ PACANOWSKA, I., *Protección de datos personales, op. cit*., p. 163.

Además, merecen especial atención las recientes Directrices 3/2022, del CEPD, sobre patrones oscuros en el interfaz de plataformas sociales: cómo reconocerlos y evitarlos, de 14 de marzo de 2022. En efecto, las Directrices identifican que este tipo de plataformas, acostumbran a incluir en su diseño una serie de patrones oscuros, entendiendo como tales, aquellas técnicas que influyen en el comportamiento de los usuarios, llevando a estos a tomar decisiones involuntarias y potencialmente perjudiciales para su información personal mediante el empleo de técnicas de manipulación o fraudulentas[466].

En concreto, el organismo europeo distingue dos grupos de patrones oscuros: por una parte, los de la interfaz, esto es, aquellos que inciden en el modo de mostrar la información, así como en el modo en el que el usuario interacciona con ella; por otra parte, los patrones oscuros de contenido, entendiendo como tales aquellos que afectan al modo de redactar el texto[467]. Sin embargo, debemos matizar, que algunas de las carencias denunciadas en anteriores epígrafes se identifican por el CEPD como patrones oscuros. Sin perjuicio de ello, nos detendremos en el estudio de aquellos sobre los que no se ha presentado la oportunidad de pronunciarnos en la presente investigación doctoral.

Podemos afirmar que los proveedores de redes sociales practican lo que el CEPD identifica como *overloading*, esto es, proporcionan al usuario un exceso de información, opciones y posibilidades para crear en este la falsa necesidad de que la misma resulta preceptiva para el buen funcionamiento del sistema o mejor experiencia. Ciertamente, en las políticas del Grupo Meta se percibe con claridad dicho espíritu cuando advierten al usuario que no consentir el tratamiento de determinada información puede incidir en la correcta prestación del servicio[468]. En efecto, estas plataformas acostumbran a solicitar repetidamente datos adicionales, abrumando al usuario con argumentos sobre la necesidad de facilitar la misma; en esencia, este patrón oscuro busca que el usuario reciba la impresión de que solamente podrá evitar estas reiteradas consultas en caso de compartir dicha información personal. Así, sirva como ejemplo que los proveedores de redes

[466] *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 7.
[467] *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 8.
[468] Véase que la política de privacidad del Grupo Meta dispone que en caso de que el usuario no permita la recogida de determinada información, puede que la calidad de la experiencia de este en el servicio se vea afectada. Política de privacidad del Grupo Meta obtenida de la página de registro de la red social Instagram: https://www.facebook.com/privacy/policy , (última consulta el 21 de septiembre de 2022)

sociales animan al usuario a compartir su número de teléfono al registrarse en la plataforma alegando que puede resultar beneficioso para la seguridad de su cuenta[469]. Estos comportamientos, sin duda, tal y como dispone el CEPD, no respetan los principios de minimización (art. 5.1.c) RGPD) y limitación de la finalidad (art. 5.1.b) RGPD).

Por otra parte, también se apoyan en la técnica del *stirring*, consistente en el empleo de emociones contra los intereses del usuario en la salvaguarda de su información personal. El fin de la señalada técnica reside en emplear frases o imágenes que acentúan en el usuario la necesidad de terminar cuanto antes el proceso de ingreso en la red social para empezar a usar la plataforma[470]. Concretamente, el lenguaje motivacional empleado por el proveedor de la red social, anima a los usuarios a compartir más datos personales de los necesarios. De esta manera, los usuarios perciben que compartir dicha información se constituye como una obligación, mientras que realmente no lo es. En consecuencia, con acierto señala el CEPD que este patrón oscuro colisiona con el principio de minimización, pues fomenta que el usuario comparta más datos de los necesarios, así como el principio de lealtad (art. 5.1.a) RGPD)[471].

De igual modo, los proveedores de redes sociales amparan en los siguientes tres patrones oscuros: el *hindering*, el *fickle* y el *left in the dark.*

Respecto al primero, su objetivo reside en desanimar al usuario para que no active los controles que protegen su información personal. En cierto sentido, se busca por parte del proveedor de la red social entorpecer la búsqueda de información al usuario, se entiende, en orden a dificultar el modo en el que este pueda proteger su información personal. Así las cosas, los proveedores de redes sociales acostumbran a invitar al usuario a reflexionar sobre sus decisiones cuando omiten el consentimiento a determinados tratamientos, mientras que, de aceptar el mismo, no conceden a este la posibilidad de replantearse dicha aceptación por medio de una advertencia[472]. Este comportamiento se

[469] *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 14.
[470] En efecto, este tipo de plataformas, con frecuencia incluyen mensajes como, "solamente un paso más y podrás disfrutar de la experiencia" o "ya casi está".
[471] *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 17.
[472] PLAZA PENADÉS, J., "La moderna configuración de la transparencia en la prestación de servicios y en la contratación en Internet", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial,* Valencia, Tirant lo Blanch, 2022, p. 245.

considera desleal por parte del responsable del tratamiento, ya que, busca que el usuario se relaje en torno al control de sus datos personales (art. 5.1.a) RGPD).

Asimismo, estas plataformas aprovechan del patrón oscuro *fickle*, esto es, diseñan la interfaz para impedir o dificultar al usuario el acceso a las herramientas de configuración, así como las finalidades de tratamiento. Tienden así a no garantizar el funcionamiento del hipervínculo que redirige a la configuración o no exponen el mismo en un modo legible. Por último, también practican el patrón oscuro *left in the dark*. Efectivamente, el diseño de la interfaz oculta información valiéndose de términos ambiguos, aportando información contradictoria o incluso camuflándola en un texto extenso. Así, se logra crear una sensación de desorientación en el usuario con el fin de que acepte la configuración predeterminada que, por supuesto, resulta más favorable para el proveedor de la red social. Sobre comportamientos relacionados con este patrón, nos hemos pronunciado en apartados anteriores.

En definitiva, a nuestro juicio, se puede apreciar como todos los patrones oscuros nacen con la vocación de infringir el principio de lealtad (art. 5.1.a) RGPD). Ciertamente, tanto el diseño de estos espacios, como las palabras escogidas para transmitir la información del art. 13 RGPD al usuario, buscan en última instancia defraudar al potencial usuario para que los proveedores de redes sociales no se encuentren con impedimento alguno a la hora de recopilar la información que les permita poner en práctica los tratamientos de datos previstos. En este contexto, nos preocupa el impacto que estas técnicas pueda generar sobre los menores de edad, ya que, estos patrones oscuros pueden alentar a los menores de edad a compartir más información dada su particular situación de vulnerabilidad, sin que perciban lo fraudulentos que estos comportamientos pueden considerarse[473].

En suma, muchos de los proveedores de redes sociales han diseñado un sistema poco transparente a la hora de informar a las personas usuarias del destino de sus datos personales, además de mecánicamente predispuesto a limitar en la medida de lo posible

[473] Así, el CEPD se muestra especialmente preocupado por el empleo de lenguaje emocional sobre menores de edad para animarlos a compartir información personal. Sin embargo, consideramos que la preocupación debe extenderse al empleo de todos los patrones oscuros sobre interesados menores de edad, ya que, estas técnicas exitosas a la hora de manipular el comportamiento de usuarios mayores de edad pueden resultar especialmente lesivas si se practican sobre personas en tránsito hacia su madurez. Véase el apartado 40 de las *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 17.

la libertad de las personas a la hora de prestar el consentimiento, contraviniendo el art. 4.11 RGPD que propugna el consentimiento del interesado como toda manifestación de la voluntad libre, específica, informada inequívoca por la que acepta el tratamiento de sus datos personales. Buena muestra de ello constituyen la carencia de elección sobre las finalidades de tratamiento que se desean aceptar o no, a lo que debe añadirse la dificultad a la hora de conocer las bases legales para cada una de las finalidades, la aceptación conjunta de las condiciones legales y la política de privacidad a través del mismo mecanismo de aceptación, la complejidad en la retirada del consentimiento, así como, en definitiva, la puesta en práctica de patrones oscuros en sus plataformas[474].

Por ello, no coincidimos con ALVAREZ RIGAUDIAS cuando señala que las políticas de privacidad no se redactan para el usuario, sino para la autoridad de control de tal modo que, la información que en ellas se contiene se dispone para el cumplimiento formal de todos los requisitos que estos organismos imponen[475]. Véase que en virtud de las consideraciones realizadas en los epígrafes precedentes, además del presente, las políticas de privacidad no se redactan de modo correcto, por una parte, para el usuario, pero tampoco para las autoridades de control, pues se ha constatado que muchas de las consideraciones realizadas por estos organismos de control, no poseen acomodo en las políticas de privacidad. Sin embargo, nos sorprende que, si bien la AEPD ha sancionado a diversas empresas por carecer de políticas de privacidad en sus páginas web[476], todavía no encontramos ningún procedimiento sancionador en el que se haya valorado la

[474] En el sentido expuesto, cabe citar la Resolución 01870/2017 de la AEPD (PS 00082/2017) contra Facebook en la que impone a la compañía una sanción de 1.200.000 euros, alegando que la red social incumple el deber de información previa al usuario, que el consentimiento no se ajusta a la normativa sobre protección de datos personales y, por último, que no se respeta la normativa sobre datos especiales ni de cancelación de la información (estas últimas cuestiones no constituyen objeto de estudio del presente epígrafe). Concretamente, la AEPD entiende que la compañía Facebook incumple el deber de información, pues el proveedor de la red social no obliga a la lectura de la política de privacidad, además de no informar de la totalidad de los datos personales tratados. En consecuencia, la AEPD señala que los comportamientos descritos conducen a cuestionar si se ha producido un verdadero consentimiento por parte del usuario para tratar sus datos personales. Obtenido de: https://www.aepd.es/sites/default/files/2019-12/PS-00082-2017_REC.pdf (última consulta el 30 de mayo de 2022).

[475] ALVAREZ RIGAUDIAS, D., "El poder del usuario digital", en ARTEMI RALLO, L., y GARCÍA MAHAMUT, R., (Editores), *Hacia un nuevo derecho europeo de protección de datos*, Valencia, Tirant lo Blanch, 2015, pp. 301-302.

[476] Destacan así los siguientes procedimientos sancionadores en los que la AEPD ha sancionado a diversas empresas y asociaciones por no disponer de una política de privacidad en sus páginas web: primeramente, la AEPD sanciona con una multa de 4.000 € a una empresa que carece de política de privacidad en el Procedimiento Sancionador PS/00437/2020. Obtenido de https://www.aepd.es/es/documento/ps-00437-2020.pdf (última consulta el 5 de enero de 2023); posteriormente, sanciona con una multa de 4.000 € a otra compañía por idénticas razones en el PS/00404/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00404-2021.pdf (última consulta el 5 de enero de 2023); por último, sanciona a una asociación con una multa de 3.000 € en el PS/00609/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00609-2021.pdf (última consulta el 5 de enero de 2023).

idoneidad tanto de la información compartida, como de la redacción empleada en este tipo de documentos.

Definitivamente, se debe imponer a los proveedores de redes sociales la adecuación de sus políticas de privacidad, así como el modo de aceptar las mismas a la normativa legal vigente[477]. De lo contrario, se permite operar a determinados proveedores de servicios digitales de un modo que vulnera la protección de datos personales de millones de personas usuarias, de las cuales, muchas son menores de edad[478]. Mientras ello ocurra, los consentimientos otorgados carecen de validez, esto es, no constituyen una base legal que legitime el tratamiento de datos, además de no garantizar al usuario el control efectivo sobre su información personal.

Sobre este aspecto, resulta interesante la reflexión que compartimos con BARRIUSO RUIZ cuando plantea que las Agencias de Protección de Datos Personales, tal vez deberían intervenir de oficio en las redes sociales para controlar determinadas políticas de privacidad, pero sobre todo, para inspeccionar sus sistemas de información y prácticas abusivas implementadas en ellas[479]. Efectivamente, el CEPD también ha afirmado que las autoridades deben asumir la responsabilidad de sancionar el empleo de patrones oscuros en caso de que estos vulneren el RGPD[480]. Por tanto, debiera obligarse a estos organismos a que adopten un comportamiento más proactivo con el control de este tipo de comportamientos que de manera evidente colisionan con la normativa sobre protección de datos personales.

---

[477] De manera acertada reclama ARENAS RAMIRO que las redes sociales deberían ofrecer una política de privacidad no demasiado extensa, fácilmente accesible, con lenguaje sencillo y que fuera ineludible para continuar con el servicio. ARENAS RAMIRO, M., "El consentimiento en redes sociales on line", RALLO LOMBARTE, A., Y MARTINEZ MARTINEZ, R., (Directores), *Derecho y redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, p. 125.

[478] Sobre este aspecto, resulta de vital relevancia la recomendación formulada en el Informe de la 30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad instando a los Estados a mostrar un mayor respeto a las normas sobre privacidad de los Estados en los que operan. 3. Resolución sobre la intimidad de los niños en línea, adoptada en la 30ª Conferencia Internacional de Autoridades de protección de datos y privacidad, propuesta por el Comisario de Protección de datos de Canadá, adoptada en Estrasburgo, octubre de 2008. Obtenido de: https://edps.europa.eu/sites/default/files/publication/08-10-17_strasbourg_children_online_es.pdf (última consulta el 8 de marzo de 2022).

[479] BARRIUSO RUIZ, C., "Las Redes sociales y la protección de datos hoy", *op. cit.*, p. 314.

[480] *Guidelines 3/2022 of European Data Protection Board, on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022, p. 7.

4.2. La prestación del consentimiento por el menor de edad al tratamiento de datos personales en redes sociales. Problemas para verificar la edad de los internautas

Disponen los arts. 8 RGPD y 7 de la LOPDGDD que el menor de edad cuya edad supere los 14 años en el caso de España, podrá prestar por sí mismo consentimiento válido al tratamiento de datos personales[481]. Por el contrario, para los casos en los que los menores de edad que no alcancen dicha edad, sus representantes legales deberán proceder a prestar dicho consentimiento. El planteamiento descrito, simpatiza con los postulados establecidos por la Convención de 1989 al permitir a este ejercitar por sí mismo los derechos concernientes a su persona; mientras que, en caso de no demostrar madurez suficiente, sus representantes legales habrán de proceder a su asistencia. Si bien es cierto que el legislador parece haberse decantado por el establecimiento de un criterio cronológico con el fin de determinar la capacidad del menor respecto al ejercicio de este derecho fundamental, ello no ha evitado la aparición de obstáculos que imposibilitan una correcta determinación de la edad del menor en el ámbito *online*[482].

A propósito de lo expuesto, el entorno digitalizado como el que vivimos en el siglo XXI, ha supuesto la aparición de pluralidad de riesgos para el respeto al planteamiento recientemente descrito. Concretamente, la prestación del consentimiento *online* ha tambaleado la posibilidad de garantizar el control en la prestación de estos consentimientos. En efecto, la imposibilidad física de fiscalizar el momento en el que el menor de edad consiente el tratamiento de datos personales, frecuentemente desde su terminal móvil y sin vigilancia parental, ha ocasionado que millones de menores de edad

[481] Sobre el establecimiento de la edad mínima legal para consentir el tratamiento de datos personales en 14 años en España, véase el apartado 4 del capítulo III del presente trabajo de investigación.

[482] De esta suerte, el ordenamiento jurídico dispone de tres criterios a efectos de remover las limitaciones a la capacidad del menor para el ejercicio autónomo de los derechos relacionados con su personalidad. Un primer criterio cronológico, basado exclusivamente en la edad del menor en el que aboga por conceder determinada capacidad a todos los menores de edad que alcancen determinada edad; así, la concesión de la capacidad ocurre independientemente del grado de desarrollo psicológico del menor y responde con mayor precisión a las exigencias de seguridad jurídica. El segundo criterio se basa en la madurez o discernimiento del menor, debiendo valorar en cada caso concreto cuál es este nivel en orden a conceder al menor la posibilidad de ejercicio autónomo de dichos derechos. Por último, el criterio mixto combina ambas formulaciones expuestas. Con todo, nuestro ordenamiento jurídico no se ciñe a una pauta clara a la hora de fijar la capacidad del menor, pues dependiendo del derecho de la personalidad que se trate, los criterios empleados varían. Véase al respecto CADENAS OSUNA, D., "El consentimiento informado y el rechazo a la intervención o tratamiento médico por el menor de edad tras la reforma de 2015: estudio comparado con el *common law*", *op. cit.*, p. 794. A modo de ejemplo, en el ámbito sanitario se ha establecido un criterio mixto que combina la edad de 16 años y el nivel de madurez. En cambio, la normativa sobre el derecho a la protección de datos personales, apunta hacia un criterio exclusivamente cronológico establecido en los 14 años.

que no cumplen con la edad mínima para prestar el consentimiento no hayan visto impedido ni limitado el acceso a dichas redes sociales.

En relación con lo expuesto, resulta complejo e incluso imposible en gran parte de las ocasiones, que los progenitores procuren la protección al menor en este ámbito, tal y como impone la LOPDGDD en su art. 84[483]. Ello se debe, principalmente a dos cuestiones: por una parte, a las facilidades del menor para navegar en solitario, sin supervisión adulta y desde cualquier parte, lo que inevitablemente extrema la dificultad en dicha asistencia; por otra parte, a las innegables dificultades que los adultos se encuentran a la hora de desenvolverse en el entorno digital. Antes bien, siguiendo a CASTILLA BAREA, los representantes legales y progenitores del menor de edad deben contar con la educación específica sobre la materia, ya que solamente de adquirir dichos conocimientos en lo concerniente a los riesgos que comportan Internet y las TIC podrán adoptar las cautelas necesarias para asistir a los menores en este contexto[484].

Volviendo a la cuestión que nos concierne, los progenitores no pueden convertirse en los responsables exclusivos de garantizar que los menores de 14 años no prestan un consentimiento al tratamiento de datos personales al darse de alta en una red social sin poseer capacidad para a tal efecto.

Así las cosas, el legislador consciente de dichas dificultades, incluye en la norma sobre protección de datos personales la obligatoriedad de los prestadores de servicios de la sociedad de la información de asegurarse de la edad del futuro usuario. Ahora bien, aunque el RGPD aboga en su art. 8.2 por imponer a los proveedores de redes sociales verificar tanto la edad, como el eventual consentimiento prestado por los representantes legales cuando el menor no puede consentir por sí mismo; gran parte de las redes sociales no han instaurado ningún sistema que verifique la edad de los usuarios, permitiendo el acceso a millones de menores de 14 años a sus servicios[485]. La afirmación no es baladí,

[483] Tal deber de asistencia también se desprende del art. 154 CC. Es más, conformes con CASTÁN VÁZQUEZ, los progenitores deben controlar el uso que sus descendientes hacen de las redes sociales. CASTÁN VÁZQUEZ, J.M., "Cometario al Título VII del Código Civil", en ALBADALEJO, M., (Director), *Comentarios al Código civil y compilaciones forales,* Madrid, EDERSA, 1978, p. 60.

[484] CASTILLA BAREA, M., "La protección de los menores el internet (Comentario al artículo 84 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.,* p. 3953.

[485] Así, la AEPD afirma en su Memoria del año 2008 que las redes sociales carecen de aplicaciones que permitan controlar la edad de los menores que tratan de acceder al servicio. Memoria de la Agencia Española de Protección de Datos del año 2008. Obtenido de:

ya que, un elevado número de menores de 14 años consienten el tratamiento de datos personales sin poseer la capacidad para ello. A tal efecto, la doctrina ha aunado esfuerzos para visibilizar en la última década esta realidad que, a día de hoy y tras varios años desde la irrupción de las redes sociales, continúa sin solución.

A este respecto, GUARDIOLA SALMERÓN afirma con acierto, que ninguna de las redes sociales dispone de un sistema eficaz y seguro de verificación de estos datos que garantice su autenticidad y veracidad (ni de la edad mínima exigida para prestar el consentimiento, ni del consentimiento de los presentantes legales en caso de que el menor no haya cumplido 14 años)[486]. Idéntica preocupación muestra MITLLANS PERELLÓ cuando aduce que uno de los problemas en el uso de redes sociales por menores de edad reside en cómo detectar de forma efectiva a estos sujetos, muchos de ellos menores de 14 años[487]. En relación con lo expuesto, ARENAS RAMIRO establece que la prueba de la edad se convierte en uno de los grandes obstáculos a salvar por las redes sociales; a su juicio, en estos casos no resulta suficiente la marcación de casillas que afirmen que la utilización de las redes sociales se desempeña por personas mayores de 18 años[488].

Por supuesto que esta circunstancia preocupa especialmente, pues ante la ausencia de un sistema que verifique la edad del menor que desea darse de alta en la red social, los jóvenes solamente deben falsear la realidad sobre su verdadera edad para prestar un consentimiento (carente de validez) al tratamiento de datos personales[489]. En relación con lo expuesto, algunas de las aplicaciones más empleadas por los menores entre las que destacan Snapchat, TikTok, y Facebook no prevén mecanismos efectivos en orden a

http://www.resi.org.mx/icainew_f/images/Biblioteca/PDP/memorias/memoria_2008.pdf (última consulta el 28 de abril de 2021).

[486] GUARDIOLA SALMERÓN, M., "Menores y redes sociales: nuevos desafíos jurídicos", *Revista de Derecho, Empresa y Sociedad,* enero-julio 2016, núm. 8. p. 55.

[487] MITLLANS PERELLÓ, E., "Impacto de las redes sociales en el derecho a la protección de datos personales", *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, p. 113.

[488] ARENAS RAMIRO, M., "El consentimiento en las redes sociales on line", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales*, *op. cit.,* p. 134.

[489] Así se manifiesta DAVARA FERNÁNDEZ DE MARCOS cuando establece que desde los ocho o nueve años, los menores se registran en redes sociales, con o sin el conocimiento de sus progenitores, poniendo una fecha de nacimiento anterior a la real DAVARA FERNÁNDEZ DE MARCOS "Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go", *XX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos,* Madrid, 2007. p. 15. Idéntica situación visibiliza GETE-ALONSO Y CALERA cuando afirma que no todas las barreras impuestas en redes sociales son efectivas, por lo que los menores solamente deben falsear u ocultar su edad real para acceder. GETE-ALONSO Y CALERA, Mª.C., "Los derechos del menor y personas discapacitadas en el entorno digital", en MARTÍNEZ VÁZQUEZ DE CASTRO, L., (Director) y ESCRIBANO TORTAJADA, P., (Coordinadora), *Internet y los derechos de la personalidad*, *Internet y los derechos de la personalidad, op. cit.,* p. 281.

verificar la edad de los usuarios[490]. Por tanto, de conformidad el informe elaborado por el grupo de investigación citado, los menores pueden evitar con facilidad los mecanismos de verificación implantados en las redes sociales que más emplean faltando a la verdad sobre su edad. Ello se debe a que, gran parte de los proveedores de redes sociales no implementan las medidas técnicas adecuadas para cerciorarse sobre la veracidad de la información aportada por los futuros jóvenes usuarios[491]..

Así, las consecuencias revisten gravedad a la hora de procurar la protección de datos personales de los más jóvenes, ya que una de las facultades de control más fundamentales sobre los datos personales como la prestación del consentimiento informado, carece de validez si se presta por un sujeto no apto para ello como resulta un menor que no alcanza la edad de 14 años. En efecto, en la actualidad, millones de consentimientos prestados por menores muy activos en estas plataformas, pueden reputarse nulos[492]. Por consiguiente, los proveedores de redes sociales realizan tratamientos ilícitos de datos personales de menores. En adición a lo expuesto, destacamos, igualmente, la ausencia de un mecanismo que verifique la prestación del consentimiento por los representantes legales del menor cuando este sea menor de 14 años a pesar de que tanto el RGPD como la LOPDGDD impongan dicha obligación.

Llegados a este punto, la AEPD afirma en la Resolución del Procedimiento Sancionador 281/2007, que se ha de adoptar una conducta razonablemente diligente con el fin de evitar el tratamiento de datos personales de menores de edad resultando procedente abstenerse del tratamiento en caso de que, la edad del interesado resulte dudosa[493]. Sin embargo, el modo de operar de estas plataformas sociales resulta el

---

[490] El informe citado trae causa de los proyectos de investigación financiados por CyberSec4Europe (CyberSec4Europe (CyberSec4Europe Network of Competence Centers for Europe) y ASAP (Adaptive Security and Privacy). Obtenido de: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9295422 , p. 5. (última consulta el 28 de septiembre de 2021). Para más detalle sobre el proyecto, consúltese el siguiente enlace sobre CORDIS Resultados de investigación de la UE: https://cordis.europa.eu/article/id/429037-bypassing-age-verification-measures-on-social-media-apps-is-easy-as-pie/es

[491] Antes bien, Instagram ha implementado a finales de 2022 en España un mecanismo de verificación que contempla dos posibilidades en orden a verificar la edad: por una parte, la solicitud del DNI del menor; por otra parte, el envío de un vídeo *selfie* al proveedor de la red social para que por medio del análisis biométrico pueda estimarse la edad del usuario.

[492] BARRIUSO RUIZ, C., "Las Redes sociales y la protección de datos hoy", *op. cit.*, p. 328.

[493] Resolución 00284/2008 del Procedimiento Sancionador 00281/2007 de la AEPD. En ese sentido, la AEPD sanciona a BANKINTER y a la empresa ANTEVENIO por no disponer de mecanismos que verifiquen la edad del menor para consentir el tratamiento de datos personales en servicios no dirigidos a menores de edad. Si bien la sociedad ANTEVENIO trata de alegar un fallo en la determinación de la edad del menor al consentir el tratamiento, la AEPD considera que no ha quedado acreditado la existencia de tal

contrario: proceden al tratamiento de los datos personales a pesar de las posibles dudas que pueda arrojar la edad del menor[494].

Desde luego que las consecuencias tanto para los derechos fundamentales del menor, como para el correcto desarrollo de este son devastadoras sin que resulte plenamente consciente cuando acepta el tratamiento de su información personal por el proveedor de redes sociales. Ello se debe a que, el gran volumen de datos que compartirá a lo largo de su infancia, adolescencia e incluso vida adulta se escaparán de su control sin que en dicho momento pueda comprender el alcance de dicho comportamiento. Resulta inadmisible legalmente que las redes sociales puedan continuar operando en las circunstancias descritas sin aportar garantías sobre la verificación de estos extremos[495]. Además, la falta de mecanismos en la verificación de la edad de los usuarios que prestan el consentimiento de datos personales, conlleva la dificultad en el control y garantía de otras premisas de obligada mención.

De este modo, las políticas de privacidad no pueden adaptarse a menores de edad en su plenitud, pues no se conoce qué usuarios alcanzan la mayoría de edad. Por otra parte, la imposibilidad de conocer la edad real del futuro usuario, dificulta considerablemente la configuración por defecto del perfil con el mayor grado de privacidad posible, tal y como aconseja el Grupo de Trabajo 29. Asimismo, impide

---

mecanismo para introducir la edad, lo que deriva en un tratamiento de datos personales de un menor de 9 años de edad.

[494] El Procedimiento sancionador anteriormente mencionado, no se trata de un caso aislado. Así, la AEPD ha tramitado los siguientes procedimientos sancionadores en los que el consentimiento del menor no ha resultado suficientemente verificado; a saber: el Recurso 01663 /2010 del Procedimiento Sancionador 00023/2010; el Recurso 02177/2010 del Procedimiento Sancionador 00234/2011; y por último, el Recurso 02636/2011 del Procedimiento Sancionador 00339/2011.

[495] Véase que incluso la LOPDGDD dispone en su art. 73 apartados a) y b) que el trato de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello o el titular de su patria potestad o tutela, así como la no acreditación de la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por una menor o por el titular de su patria potestad o tutela, constituyen una infracción grave cuya sanción (art. 76.f.) puede alcanzar un máximo de 10.000.000 euros o, tratándose de una empresa, la cuantía equivalente a un 2% del volumen de negocio anual global. Sin embargo, la AEPD no ha actuado contundentemente para reprimir este incumplimiento. Por el contrario, la Information Commisioner's Office (ICO) inglesa ha sancionado recientemente a la red social TikTok por no verificar la edad de los usuarios de su servicio con un importe total de 12, 7 millones de libras esterlinas. FERNÁNDEZ, C., "La autoridad británica de protección de datos sanciona a TikTok con 12,7 millones de libras por tratar indebidamente datos de menores", La Ley digital (Ciberderecho). Obtenido de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAEWQTU_DMAyGf81yROkHhx1yWdtDUTf2URCckNtabURIqjgp7N_jrRIc_Eq2Xz-yHaAjlWcC-hDBlK5XaX5L9IItdLeO8wP63VVJEVwAc0ZSSZYngib3fYBFjxC0szvwqvURhR72zemCRu3RxqPXttczmCT9SCT3BnWopJRpss228lEs6ImH1ase0QYUkx6nhiOsLCDSVEIAVT4X7fux2qR52W6yrnpjeXphOVSCEHw_HWFE1WgKwBtGE2Bw1NbFA9D8I4z95NMud-OK7g0njMYCDNrhb3tqINp-OkX017Vk_gv1oJoTQwXMs7meneFf3D2zI-bHLz6itgV4F4k_IH8BxastRl0BAAA=WKE (última consulta el 4 de mayo de 2023).

instaurar comunidades separadas entre adultos y menores de edad en el contexto descrito[496]. Incluso cabe la posibilidad de que se oferten productos y servicios al menor para los que legalmente no posee la capacidad de contratar como, por ejemplo, bebidas alcohólicas, juegos en línea o servicios *premium*. En relación con lo expuesto, los propios proveedores de redes sociales han tomado conciencia de dicha circunstancia. Sirva como ejemplo que, Instagram afirma en su política de privacidad que en el caso de personas que no han alcanzado la mayoría de edad, a fin de garantizar la protección especial de este colectivo, restringen el acceso a ciertas funciones en relación con los datos que la plataforma emplea para seleccionar anuncios[497].

No obstante, reiteramos que, dicha garantía es más una proclamación formal que no consigue que estos proveedores de servicios verifiquen de manera real la edad del usuario. Efectivamente, tal y como afirma REYES MENÉNDEZ no basta con prohibir formalmente el uso de estas plataformas a partir de una determinada edad, si ello no se acompaña de fórmulas eficaces de comprobación real de la misma[498]. En definitiva, se permite el empleo estas plataformas, sin garantías, a sujetos que, dada su particular situación de tránsito a la madurez, no demuestran la capacidad de comprender la relevancia y vitalidad que el consentimiento supone para el control de su información personal.

Así las cosas, de acuerdo con GARCÍA ATANCE la solución en torno a la verificación de la edad de los menores de 14 años, así como la verificación de que el consentimiento se ha concedido por los representantes legales, en su caso, encierra una dificultad añadida, ya que los más jóvenes habitualmente no disponen de tarjetas de crédito o permiso de conducir que pueda acreditar su edad real[499]. En ese sentido,

[496] Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, p. 13.

[497] Véase la política de privacidad de Instagram/Facebook: https://www.facebook.com/about/privacy/legal_bases "En el caso de personas que no hayan alcanzado la edad de consentimiento establecida en el Estado miembro en el que residan, modificamos nuestros Productos de Facebook para garantizar la aplicación de protección especial y restringimos el acceso a ciertas funciones en relación con los datos que usamos para seleccionar los anuncios" (última fecha de consulta el 21 de septiembre de 2022).

[498] REYES MENÉNDEZ, D., "El acceso del menor a las redes sociales y el problema de su autentificación: La necesidad de una respuesta tecnológica", *op. cit.*, p. 1. De manera similar se pronuncia TORAL LARA, E., "Menores y redes sociales: consentimiento, protección y autonomía", *Derecho privado y constitución*, 2020, núm. 36, p. 205.

[499] GARCÍA-ATANCE GARCÍA DE MORA, M.V., "Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación (TIC)", *op. cit.*, p. 1279.

destacamos que, la red social Tuenti, configuró un sistema diseñado expresamente con el objetivo de cumplir con la normativa sobre protección de datos personales cuando esta exige la realización de esfuerzos razonables por parte del responsable para verificar la edad de los usuarios[500].

Es cierto que el sistema implementado por Tuenti era manifiestamente mejorable. Ahora bien, consideramos que, tras más de una década de la irrupción de las TIC, que no se controle la edad de acceso resulta inadmisible. Los problemas en torno a la verificación de la edad de los usuarios demandan una solución de manera urgente, ya que resulta evidente que, los arts. 8.2 RGPD y 7.2 LOPDGDD resultan reiteradamente vulnerados por los proveedores redes sociales sin que se prevean consecuencias por ello. Ya en el año 2010, MARTÍNEZ MARTÍNEZ apremiaba a desarrollar herramientas eficaces que auxiliaran en el conocimiento de la edad de los usuarios de servicios en Internet y se recabara el consentimiento de sus representantes legales en caso contrario[501]. Más aún, en el año 2008, el *International Working Group on data protection in telecommunications*, en su informe conocido como Memorándum Roma ya advertía que el consentimiento prestado por menores de edad al darse de alta en la red social, consintiendo el tratamiento de sus datos personales, demandaría una solución específica a futuro[502]. No podemos sino sentir decepción al comprobar que, a pesar de que la

[500]Así, descartada por la plataforma la exigencia de vincular el acceso a la plataforma a la lectura del DNI electrónico debido a la falta de extensión de su utilidad entre la población en el año 2010, la compañía diseñó un sistema que fusionaba un control analógico a la vez que digital, tal y como se expone a continuación. La red social Tuenti implementó un protocolo para la detección de perfiles sospechosos de corresponder a menores de 14 años a cuyo fin, en caso de que el equipo de Soporte detectara estos perfiles sospechosos, les remitiera una comunicación a través del correo electrónico solicitando al supuesto menor de 14 años remitir una copia del DNI o Pasaporte mediante escáner o fax en un plazo no inferior a 96 horas. Transcurrido dicho plazo sin recibir la identificación, Tuenti procedía al borrado automático de dicho perfil. Deseamos destacar que de 1.000 perfiles sospechosos que fueron requeridos para que remitieran la información acreditativa de la edad, el 98% no ofrecieron identificación, siendo los perfiles borrados de manera automática por la plataforma. MARTOS DÍAZ, N., "Las políticas de privacidad, Redes sociales y protección de datos. El problema de la verificación de la edad", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores) *Derecho y Redes sociales, op. cit.*, p. 160.

[501] MARTINEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales, op. cit.,* p. 103.

[502] INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS, *Report and Guidance on Privacy in Social Network Services (Memorandum Roma)*. 43ª reunión celebrada en Roma los días 3 y 4 de marzo de 2008, p. 4. En ese mismo sentido se manifestaban el Parlamento Europeo y el Consejo por medio de la Decisión 1351/2008/CE, de 16 de diciembre de 2008, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación, Diario Oficial de la Unión Europea, de 24 de diciembre de 2008 Considerando 12 cuando rogaban que se desplegaran esfuerzos necesarios en orden a proteger a los niños mediante el desarrollo, por ejemplo, de sistemas efectivos de comprobación de la edad y de etiquetas de certificación voluntarias.

normativa actualmente vigente prevea la necesidad de verificar dicha información, cuestión que no se preveía en la normativa que regía cuando el autor y los participantes en la Conferencia Internacional profirieron dicha necesidad, los artículos citados constituyen una obligación carente de aplicabilidad en plena era digital.

Incluso la UE, ya animaba a la industria a que implementaran medios técnicos para la identificación y la autenticación electrónicas, obligándose la Comisión a proponer en 2012 un marco comunitario para la autenticación electrónica que permitiera el uso de atributos personales (la edad, en particular) para garantizar el cumplimiento de las disposiciones relativas a las edades del aquel entonces, propuesta de RGPD[503]. Lamentablemente, dicho marco no llegó a materializarse.

Ante la ausencia de diligencia por parte de los proveedores de redes sociales en la implementación de mecanismos que de manera real y efectiva protejan la información personal de los usuarios y con especial énfasis la de los usuarios más jóvenes, diferentes Autoridades de Datos Nacionales han impulsado campañas de educación en el entorno digital dirigidas a representantes legales y menores. Concretamente, en España, la AEPD publicó en el año 2008 la Guía de Recomendaciones sobre "Derechos de niños y niñas-Deberes de padres y madres" con sencillos consejos con el cometido de asesorar a estos sobre la protección de su información personal en un lenguaje accesible[504]. Así lo han llevado a cabo también la Agencia de Protección de datos de Noruega a través del proyecto "You decide"[505] o la Comisión Nacional de Protección de Datos de Portugal, con el Proyecto "Dadus"[506]. Si bien resulta loable la labor desempeñada por las mencionadas Autoridades en la educación de las personas usuarias sobre los aspectos

[503] Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones una "Estrategia europea en favor de una Internet más adecuada para los niños", del 2 de mayo de 2012, COM (2012)196 final, p. 12.

[504] Recomendaciones de la AEPD sobre los Derechos de los niños y niñas y deberes de los padres y madres, año 2008. Obtenido de: https://www.adolescenciasema.org/usuario/documentos/Derechos%20y%20deberes%20padres%20y%20menores%20en%20internet%20de%20la%20agencia%20de%20proteccion%20de%20datos.pdf (última consulta el 1 de septiembre de 2022).

[505] La Agencia Vasca de Protección de Datos ha traducido dicho informe a español con el fin de concienciar a la juventud sobre los usos inadecuados que pueden realizarse en la red con su información personal, además de recomendar a estos proteger su información personal. Véase la Guía de la AGENCIA VASCA DE PROTECCIÓN DE DATOS sobre Decides tú cómo proteger tu privacidad, enero de 2007. Obtenido de: https://www.avpd.euskadi.eus/contenidos/informacion/udcd/es_udcd/adjuntos/folleto.pdf (última consulta el 12 de septiembre de 2022).

[506] Para mayor información véase la iniciativa portuguesa "Dadus" en http://dadus.cnpd.pt/ (última consulta el 2 de enero de 2021).

técnicos básicos para la protección de su información privada, transcurrida una década desde la adopción de estos proyectos, la protección de la información personal del menor no ha sufrido grandes avances.

Más no se trata de ello únicamente, la ausencia de herramientas que permitan verificar la edad del menor para eventualmente solicitar el consentimiento a sus progenitores, también obstaculiza la posibilidad de que estos brinden asistencia a los más jóvenes en el ejercicio de sus derechos fundamentales (art. 154 CC). Esta afirmación trae causa de la dificultad a la que se enfrentan los progenitores para conocer si el menor de edad se ha dado de alta en redes sociales sin su consentimiento, pues al poseer un terminal móvil de su uso exclusivo desde edades tempranas, la facilidad de acceder a estas plataformas sin cumplir los requisitos legales a tal efecto aumenta exponencialmente. Así las cosas, una consulta pública elaborada por la Comisión francesa de protección de datos personales (CNIL) revela que, el 86% de los progenitores se muestra a favor del establecimiento de un mecanismo eficaz de verificación de la edad de los menores internautas, así como de los representantes legales para los casos en los que este resulte preceptivo[507].

Sin embargo, tomamos conciencia de lo complejo que puede resultar en la práctica implementar un mecanismo de verificación de la edad de los jóvenes usuarios. En ese sentido, el mecanismo cuya implementación se pretenda habrá de mostrarse respetuoso con el principio de minimización, procurando la solicitud del mínimo de datos personales posibles para ello, tanto al menor como a sus progenitores, así como un enfoque proporcionado basado en la evaluación de los riesgos incurridos. Concretamente, la Comisión francesa de protección de datos personales (CNIL) propone una serie de recomendaciones que habrán de servir de guía en la elección del mecanismo de verificación adecuado[508].

En primer lugar, el mecanismo de verificación habrá de considerarse proporcionado, esto es, la adecuación del mismo dependerá de los fines de tratamiento,

[507] Consulta pública de la Comisión francesa de protección de datos (CNIL) sobre los derechos de los menores en el entorno digital del año 2021. Obtenido de: https://www.cnil.fr/sites/default/files/atoms/files/consultation_publique_sur_les_droits_des_mineurs_-_synthese_des_contributions.pdf , p. 3. (última consulta el 29 de septiembre de 2021).

[508] Véase al respecto la Recomendación núm. 7 realizada por la Comisión francesa de protección de datos (CNIL) en relación a los derechos digitales de los menores. Obtenido de: https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee (última consulta el 29 de septiembre de 2021).

así como de los riesgos asociados a este. En palabras similares se pronunció el *Information Commissioner´s Office* de Reino unido (ICO) cuando aboga por la desproporcionalidad de un sistema de reconocimiento facial para aquellos tratamientos que supongan un bajo riesgo[509]. En segundo lugar, el mecanismo habrá de gozar de robustez cuando el responsable trate datos con fines de publicidad y marketing dirigida a menores debido al riesgo que suponen, lo que implica descartar los mecanismos meramente declarativos que el menor puede sortear sin gran dificultad. Por último, el sistema implementado habrá de respetar el principio de minimización, es decir, no habrá de conllevar la recogida y tratamiento de más datos de los necesarios a efectos de verificar la edad del menor.

De este modo, para el caso de proveedores de redes sociales, ha quedado de manifiesto que su finalidad principal reside en la cesión de datos con fines de venta y marketing, por lo que el sistema de verificación elegido habrá de resultar acorde al riesgo que los tratamientos de menores conllevan. Es más, tal y como quedará de manifiesto, los potentes algoritmos diseñados por estos proveedores causan un especial riesgo para la protección de datos cuando se aplican sobre jóvenes que no alcanzan la mayoría de edad. Por otra parte, los mecanismos de verificación instaurados actualmente, son poco vigorosos. En efecto, los proveedores de redes sociales dirigen publicidad y marketing a los jóvenes internautas, sin embargo, el mecanismo de verificación instaurado resulta meramente declarativo y fácilmente sorteable por los menores no declarando su verdadera edad.

Finalmente, quizás los mayores obstáculos se presenten con el cumplimiento del principio de minimización de los datos a la hora de instaurar el sistema de verificación, dado que, muchos de ellos pueden conllevar el tratamiento de más datos personales del propio menor o incluso de sus progenitores[510]. Antes bien, puesto que este mecanismo de verificación es una garantía para el ejercicio de un derecho fundamental, creemos que pueden considerarse proporcionales incluso aquellos sistemas que recaban volúmenes

[509] Código de Edad del Information Commissioner´s Office de Reino unido (ICO). Obtenido de: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (última consulta el 29 de septiembre de 2021).

[510] Sirva como ejemplo, que los sistemas de reconocimiento facial pueden conllevar la recogida masiva de información personal para su correcto funcionamiento. No obstante, entidades como ONCE han implementado estos mecanismos en sus apartados de compra *online* de apuestas y loterías en orden a verificar la edad de los compradores *online*. Obtenido de: https://www.juegosonce.es/verificacion-documental-manual (última consulta el 30 de septiembre de 2021).

elevados de datos personales en contra de lo que determinado sector de la doctrina considera[511]. Cabe decir también, que conscientes de que sistemas de verificación basados en parámetros biométricos pueden presentar inconvenientes para poder verificar de manera fiable[512], las investigaciones más recientes se decantan por la combinación de diferentes sistemas en orden a verificar la edad de los usuarios con éxito[513].

Sobre este particular, si bien la UE todavía no se decanta por un sistema o sistemas de verificación concreto de la edad de menores internautas[514], EEUU ha establecido una serie de métodos de verificación del consentimiento parental que pueden resultar aceptables acordes a la norma sobre privacidad *Children's Online Privacy Protection Act (COPPA)*[515], a saber: la firma de un formulario de consentimiento y envío por fax o, correo o escaneo electrónico al progenitor de dicho documento; el empleo de la tarjeta de crédito o débito en línea que notifique cada transacción por separado al titular de la cuenta; la llamada a un número gratuito con personal capacitado; proceder a la conexión a través de una video llamada con personal capacitado; proporcionar una copia de una forma de identificación emitida por el gobierno que verifique con una base de datos la información, siempre que elimine la identificación de sus registros cuando termine el proceso de verificación; la respuesta a una serie de preguntas de desafío basadas en el

[511] Véase así, TORAL LARA, E., "Menores y redes sociales: consentimiento, protección y autonomía", *op. cit.*, pp. 205-206.
[512] Informe relativo a los proyectos de investigación financiados por CyberSec4Europe (CyberSec4Europe (CyberSec4Europe Network of Competence Centers for Europe) y ASAP (Adaptive Security and Privacy), publicado en https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9295422 , pp. 5-6. (última consulta el 30 de septiembre de 2021). Así, el grupo de investigación autor del informe asegura que los sistemas de verificación de la edad basados en parámetros biométricos de la voz, si bien pueden demostrar una alta precisión también pueden sortearse fácilmente por los menores empleando grabaciones de voz con la voz de una persona que alcance la mayoría de edad; por otra parte, la lectura de la huella dactilar quedaría descartada ante la limitación del anonimato que puede acarrear además de requerir un lector de huella para su correcta implementación; en adición, el reconocimiento facial también puede sortearse con facilidad aportando una fotografía de una persona adulta para su escaneo.
[513] SHOPON, M.; TUMPA, S.N.; BATHIA, Y.; PAVAN KUMAR, K.N.; GAVRILOVA, M.L., "Biometric Systems De-Identification: Current Advancements and Future Directions", *Journal of Cybersecurity and Privacy*, 2021, núm 1, pp. 470-495.
[514] Sin embargo, la UE ha aprobado recientemente un breve documento sobre los Métodos de verificación de la edad de los niños (Verification methods for children), en el que, si bien reconoce que impera la necesidad de establecer mecanismos de venificación eficaces, no termina de decantarse por los sistemas idóneos que enumera, entre los que destacan: la solicitud de la tarjeta de crédito, sistemas de autodeclaración, sistemas biométricos, el análisis de patrones de uso en línea, o la identificación digital. Documento del Servicio de Investigación del Parlamento Europeo, sobre *Verification methods for children*, de febrero de 2023. Obtenido de: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf (última consulta el 8 de marzo de 2023).
[515] Children's Online Privacy Protection Act of 1998 (COPPA), 15 USC 6501-6505 issued in November 1999 by the Federal Trade Commission (FTC) and became effective in April 2000. Véase Section 312.5, *Parental Consent.*

conocimiento que resultarían difíciles de responder para una persona que no sea adulta; o verificar una foto de una licencia de conducir con foto presentada por los progenitores a efectos de comparar dicha fotografía con una segunda enviada por los progenitores, empleando tecnología de reconocimiento facial para dicho fin. Por otra parte, también prevé para los casos de no divulgación de la información, la posibilidad de enviar un email de confirmación a los progenitores cuando el menor pretenda prestar el consentimiento en determinado servicio que requiere del tratamiento[516].

Así las cosas, algunos de los métodos no cuentan con el beneplácito de las investigaciones -recientemente citadas- llevadas a cabo en el ámbito europeo; sin embargo, entendemos que el método consistente en realizar una serie de preguntas que solamente una persona adulta podría contestar con éxito se configura como un mecanismo a considerar ya no solamente para verificar el consentimiento parental sino también para verificar por lo menos la mayoría o minoría de edad del usuario. De este modo, unas respuestas poco concluyentes que conduzcan a considerar el futuro es usuario menor de edad, pueden conducir a los responsables a exigir métodos de verificación mayores a efectos de determinar la edad del usuario. Hasta la determinación de un método fiable de verificación, la medida traída a colación puede servir para cautelarmente, denegar el acceso al potencial usuario menor o acomodar el servicio a usuarios menores de edad al no arrojar resultados que una persona mayor de edad alcanzaría. Asimismo, se trata de un método que cumpliría con la proporcionalidad exigida por la CNIL e ICO citadas recientemente, pues no se requeriría en principio más información personal a efectos de verificar la mayoría o minoría de edad o el consentimiento parental[517]. Por otra parte, para los usuarios menores de edad que no hayan visto impedido su acceso, resulta de verdadero interés la propuesta de GIL MEMBRADO, consistente en emplear un *software* específico en orden a detectar la edad aproximada del usuario por medio del lenguaje y las

[516] Véase al respecto la página web del gobierno estadounidense Federal Trade Commission para la protección de los consumidores, en la que se establecen las reglas de protección de la privacidad en línea de los niños. Obtenido de: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4 (última consulta el 27 de octubre de 2021).

[517] Véase que la propia Comisión Europea reconoce la viabilidad de dichos mecanismos de verificación en su página web obtenida del siguiente enlace: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_es (última consulta el 4 de noviembre de 2021).

expresiones vertidas en los mensajes[518]. Véase que el señalado método, puede resultar verdaderamente útil para detectar la presencia de menores en estos espacios. Así, debería denegarse continuar empleando la plataforma a aquellos usuarios cuya minoría de edad detecte el programa empleado a tal efecto.

Podemos afirmar así, que las redes sociales vulneran sistemáticamente y de manera reiterada el habeas data del menor al no establecer sistemas de verificación de la edad del futuro internauta o la de sus representantes legales, incumpliendo el deber de responsabilidad proactiva que los proveedores de redes sociales deben probar (art. 5 RGPD) y que queda vulnerado en el presente contexto. De este modo, los tratamientos de datos personales de menores de edad no alcanzarán un grado mayor de seguridad hasta que se proceda a la implementación de mecanismos de verificación eficaces. Tanto es así que del consentimiento dependen, en gran medida, el cumplimiento de otra serie de garantías adicionales para los más jóvenes cuando emplean las redes sociales a diario, a saber: restringir determinadas funciones si el usuario es menor de 14 años como, evitar determinado tipo de publicidad o anuncios; configurar por defecto el perfil de la manera más restrictiva posible en orden a proteger la privacidad e intimidad del menor[519]; o impedir el etiquetado de terceras personas en sus publicaciones para evitar su consideración de responsable del tratamiento (circunstancia que ocurrirá cuando su perfil se configure de modo público o posea un elevado número de contactos).

En definitiva, la implementación de un mecanismo de verificación de la edad debe convertirse en una necesidad de primer orden para responsables del tratamiento, pero en especial para el legislador, que debe exigir legalmente la implantación de estos mecanismos con carácter urgente[520]. En la era del *big data* e IA, no parece creíble que la tecnología no permita verificar la edad *online* con garantías, por tanto, el legislador debe optar por sistemas que respeten las premisas expuestas a la mayor brevedad posible, pues

[518] GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 132.

[519] En efecto, tal y como señala GIRÓN REGUERA, el acceso de menores con edades manifiestamente inferiores a la legalmente establecida para otorgar un consentimiento válido al tratamiento, dificulta que los responsables puedan garantizar que los perfiles de los menores se configuren predeterminadamente de modo privado. GIRÓN REGUERA, E., "La protección de datos de los menores de edad en internet", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit*., p. 4272.

[520] Así, el propio Gobierno Español, reconoce que, promoverá la implantación de procedimientos para la verificación de la edad en el art. 10.2 de la Carta de Derechos Digitales aprobada en julio de 2021. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022), p. 12.

de ello depende la protección de los menores internautas cuando emplean redes sociales[521].

[521] En ese sentido, algunos Estados de EEUU se encuentran avanzados en la materia, pues están comenzando a aprobar normas que prohiben el manejo de redes sociales por parte de menores en caso de que no se verifique el consentimiento de los representantes legales al tratamiento de datos. Véase la norma aprobada por el Estado de Utah Bill HB 311, Social Media Usadge Amendments. Obtenido de: https://le.utah.gov/~2023/bills/hbillenr/HB0311.pdf (última consulta el 26 de abril de 2023).

CAPÍTULO IV:

HACIA UNA EXPERIENCIA PERSONALIZADA DEL USUARIO EN REDES SOCIALES COMO FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES. LA INTELIGENCIA ARTIFICIAL APLICADA AL PROCESO DE RECOPILACIÓN MASIVA DE INFORMACIÓN PERSONAL DEL MENOR CON FINES DE PUBLICIDAD Y MERCADOTECNIA DIRECTA

Las TIC han evolucionado de un modo vertiginoso en las últimas décadas, tanto es así que resulta complejo pensar en un día a día sin las múltiples funcionalidades que estas herramientas digitales aportan a nuestra vida. Tareas cotidianas, como realizar pagos a través de la banca *online*, programar el funcionamiento del aspirador o la alarma del hogar de modo remoto, comunicarse a través de plataformas de mensajería a tiempo real, se constituyen como comportamientos plenamente interiorizados en las personas. No obstante, este tráfico desinhibido de información multidireccional ha ocasionado la superproducción de miles de billones de datos a escala mundial, que posteriormente se someterán a tratamiento. Concretamente, por medio de búsquedas en Internet, interacciones en redes sociales, o incluso muchos de los dispositivos empleados como, por ejemplo, relojes o vehículos conectados a la red, se generan datos mediante el monitoreo constante del comportamiento de sus usuarios.

En este nuevo paradigma de recopilación masiva de información, se han desarrollado modernas soluciones de recopilación, almacenamiento, análisis y procesamiento de los datos personales. Todo ello, ha convertido los datos personales en un bien especialmente preciado para las entidades privadas, que por medio de métodos de análisis y soluciones técnicas posibilitan inferir de los datos disponibles, informaciones predictivas cuyo fin reside en informar los procesos de toma de decisiones. Así las cosas, lo verdaderamente característico de fenómenos como el *big data* o la IA no reside en un mero incremento en el volumen de información, sino en la complejidad de los procesos de tratamiento de datos y en su utilización para la toma de decisiones, ya que estos generan importantes tensiones con la protección de la información personal.

1. LA ERA DE LOS MACRODATOS

Las personas han almacenado paulatinamente grandes volúmenes de información en los formatos disponibles en cada época. Desde la invención de la escritura, hasta nuestros días, se ha sentido la necesidad de recoger, guardar y procesar la información recabada a efectos de que todo tipo de instituciones, públicas o privadas, desarrollen sus funciones y actividades[522]. Frente a la recopilación, conservación y procesamiento de la

[522] GARRIGA DOMINGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data y de la Computación ubicua, op. cit.*, p. 25.

información, pronto surgió la necesidad de clasificar los datos recabados con el fin de alcanzar una gestión más eficiente de los servicios disponibles. En este devenir, la primera empresa precursora en el tratamiento automatizado de datos personales nace de la mano de Herman Hollerith en el año 1884, cuya actividad consistía en desarrollar un sistema de cómputo mediante tarjetas perforadas en las que cada agujero representaba el sexo, la edad o raza, entre otros. Gracias a esta máquina tabuladora, el censo de Estados Unidos se confeccionó en dos años y medio, cinco años menos que el anterior censo confeccionado en 1880, ya que, entre otros beneficios, este sistema permitía clasificar la información de manera sencilla, a la vez que proveía el conocimiento sobre cuántas tarjetas cumplían determinados requisitos o parámetros[523].

Sin embargo, el nivel de desarrollo digital desde la invención de la máquina tabuladora nos remite a una realidad sin precedentes en cuanto a las posibilidades sobre el análisis y clasificación de datos. Ahora bien, el objetivo continúa tratándose del mismo que siglos atrás, extraer el mayor rendimiento posible a los datos disponibles. En efecto, desde la última década del siglo XX, el rápido desarrollo de Internet y el desenfrenado incremento de los servicios disponibles a través de la red, han concedido acceso a toda clase de información. Ciertamente, la aparición de ordenadores y dispositivos ha posibilitado el almacenamiento de un volumen de datos mayor que la que se podría imaginar años atrás. En ese sentido, en el año 2010 se habían producido 5 exabytes de información desde el amanecer de la civilización hasta el año 2003[524]. No obstante, en el año 2019 esa misma cantidad de datos se creaba al día[525].

Es cierto que imaginar la magnitud del tratamiento de dichos datos puede resultar complejo, por lo que, pueden ayudar a comprender la dimensión de este fenómeno dos ejemplos de MAYER SCHÖNBERGER y CUKIER cuando afirman que, si dichos datos se encontraran impresos en libros, cubrirían la superficie entera de Estados Unidos o de hallarse grabados en CD-ROMs apilados, alcanzarían la luna formando cinco pilas separadas[526].

[523] *Ibid*, p. 26.
[524] Para mayor entendimiento, 1 exabyte equivale a un millar de millones de gigabytes.
[525] TORO, M., y LANIADO, H., "Big data: historia, definición, herramientas y aplicaciones en la industria", *Revista VirtualPro*, 2019, núm. 204, p. 2.
[526] MAYER-SCHÖNBERGER, V., Y CUKIER, K., *Big Data. La revolución de los datos masivos*, Turnen Noema, Madrid, 2015, pp.187-211.

Como es de intuir, de conformidad con COTINO HUESO, estos datos no pueden constituir objeto de análisis, manipulación y procesamiento por medio de mecanismos tradicionales[527]. En consecuencia, la necesidad en la exploración de nuevos métodos de análisis de grandes escalas de datos, ha conducido al aumento de la capacidad informática en el procesamiento y almacenamiento de datos.

Más no se trata tan solo de propiciar que a las compañías privadas el logro de un mayor rendimiento de los datos personales recabados en la red. En este contexto, la protección de la privacidad se torna verdaderamente compleja, en el sentido que, cuanto mayor volumen de información se comparta a través de un canal abierto al mundo como Internet, más probable resultará que los datos personales se sometan a tratamientos cada vez más intrusivos. Efectivamente, el rendimiento que las compañías privadas generan a través de las interacciones de los usuarios en la red, genera nuevos riesgos hasta la fecha insospechados para los datos personales.

El ingente volumen de datos disponibles en la red ha desembocado en el nacimiento del nuevo fenómeno denominado *big data*. El término ve la luz por primera vez de la mano de SCHÖNBERGER y CUKIER en el año 2013 para referirse a dicho fenómeno que, en español, recibe el nombre de "macrodatos"[528]. Ahora bien, el término *big data* alude a una técnica mucho más compleja que a la disponibilidad de un gran volumen de datos[529]. A propósito de ello, el *big data* se refiere a dos cuestiones íntimamente relacionadas entre sí: de un lado, al gran volumen de datos disponibles; pero de otro lado, al conjunto de tecnologías cuyo objetivo reside en tratar grandes cantidades de datos a través del empleo de complejos algoritmos y estadística[530]. Así, el fin último de la aplicación de dichas operaciones a la suma de información recabada, se halla en la

[527] COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, 2017, núm. 24, p. 132.

[528] MAYER-SCHÖNBERGER, V., Y CUKIER, K., *Big Data. A revolution That Will Transform How We Live, Work and Think*, London, Ed. John Murray, 2013.

[529] En efecto, tal y como señala PLAZA PENADÉS, los datos se configuran como un bien verdaderamente preciado no para quien los posea, sino para quienes sepan emplearlos para extraer de los mismos información. PLAZA PENADÉS, J., "Los derechos en la era digital (Comentario al artículo 79 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 3864.

[530] GARRIGA DOMINGUEZ, A., "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea", *Derechos y libertades*, 2018, núm. 38, Época II, p. 112.

realización de predicciones, así como en la extracción de información que hasta ese momento resultaba desconocida, todo ello, en orden a favorecer la toma de decisiones.

Si bien no disponemos de una definición unánime del *big data*, podemos tomar como referencia la configurada por SOTO cuando afirma que el *big data* se refiere al tratamiento de grandes volúmenes de datos a través de algoritmos matemáticos con la finalidad de establecer correlaciones entre estos, predecir tendencias y tomar decisiones[531]. De manera semejante conceptualiza el Parlamento Europeo el fenómeno de los "macrodatos" cuando dispone que este se refiere a la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos los personales, procedentes de diferentes fuentes objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, empleando a tal efecto tanto los datos almacenados como los transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones[532].

Así, un algoritmo se configura como una secuencia de instrucciones, que insertas en un programa informático, pueden acometer procesos similares a los llevados a cabo por seres humanos. A modo de ejemplo, estos programas albergan la capacidad de realizar tareas sencillas como contar el número de matrículas formalizadas en un curso, pero también de calcular el riesgo de reincidencia de las personas condenadas penalmente[533].

Ciertamente, el *big data* supone una nueva manera de procesar la información a nivel global ante la falta de medios tecnológicos que propiciaran la necesidad de analizar y procesar el volumen de datos disponibles[534]. En este quehacer, los sistemas de *big data*

---

[531] SOTO, Y., "Datos masivos con privacidad y no contra privacidad", *Revista Biología y Derecho*, 2017, núm. 40, p. 102. En términos similares define la tecnología *big data* GIL GONZÁLEZ, cuando afirma que se puede definir esta técnica como el conjunto de nuevas tecnologías que permiten analizar ágilmente, a través del uso extenso de algoritmos, cantidades masivas de datos provenientes de fuentes dispares con el objetivo de crear valor. GIL GONZÁLEZ, E., "Big Data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley*, septiembre 2017, núm. 9050, p. 2.

[532] Considerando A) de la Recomendación del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, Diario Oficial de la Unión Europea, C 263/10, de 25 de julio de 2018.

[533] SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Revista de Derecho Público: Teoría y Método*, 2021, vol. 3, p. 87.

[534] En ese sentido, destacamos las palabras de CASAS ROMA, NIN GUERRERO y JULBE LÓPEZ cuando afirman que empresas de Internet como Google o Amazon se encontraron con serios problemas para continuar desempeñando sus tareas cotidianas ante el colosal volumen de datos disponible. Efectivamente, el volumen de datos generado imposibilitaba su procesamiento en un único ordenador. Por lo tanto, se debía acudir a un procesamiento distribuido para involucrar distintos ordenadores que trabajaran con los datos de manera paralela a efectos de procesarlos en menor tiempo. Por otra parte, los datos habían de procesarse de manera rápida, aunque el número disponible resultase elevado. Así, por ejemplo, piénsese que resultaría poco útil que un buscador devolviera los resultados de la búsqueda introducida después de una hora. En

no se limitan a recabar y procesar grandes bancos de datos, sino que se propone agregar valor a los volúmenes de datos poco utilizados o incluso inaccesibles hasta la fecha con fines de descubrir un conocimiento hasta hoy oculto. De conformidad con PUYOL MORENO, lo que se busca por medio de esta tecnología, consiste en descubrir conocimiento oculto a partir de grandes volúmenes de datos[535], en orden a convertirlo en información valiosa.

En definitiva, el empleo de algoritmos no obedece a un fenómeno novedoso en sí mismo. El empleo de los mismos se remonta varios siglos atrás con diversas aplicaciones prácticas, véase que el término proviene del griego antiguo *Arithmos*[536]. Ahora bien, lo verdaderamente destacable se halla en que, determinadas categorías de algoritmos albergan la capacidad de arrojar predicciones basadas en datos. Es más, en la actualidad, cabe la posibilidad de que una serie de algoritmos simulen una suerte de razonamiento humano en la toma de decisiones e inferencia de nuevos datos. Estos algoritmos, se encuadran en el campo de la IA, técnica cuyo análisis desarrollaremos con posterioridad.

2. TÉCNICAS DE ANÁLISIS MASIVOS DE DATOS PERSONALES EN REDES SOCIALES: UN NUEVO DESAFÍO PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DEL MENOR

Asentado que el *big data* se refiere a una serie de técnicas de captura, almacenaje, búsqueda y puesta en valor de datos inaccesibles, cabe preguntarse el origen de los datos disponibles para su posterior tratamiento por medio de la técnica expuesta. En ese sentido, tal y como se ha anticipado, el 70% del universo digital lo han generado las propias personas a través de las constantes interacciones en los diferentes servicios *online* como redes sociales, buscadores, blogs, emails, etc.[537]. Sobre esta cuestión, debemos incidir en que, cuanto más activos resulten los usuarios en estos servicios, mayor resultará también la información puesta a disposición para su posterior análisis.

consecuencia, estas compañías se vieron en la necesidad de crear nuevas tecnologías que les permitieran continuar con el modelo de negocio que ellas mismas habían creado. CASAS ROMA, J., NIN GUERRERO, J., y JULBE LÓPEZ, F., *Big data: análisis de datos en entornos masivos*, Barcelona, UOC, 2019, pp. 25-26.

[535] PUYOL MORENO, J., "Una aproximación a Big Data", *Revista de Derecho UNED*, 2014, núm. 14, p. 485.

[536] PERIS MANGUILLOT, A., "Algoritmos: ¿podemos hacerlos transparentes y trazables en su proceso?", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2022, p. 71.

[537] CRAIG, T., y LUDLOFF, M., *Privacy and Big Data*, Sebastopol (California), O´Really, 2011, p.4.

2.1. La inevitable relación entre los datos de carácter personal y el desarrollo de las técnicas de análisis masivos de datos

Particularmente, dos son los ámbitos de nuestro comportamiento *online* que contribuyen a una mayor generación de datos. Por una parte, las redes sociales en las que los usuarios comparten información voluntariamente, pero en las que también dejan un rastro económicamente rentable para el proveedor del servicio[538]. Por otra parte, en los últimos años se ha observado un incremento considerable de datos creados por sensores conectados a dispositivos que a su vez se conectan a Internet, como relojes inteligentes, *smartphones*, tabletas, sistemas inteligentes etc. Así las cosas, los usuarios generaban en 2020 una media de 1,7 megabytes cada segundo por medio de su actividad *online*[539].

Así es que, cuando se accede a la red se genera lo que se conoce como un rastro digital, esto es, una huella que las interacciones de los usuarios arrojan en la red. Efectivamente, cada movimiento *online*, genera una información susceptible de captura para su posterior tratamiento. En realidad, la información que puede recabarse para su análisis no se refiere únicamente a aquellos datos que voluntariamente se comparten en el universo en línea, sino también todos aquellos que, de manera involuntaria se generan con el habitual empleo de estas herramientas digitales. Nos referimos así a lo que LLANEZA GONZÁLEZ califica como datos pasivos, esto es, toda aquella información intercambiada en segundo plano por el dispositivo y las aplicaciones sin ninguna notificación obvia al usuario[540]. En el contexto descrito, los usuarios menores de edad, propensos a compartir mucha y variada información, ponen a disposición de las empresas cuyo lucro reside en analizar datos masivamente, la materia prima que permite su actividad: la información.

En este contexto digital, debemos añadir que los datos disponibles no provienen únicamente de las interacciones en la red de los usuarios. En los últimos años, la popularidad en el empleo de objetos cotidianos conectados a la red ha avanzado considerablemente hasta la denominación de dichos aparatos como Internet de las

[538] Redes sociales como Facebook generan 1,5 petabytes de datos al día. HOLMES DAWN, E., *Big data: una breve introducción*, Barcelona, Antoni Bosch, 2017, p. 16.
[539] Informe "Data Never Sleeps 8.0" elaborado por DOMO. Obtenido de: https://www.domo.com/learn/data-never-sleeps-8 (última consulta el 26 de mayo de 2021).
[540] LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*, *op. cit.*, p. 75. Tanto es así que, la propia autora afirma en su obra que Google recopiló o infirió más de dos tercios de la información de los usuarios a través de medios pasivos identificando al final del día los intereses del usuario con una precisión destacable.

cosas[541]. Estos dispositivos de uso común como relojes, aspiradores, tabletas, teléfonos, recopilan información sobre el uso que se realiza de los mismos, transformando aquella en datos que se constituirán objeto de tratamiento. En la práctica, estos aparatos miden hábitos como el empleo que se concede al dispositivo, pero también sobre hábitos diarios como las horas de sueño, pulsaciones, etc. Así las cosas, en la actualidad muchos de los datos quedarán disponibles para su posterior análisis en Internet, arrojando informaciones verdaderamente detalladas sobre aspectos personales.

Directamente relacionado con el Internet de las cosas, hemos de referirnos a los dispositivos que permiten geolocalizar la posición del dispositivo en uso. Los teléfonos móviles, los relojes, los coches, y una gran variedad de objetos conectados a la red, ofrecen la posibilidad de localizar la posición geográfica del dispositivo, y, por ende, la del usuario del mismo. Efectivamente, estos aparatos realizan un seguimiento constante de la posición del dispositivo, llegando a determinar con exactitud el lugar donde reside la persona usuaria, dónde aparcó su vehículo por última vez, dónde se encuentra su centro de trabajo, etc.

Sin embargo, esta técnica cuya aplicación puede resultar muy práctica en publicidad como veremos posteriormente, puede conllevar resultados lesivos para la privacidad de las personas, especialmente si los usuarios de estos dispositivos no alcanzan la mayoría de edad. Mediante el uso de estos dispositivos por menores, se puede inferir sin dificultad el colegio al que acuden, el lugar en el que realizan sus actividades extraescolares o incluso el lugar en el que se emplaza su domicilio. Incluso se pueden llegar a inferir datos sensibles, como visitas a hospitales o lugares de culto sin que el usuario tome conciencia de ello.

Definitivamente, cobran sentido las afirmaciones expuestas hace escasas líneas cuando disponíamos que el volumen de datos compartidos diariamente por las personas usuarias comienza a resultar incuantificable. El éxodo de los hábitos al contexto *online* se considera como principalmente responsable de que, cada vez más compañías visionen la posibilidad de lucrarse gracias al rastro digital que las interacciones generan en la red.

[541] Véase en ese sentido el Dictamen 8/2014, del Grupo de Protección de datos del Artículo 29 sobre la evolución reciente del Internet de los objetos, de 16 de septiembre de 2014, WP 223, p.4.

En cambio, tal y como se ha expuesto hace escasas líneas, el fenómeno del *big data* no se caracteriza exclusivamente por la disponibilidad masiva de datos, sino por la capacidad tecnológica que se ha desarrollado para su tratamiento y análisis. De acuerdo con MAYER SCHÖNENBERGER y CUKIER el valor no reside en los datos sino en la forma de correlacionarlos entre sí para descubrir patrones[542]. En particular, la huella digital se emplea para la transformación de datos aparentemente irrelevantes, en un perfil detallado de las personas que comparten dicha información. Esto es, la capacidad tecnológica del *big data* reside en buscar referencias cruzadas de esos grandes volúmenes de datos, muchos de ellos personales, que permiten obtener patrones de comportamiento y perfiles verdaderamente detallados de las personas[543]. Al hilo de lo expuesto por MORENTE PARRA, nos encontramos ante una nueva tecnología de tratamiento y análisis de datos, o dicho de otro modo, de un nuevo método de trabajo en el procesamiento de información entre los que se encuentra, entre otros, la elaboración de perfiles[544].

En la consecución de esta operación, intervienen tres tipos de sujetos: en primer lugar, aquellos que generan los datos, bien de manera consciente o inconscientemente (los usuarios de la red); en segundo lugar, los sujetos que detentan los medios para recabar los datos, como por ejemplo una red social; en tercer lugar, los analistas de estos datos recabados de las interacciones en la red. Estos últimos, han hallado la tecnología para atribuir un valiosísimo rendimiento de los datos en la red. Ello se debe a que, estos analistas, también conocidos como científicos de los datos, han desarrollado una tecnología capaz de generar patrones que predicen tendencias de futuro[545]. No obstante, el riesgo resulta evidente en el sentido que, los patrones de conducta obtenidos como resultado de la aplicación de esta técnica, no se limitan a describir la realidad del presente, sino que, muestran el futuro probable.

---

[542] MAYER-SCHÖNBERGER, V., Y CUKIER, K., *Big Data. A revolution That Will Transform How We Live, Work and Think, op, cit.*

[543] En palabras de ARMADA VILLAVERDE y LÓPEZ BUSTABAD, la elaboración de perfiles y las decisiones automatizadas, constituyen una parte integral de los procesos de *big data*. ARMADA VILLAVERDE, M.E., Y LÓPEZ BUSTABAD, I.J., "El Reglamento General de Protección de Datos ante el fenómeno del "Big Data", *Revista Aranzadi de Derechos y Nuevas Tecnologías,* 2019, núm. 51, p. 18.

[544] MORENTE PARRA, V., "El Big Data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", *Derechos y libertades,* 2019, núm. 41, Época II, p. 227.

[545] El término científico de los datos se emplea para identificar a aquellas personas que trabajan en el campo de los datos masivos. HOLMES DAWN, E., *Big data: una breve introducción, op. cit.,* p. 101.

En efecto, la información que ha dejado huella en Internet, se recopila, clasifica y analiza por estos analistas, proporcionando un valor a la información que previamente permanecía descontextualizada en la red. Más aún, se ha llegado a la creación de un sistema capaz de anticipar las decisiones de una concreta persona, para posteriormente llegar a influir en ellas[546]. Esta capacidad de incidir en la toma de decisiones, resulta más sencilla si la persona se encuentra en tránsito hacia su madurez como puede tratarse del caso de un menor de edad. Sobre este aspecto volveremos en apartados posteriores de la investigación que aquí se trabaja.

Por otra parte, los últimos años son testigos de la proliferación de nuevas técnicas de tratamiento de datos masivos como la IA para los que el *big data* se erige como el motor necesario[547]. Antes bien, IA, no es un fenómeno novedoso del presente siglo, ya en el año 1982, FROSINI dedicaba unas líneas a este fenómeno de tratamiento de datos[548]. En esencia, la IA busca simular el comportamiento de la mente humana en máquinas a través de diversas técnicas[549]. En efecto, la Comisión Europea señala que el término IA se aplica a los sistemas que manifiestan un comportamiento inteligente, dado que estos se muestran capaces de analizar su entorno y pasar a la acción-con cierto grado de autonomía-con el fin de lograr objetivos específicos[550]. De este modo, las principales características de la IA podrían resumirse en dos: por una parte, la recopilación masiva de información del entorno que la rodea; por otra parte, la capacidad que esta posee de

[546] Con manifiesto acierto, GARRIGA DOMÍNGEZ afirma que estas técnicas permiten una peligrosa filosofía de la anticipación. Véase GARRIGA DOMÍNGUEZ, A., "Decisiones automatizadas basadas en algoritmos y protección de datos personales", en TOMÁS MALLEN, B., GARCÍA MAHAMUT, R., y PAUNER CHULVI, C., (Editores), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español*, Valencia, Tirant lo Blanch, 2022, p. 339.

[547] El término Inteligencia Artificial nace en Los Ángeles en el año 1955 en un congreso sobre máquinas que aprenden. Así John McCarthy introduce la expresión "inteligencia artificial" en 1956, refiriéndose con ella a la creación de máquinas que pueden considerarse inteligentes porque interactúan con los seres humanos de tal modo que un ser humano no pueda apreciar si interactúa con otra persona humana o una máquina. CORTINA ORTS, A., "Ética de la Inteligencia Artificial", *Anales de la Real Academia de Ciencias Morales y Políticas*, 2019, núm. 96, p. 382. Sobre la estimación del *big data* como presupuesto indispensable para el funcionamiento de la IA véase CASTELLANOS CLARAMUNT, J., "La gestión de la información en el paradigma algorítmico", *Métodos de información*, 2020, núm. 21, p. 60.

[548] Efectivamente, FROSINI afirma que el ordenador representa una prótesis electrónica de la inteligencia humana, por eso cabe referirse a ella como inteligencia artificial, pues actúa como una mimesis mecánica de la inteligencia humana. FROSINI, V., *Cibernética, derecho y sociedad*, Madrid, Tecnos, 1982.

[549] Guía de la AEPD sobre la Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, febrero de 2020. Obtenido de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (última consulta 16 de julio de 2021), p. 5.

[550] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico Social Europeo y al Comité de las Regiones, sobre "Una Inteligencia artificial para Europa", de 25 de abril de 2018, COM (2018) 237 final, p. 1.

tomar decisiones o acciones autónomas para un fin concreto y determinado. Antes bien, como señala ESPARZA LEIBAR, todavía no encontramos una definición convincente ni clara sobre la IA[551].

Así las cosas, el énfasis realizado por la industria tecnológica en el desarrollo de este tipo de técnicas, ha conducido a la aparición de diversas categorías de IA. Por una parte, hallamos el aprendizaje automático o *machine learning* cuya finalidad reside en, a partir de grandes volúmenes de datos, detectar patrones y aprender a realizar predicciones y recomendaciones sin recibir instrucciones explícitas previas de programación. Estos algoritmos, se adaptan en respuesta a nuevos datos y experiencias en orden a mejorar su eficacia en las predicciones a lo largo del tiempo[552]. Por otra parte, se encuentra el aprendizaje profundo o *deep learning,* acometido por redes neuronales. Tal y como señala PERIS MANGUILLOT, una red neuronal artificial, consiste en un conjunto de unidades llamadas neuronas artificiales, conectadas entre sí con el fin de transmitirse señales. Así, la información de entrada, atraviesa la red neuronal (donde se somete a diversas operaciones) produciendo determinados valores de salida[553]. Esta red neuronal, puede cargar un gran volumen de datos de entrada y procesarlos a través de las múltiples capas que aprenden características cada vez más complejas sobre esta información. Seguidamente, la red neuronal puede tomar una decisión sobre los datos, además de conocer si esta es correcta, con el fin de emplear lo aprendido en otra resolución sobre otros datos nuevos. A modo de ejemplo, la red neuronal puede aprender la apariencia de un objeto, para a posteriori, reconocerlo en una nueva imagen[554].

Adicionalmente, se pueden encontrar tres tipos de aprendizaje automático, a saber: el aprendizaje supervisado, el aprendizaje sin supervisión y, por último, el aprendizaje reforzado. En el primero de ellos, el algoritmo emplea datos de entrenamiento y los comentarios de los humanos para conocer la relación de los *inputs* para un resultado dado. En este caso, las personas clasifican los datos de entrada al algoritmo y el tipo de

[551] ESPARZA LEIBAR, I., "La Inteligencia Artificial y el derecho fundamental a la protección de datos personales", en BARONA VILAR, S., (Editora), *Justicia algorítmica y neuroderecho: una mirada multidisciplinar,* Valencia, Tirant lo Blanch, 2021, p. 266.
[552] Para mayor detalle consultar LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos, op. cit.,* pp. 119-120.
[553] PERIS MANGUILLOT, A., "Algoritmos: ¿podemos hacerlos transparentes y trazables en su proceso?", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial, op. cit.,* p. 74.
[554] LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos, op. cit.,* pp. 119-120.

comportamiento que desean predecir, precisando del algoritmo para su cálculo. En el segundo tipo de aprendizaje automático, el algoritmo no recibe instrucciones de entrada ni una variable de salida concreta, deberá el propio algoritmo hallar la clasificación de los datos, así como los patrones entre estos. Por último, el aprendizaje reforzado supone que el algoritmo aprenda a realizar una tarea procurando maximizar las recompensas que recibe por sus acciones. En este caso, no se cuenta con datos de entrenamiento variados ni se define lo que se desea lograr al algoritmo, pero este aprende en el terreno interactuando con el mismo.

En definitiva, puede advertirse que los algoritmos que se encuadran en el campo de la IA se encuentran dotados de mayor complejidad que los algoritmos empleados hasta la fecha[555]. Estos, pueden llegar a advertir acciones humanas como detectar emociones, seguir a un individuo a medida que envejece, conocer si un individuo llora o se ríe y tomar decisiones en consecuencia. Así, estos algoritmos, interactúan con las personas, toman decisiones concernientes a las mismas basadas en datos. Como cabe esperar, la puesta en práctica de esta tecnología en diversos sectores gracias la disponibilidad de un ingente volumen de datos de diversas categorías, apareja nuevos riesgos para la protección de los datos de las personas usuarias de Internet.

Desde el punto de vista de la protección de datos de carácter personal, la fricción que estas técnicas de tratamiento generan con la información personal resultan evidentes. Principalmente porque la base tanto del *big data* como de la IA reside en la capacidad de extraer un rendimiento o una predicción de los datos, de suerte que, se generen nuevos datos a partir de los datos primitivos. Sin embargo, en muchas ocasiones, el usuario no ha consentido el tratamiento de estos datos inferidos.

A ello se debe agregar, que las principales entidades que emplean esta tecnología, se constituyen como compañías privadas cuyo fin reside en el lucro, mas este se alcanza a través del tratamiento masivo de datos generados por las personas usuarias. De igual suerte, persuadidas por el potencial valor económico que los datos pueden proporcionar, las empresas privadas han desarrollado mecanismos de recogida de datos que monitorizan

[555] Ya en el siglo XVII, Leibniz creía que el pensamiento cognitivo y la lógica podrían reducirse a una suerte de expresiones binarias. CHABERT, J.L., "A History of Algorithms: From the Pebble to the Microchip", en STEINER, C., *Una breve historia de hombres y algoritmos*, 1999. Obtenido de: https://catedradatos.com.ar/media/5.-Steiner-Una-breve-historia-de.pdf (última consulta el 7 de febrero de 2022), p. 5.

el comportamiento de sus usuarios garantizándose la disponibilidad de la materia prima que les permite lucrarse: los datos. En definitiva, las compañías abogan por sistemas de recogida masiva de datos personales en orden a aumentar los datos sobre los que extraer predicciones del comportamiento de sus millones de usuarios[556].

Con todo, mucha de la información recabada posee carácter personal y a pesar de ello, se emplea para extraer más informaciones inferidas de los datos recabados. Sobre este aspecto, cabe mencionar, además, que los potentes algoritmos albergan la capacidad de deducir informaciones de carácter sensible no desveladas por los propios usuarios. Sirva como ejemplo que, de las múltiples de interacciones en la red, los analistas de datos cuentan con la posibilidad de deducir la orientación sexual de una persona a partir de la información compartida por esta, todo ello a pesar de que dicha información no revele de por sí dicha orientación[557].

En definitiva, como quedará de manifiesto en apartados posteriores, tanto el *big data* como la IA se posicionan como una nueva preocupación para la protección de datos de carácter personal, especialmente de los menores de edad. De conformidad con GARRIGA DOMINGUEZ, personas ajenas a nuestro entorno toman determinadas decisiones que afectan a las personas en base a informaciones que estos usuarios no han suministrado, o lo han hecho con otras finalidades[558]. Es más, esas personas que no nos conocen, forman parte de compañías privadas que como quedará de manifiesto, no en todas las ocasiones respetarán los límites a la privacidad de las personas usuarias.

2.2. Sobre el empleo de técnicas de *big data* e inteligencia artificial por proveedores redes sociales como instrumento para rentabilizar sus servicios

La extracción de valor de los datos con el fin de rentabilizarlos en múltiples sectores tanto públicos como privados, sitúan al *big data* y a la IA como una nueva

[556] Véase así la política de privacidad del Grupo Meta cuando informa sobre las diversas categorías de datos que se someterán a tratamiento por la empresa. Política de privacidad del Grupo Meta obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse , apartado ¿Qué información recogemos?, (última consulta el 21 de septiembre de 2022), pp. 3-4.

[557] Así, una investigación revela que a través del análisis mediante algoritmos de los "Me gusta" proporcionados por los usuarios de la red social Facebook se pueden revelar rasgos y atributos privados, muchos de ellos altamente sensibles como la raza, sexo u orientación sexual, entre otros. WACHTER, K., "Los rasgos y atributos privados son predecibles a partir de registros digitales del comportamiento humano", *PNAS*, 2013, núm. 15, p. 5802.

[558] GARRIGA DOMINGUEZ, A., "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea", *op. cit.*, p. 126.

oportunidad a la hora de lograr ventajas comerciales. Lo cierto es que cualquier empresa desea obtener más información acerca de sus usuarios, motivo por el que estas recopilan y almacenan datos con el fin de posteriormente someterlos a análisis. El objetivo de dicha recopilación se halla generalmente en conocer mejor a sus clientes para ofrecerles productos que mejor se adecúen a sus necesidades[559].

Efectivamente, la llegada de técnicas de análisis masivos de datos como las expuestas ha facilitado considerablemente la posibilidad de obtener perfiles de consumo verdaderamente detallados. Muchos usuarios de aplicaciones *online*, Internet, redes sociales, etc., ceden sus datos para determinados fines concretos: en el caso de las redes sociales, a cambio de disponer de una plataforma de comunicación; en las aplicaciones de salud, por ejemplo, para proveerse de una relación médico-paciente más directa. Sin embargo, este nuevo modo de operar puede vulnerar el derecho a la protección de datos personales. Las redes sociales almacenan todos los datos que los usuarios comparten en su plataforma como, los "me gustas", sus contactos, los comentarios publicados, etc., pero también aquella información que los usuarios comparten fuera de sus espacios, de modo que, redes sociales como Twitter, Instagram, Facebook o TikTok conocen todos los detalles acerca de las conexiones, opiniones, modo de comportarse y preferencias personales de sus usuarios. En definitiva, los proveedores de redes sociales recopilan información de un gran abanico de fuentes, incluida aquella que no se comparte en sus plataformas[560].

Tal y como se ha expuesto anteriormente, los patrones diarios de la vida de las personas, unidos al conjunto de datos personales que se encuentran disponibles sobre las personas en la red (especialmente en redes sociales), arrojan un perfil detallado sobre los atributos personales, gustos y preferencias, entre otros, de los usuarios. En consecuencia,

---

[559] Tal es la capacidad de las empresas analistas de datos masivos de hallar correlaciones que, Amazon ha patentado el envío anticipado denominado *Method and System for Anticipatory Package Shipping*, un sistema basado en el análisis de datos masivos consistente en prever de antemano lo que encargará el cliente para proceder al envío del pedido al centro de reparto de manera previa a la materialización del encargo. HOLMES DAWN, E., *Big data: una breve introducción, op. cit.,* p. 97.

[560] Así, los proveedores de redes sociales recopilan, a grandes rasgos, la información que los usuarios comparten activamente en su perfil, aquella que su comportamiento en el espacio genera, pero también toda la información pública en la red, además de la compartida con otros responsables del tratamiento que se consideren colaboradores de la red social. Véase así la política de privacidad del Grupo Meta cuando informa sobre las diversas categorías de datos que se someterán a tratamiento por la empresa. Política de privacidad del Grupo Meta obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse , apartado ¿Qué información recogemos?, (última consulta el 21 de septiembre de 2022), pp. 3-4.

esta información tan pormenorizada, habitúa a compartirse (bien por venta, alquiler, cesión…) con terceras empresas publicitarias que conocerán con precisión las inclinaciones y hábitos de los usuarios para ofrecerles publicidad basada en sus preferencias. Tal y como afirma SOTO, podemos encontrar empresas que se dedican de manera exclusiva a la compraventa o alquiler de datos con la finalidad de conocer mejor a los usuarios o a la población y así, ofrecer productos que se adecuen mejor a sus necesidades y preferencias[561].

Actualmente, tal es el uso de Internet, que los anunciantes se decantan por dirigir su atención a este espacio y, en especial, a las redes sociales a la hora de transmitir su publicidad. Tal y como dispone PEGUERA, muchos servicios que se muestran gratuitos para las personas usuarias –como el que ofrecen las redes sociales- basan su rentabilidad en los ingresos derivados de la publicidad[562]. Concretamente, las redes sociales buscan un mayor número de usuarios a efectos de incrementar su rentabilidad a través de los ingresos que la publicidad ofertada les ofrece[563]. Cabe destacar, que la importancia de la publicidad *online* se refleja en cifras de inversión, en el sentido que, en 2019 la inversión en Internet se consolidaba en primera línea, pues esta se situaba 3.150 millones de euros por encima de la televisión, alcanzando un 46,7% de toda la inversión realizada en medios[564].

Así, los datos que el usuario aporta, pero también los que genera involuntariamente a través del empleo de dichos servicios, se someterán a tratamiento por el proveedor de la red social con el fin de emplearse en marketing personalizado. Además, estas nuevas técnicas predictivas de análisis masivos de datos propician que la publicidad *online* se caracterice por la posibilidad de un altísimo grado de contextualización y personalización. No obstante, debemos diferenciar distintos mecanismos o técnicas de

[561] SOTO, Y., "Datos masivos con privacidad y no contra privacidad", *op. cit.*, p. 112.
[562] PEGUERA POCH, M., "Publicidad online basada en comportamiento y protección de la privacidad", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores) *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2ª ed., 2013. (versión online sin paginación).
[563] De este modo, la red social Facebook ingresó 70.000 millones de dólares en 2019 por esta vía publicitaria, seguida de YouTube con un ingreso de 15.200 millones. Posteriormente se posiciona Twitter con 3.000 millones y finalmente, Snapchat con un ingreso de 1,700 millones. RISBERG, E., "Las cinco redes sociales más poderosas en ingresos publicitarios", *Semana.* Obtenido de: https://www.semana.com/empresas/articulo/cuales-son-las-redes-sociales-con-mas-ingresos-publicitarios/291323/ (última consulta 22 de junio de 2021).
[564] Guía sobre el uso de las cookies de la AEPD, de julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta 1 de julio de 2021).

publicidad *online* disponibles sin perjuicio de que éstas puedan emplearse conjuntamente o de manera combinada.

En primer lugar, la publicidad contextual se refiere a aquella que se relaciona con la información que el usuario visualiza en un momento dado en una página web concreta. Es decir, el propósito de este tipo de publicidad se encuentra en lograr que los anuncios que se presentan en una determinada página guarden relación con el contenido de la misma dado que se presupone que el contenido de esta página web que se visita redunda en los intereses del usuario. Sirva como ejemplo, que la publicidad mostrada en las páginas web, guardará relación con la búsqueda introducida en el buscador de Google[565]. Sin embargo, este tipo de publicidad *online* no alcanza un grado de personalización elevado, ya que, no necesita algoritmos predictivos para su funcionamiento, ni de un rastreo exhaustivo de la actividad del usuario.

En segundo lugar, la publicidad personalizada se refiere a aquella que se adapta a las características de los usuarios y precisa que previamente estos hayan procedido al registro en la plataforma, compartiendo con el proveedor de estos servicios datos propios como la edad, sexo, estudios, condición civil o situación geográfica. Este tipo de publicidad, como veremos posteriormente, se emplea a menudo por los proveedores de redes sociales. Ello se debe principalmente a que los proveedores de redes sociales cuentan con una base de datos personalizada sobre los intereses de los usuarios que ellos mismos revelan libre y voluntariamente en la plataforma[566], además de los datos pasivos, que de manera inconsciente también ponen a disposición del proveedor de la red social cuando emplean su servicio.

En tercer lugar, la publicidad social consiste en mostrar al usuario publicidad *ad hoc* en relación a la interacción que comparte con otros usuarios. En concreto, la publicidad social emplea los datos del perfil de una persona, sus contactos sociales e información de sus relaciones con otros usuarios para incorporarlos a la propia publicidad que se muestra a la red de contactos de dicho usuario[567].

Por último, en los últimos años se ha extendido la personalización de la publicidad basada en la observación del comportamiento del usuario a través del rastreo del historial

[565] A modo de ejemplo, en páginas web sobre deporte aparecerán anuncios sobre artículos de deporte. En páginas sobre vehículos, se mostrarán anuncios sobre vehículos, etc.
[566] PÉREZ BES, F., *La publicidad comportamental online,* Barcelona, UOC, 2012, pp. 34-35.
[567] *Ídem.*

de navegación. Sin intención de ahondar ahora, pues no es objeto del presente apartado, cada detalle del comportamiento *online* del usuario se almacena y comparte con proveedores de publicidad tras la instalación de una *cookie* en el dispositivo del internauta. Así, la información recabada tras la monitorización de la conducta del usuario, desvela las pautas, gustos de consumo, etc., de este en cuestión de segundos, en orden a proporcionar al usuario anuncios a medida basados en los intereses inferidos de su comportamiento *online*[568].

En virtud de lo expuesto, los proveedores de redes sociales habitúan a combinar diversas técnicas de publicidad *online* entre las que destacan: la publicidad basada en la los datos proporcionados por los usuarios al proveedor de redes sociales; la publicidad basada en la observación del comportamiento del usuario de la red social, concretamente del análisis del rastro que el uso de la red social arroja; por último, la publicidad basada en datos inferidos a raíz de los datos proporcionados por los usuarios de la red social.

En definitiva, las redes sociales forman parte de un complejo entramado publicitario en el que desempeñan un papel fundamental: proveer de un elevado volumen de datos personales de las personas usuarias de su servicio. En los casos más sencillos, es posible, que los anunciantes solamente deseen conocer los usuarios que reúnen determinada característica como, por ejemplo, la edad. Antes bien, estas técnicas aparejan mecanismos más complejos que pueden poner en riesgo la privacidad de las personas. En realidad, la variada información desvelada por el usuario, unida a la que su navegación arroja, correctamente sometida a análisis con parámetros del *big data* e IA se convierte en una información con alto valor añadido para las empresas anunciantes, ya que se pueden inferir informaciones que el usuario no ha revelado a través de conexiones e interrelaciones a partir de dichos datos. Con todo, las empresas de publicidad pueden dirigirse a usuarios cuyos gustos y hábitos conocen minuciosamente de antemano.

Así las cosas, en orden a guiar estas campañas publicitarias, resulta habitual proceder a la elaboración de un perfil de personalidad con la información recopilada, perfil que puede realizarse tanto por los proveedores de redes sociales como los anunciantes[569]. En definitiva, los proveedores de redes sociales, así como los actores implicados en la personalización de publicidad, han implementado algoritmos basados en

[568] *Ídem.*
[569] En apartados posteriores analizaremos sus implicaciones jurídicas desde la perspectiva de la protección de la información personal.

IA en sus negocios en orden a extraer el máximo rendimiento la información concerniente a sus usuarios.

Antes bien, los usuarios no acostumbran a conocer que sus datos pueden destinarse a usos posteriores, entre los que se encuentra la reutilización lucrativa de dicha información[570]. En efecto, los usuarios no perciben este peligro específico al no tomar conciencia del tráfico de datos que se produce cuando manejan estas herramientas. Por otra parte, también advertimos una visible despreocupación por parte de estos, pues tienden a considerar que recibir publicidad no se identifica con una conducta que perjudique su privacidad; ahora bien, el usuario no advierte la trascendencia y extensión de la vigilancia ejercida por empresas como Google, así como la persistencia en el tiempo de ese control[571]. Es más, en un mundo singularmente digitalizado e interconectado, la multiplicidad de actividades que se realizan *online* son susceptibles de contribuir al enriquecimiento de una empresa privada que extraiga determinado rendimiento y valor económico a dichos datos. En este devenir, los proveedores de redes sociales contribuyen en gran medida a que los datos personales de los usuarios se desvelen sin su conocimiento a millones de empresas privadas con fines distintos a los consentidos.

Llegados a este punto, la evolución de la Web 2.0 a la Web 3.0 o web semántica se presenta como una herramienta esencial para la aceptación, adopción y funcionalidad de la publicidad de la empresa con el objetivo de fidelizar al usuario con las marcas que se presentan en la red[572]. Ello se debe a que, mientras que la gestión de la web 2.0 se lleva a cabo por el propio usuario humano, la web 3.0 se halla gestionada en la nube o *cloud computing* y ejecutada por cualquier dispositivo con un alto grado de viralidad y personalización. Así, la web semántica resulta plenamente capaz de conocer los gustos, modo de ser y comportarse de las personas, así como anticiparse a sus decisiones[573]. Con todo, mientras que la industria tecnológica alaba la capacidad que la web semántica posee

[570] En efecto, tal y como afirma SANTAMARÍA RAMOS, los usuarios suelen desconocer el valor que sus datos personales pueden alcanzar en el mercado. SANTAMARÍA RAMOS, J.F., "Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (Comentario al artículo 95 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.,* p. 4302

[571] LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.,* pp. 72-74.

[572] HERNÁNDEZ, A., Y KÜSTER, I., "Brand impact on purchasing intention. An approach in virtual social networks channels", *op. cit.,* p. 1 a 9.

[573] En ese sentido, mientras que una búsqueda de la palabra "perro" en un buscador basado en la web 2.0 mostraría todo tipo de perros, la misma búsqueda basada en parámetros de la web 3.0 mostraría al usuario los perros o razas de perros que le gustan, descartando los demás.

de personalizar en virtud de la información analizada en la web y redes sociales sobre las personas usuarias, no podemos sino mostrar nuestra inquietud sobre el impacto que las mismas producen sobre la privacidad de las personas.

Por otra parte, en este nuevo modelo de publicidad en el que la información suministrada por las redes sociales resulta una de las claves del funcionamiento del sistema de anuncios, estas plataformas han desarrollado mecanismos basados en la "personalización de la experiencia" para retener y enganchar al usuario para asegurar una mayor producción de datos enseñándole lo que le gusta o le atrae. Así, la red social garantiza su rentabilidad, pues las personas usuarias de su servicio generarán cada vez un rastro mayor para su posterior recopilación, cesión y análisis a empresas anunciantes. Este riesgo resulta mayor en menores de edad, dado que su falta de madurez les convierte en personas susceptibles de resultar víctimas de estas técnicas de enganche para una mayor producción de datos para su posterior cesión. Ha quedado evidenciado en apartados precedentes que los menores de edad pasan muchas horas conectados a las redes sociales sin resultar plenamente conscientes del transcurso del tiempo de sus conexiones.

Los propios proveedores de redes sociales han diseñado mecanismos que animan a los usuarios a permanecer activos en las plataformas. Así, tanto Instagram, como TikTok o Facebook entre otros, notifican novedades al usuario en sus dispositivos para el caso de que detecten una falta de actividad durante un lapso de tiempo. El fin de dicha notificación se halla en lograr que el usuario vuelva a acceder a la plataforma y así generar nuevamente datos para el proveedor de servicios a costa de desvelar su privacidad. De igual modo, estas aplicaciones implementan el sistema de *pull to refresh*, lo que se conoce como deslizar la pantalla a efectos de actualizarla y que el usuario continúe consumiendo el nuevo contenido emergente[574]. En efecto, los menores se entretienen, juegan, se comunican a través de estas plataformas; no obstante, su activa interacción resulta materia prima para los proveedores de redes sociales con motivo del uso que posteriormente proporcionan a estos datos de los menores: compartirlo con empresas anunciantes.

[574] El sistema *pull to refresh* se diseñó por la ingeniera Loren Brichter y consiste en deslizar hacia abajo la pantalla para esperar que se cargue nuevo contenido a visualizar por el usuario. Brichter, diseño este mecanismo para la conocida red social Twitter; sin embargo, otras redes sociales han terminado por incluirlo en sus servicios, como por ejemplo Instagram o Facebook. LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.,* p. 149.

2.3. *Big data* e inteligencia artificial: su impacto sobre los derechos fundamentales de personas en tránsito hacia su madurez

El empleo de la analítica de los macrodatos incide en el bienestar de los ciudadanos, ya que contribuyen mediante su uso a la mejora de la eficiencia de las empresas, a la distribución de los recursos públicos, a la mejora las condiciones laborales, a la lucha contra el fraude, etc.[575]. Además, el *big data* y la IA pueden conceder una ventaja competitiva en la toma de decisiones de las empresas gracias al mejor conocimiento de los niveles de desarrollo socioeconómico[576].

En el ámbito de la publicidad *online*, se ha podido constatar, que técnicas como las expuestas resultan de vital importancia para someter a análisis el volumen de datos que circulan en la red a fin de redirigir publicidad a las personas usuarias. Sin embargo, estas técnicas también conllevan riesgos significativos para los derechos y libertades de las personas, especialmente si se utilizan sobre los datos de menores de edad. De acuerdo con MORENTE PARRA, no se puede acometer un análisis exclusivamente técnico-económico del *big data*, pues ello obviaría el estudio de las consecuencias ético-jurídicas que dicho fenómeno conlleva[577]. De igual modo, consideramos necesario extender dicho razonamiento a técnicas de IA.

Así pues, los tratamientos de datos sometidos a parámetros del *big data* e IA, se centran en establecer patrones de conducta que no solo describen la realidad presente, sino que los cruces de datos disponibles para su análisis, arrojan la probabilidad de que una determinada persona adopte un comportamiento concreto en el futuro. Así, las compañías poseen la capacidad de anticiparse a las decisiones de sus clientes puede brindarles la posibilidad de influenciarlas.

---

[575] Efectivamente, incluso el tratamiento de datos de la población por medio de metodologías de tratamiento masivo como el *big data*, se ha constituido como un poderoso instrumento en la lucha contra el SARS-COV-2. GIL MEMBRADO, C., "Autonomía y tratamiento de datos personales de salud en tiempo de pandemia", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, Madrid, Dykinson, 2021, p. 154.

[576] Considerando H) de la Recomendación del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, Diario Oficial de la Unión Europea, C 263/10, de 25 de julio de 2018.

[577] MORENTE PARRA, V., "El Big Data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", *op. cit.*, p. 230.

Ahora bien, la técnica descrita presente riesgos para los derechos y libertades de las personas usuarias de la red y especialmente usuarias de redes sociales. Sobre este punto debemos subrayar, que el desmesurado rastro que las personas usuarias generan en la red, especialmente si estas no alcanzan la mayoría de edad, -pues pasan muchas horas navegando en redes sociales y en Internet, comparten ingentes volúmenes de datos en redes sociales o visualizan miles de vídeos para entretenerse- contribuye a facilitar a las compañías la predicción de su comportamiento futuro. Efectivamente, como las compañías han desarrollado un mecanismo capaz de conocer a las personas usuarias a través de la información que comparten y el comportamiento que adoptan en Internet y redes sociales, consecuentemente, también poseen la capacidad de anticiparse a sus decisiones o incluso llegar a influenciarlas[578].

El propio CEPD reconoce que las técnicas de análisis ajustadas a parámetros del *big data* potencian la posible manipulación de los usuarios, dado que, principalmente, las técnicas de análisis de macrodatos buscan influenciar el comportamiento y las elecciones de las personas[579]. En efecto, los proveedores de redes sociales construyen modelos que predicen las acciones y comportamientos de las personas, con el fin de incidir en las mismas. Sirva como ejemplo, que los datos compartidos en redes sociales, pueden llegar a revelar un determinado estado emocional del usuario; información que puede emplearse por los anunciantes con el fin de valorar cuándo el usuario se encuentra eventualmente más receptivo para cambiar su modo de pensar, y, por ende, su comportamiento. Según dispone COTINO HUESO, con el *big data* se puede inducir a un comportamiento como a quién votar, qué estudiar, dónde viajar o incluso qué comprar[580]. Por tanto, la práctica de estos métodos de análisis sobre información de usuarios menores de edad constituye una cuestión que debería preocupar considerablemente, ya que su falta de madurez ya les convierte en personas especialmente vulnerables, lo que, sin duda, convierte las técnicas como el *big data* e IA en un peligro todavía mayor para el desarrollo de los jóvenes.

[578] Sirva como ejemplo que, cuando los más jóvenes contestan a un test formulado por sus amistades en redes sociales, funcionalidad que ofrecen redes sociales como Instagram, dicha aportación a través de sus contestaciones proporciona un haz de informaciones adicionales sobre su modo de ser, a saber: el deseo de mejorar su autoestima mediante la formulación del cuestionario y obtención de las respectivas respuestas, sentirse especiales al acertar las respuestas etc. LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.,* p. 39.
[579] *Guidelines 8/2020 of European Data Protection Board on the targeting of social media users,* Version 2.0, adopted on 2 september 2020, p. 5.
[580] COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *op. cit.,* p. 141.

Otra cuestión controvertida derivada de la aplicación de estas técnicas al tratamiento de datos, se halla en la falta de objetividad en el acceso a la información que pueden ocasionar, limitando el acceso a las fuentes de información a los usuarios[581]. Esto es, los algoritmos empleados en el análisis de datos masivos, muestran a cada individuo la información que mejor se ajusta a sus intereses; consecuentemente, el algoritmo muestra a cada usuario informaciones diferentes. Como muestra de ello, Google o Facebook facilitan a unos usuarios un tipo de información y a otros, les facilita otra diferente en función de sus intereses. Incluso la introducción de una búsqueda concreta puede mostrar resultados diferentes dependiendo del perfil del usuario que la haya introducido. Efectivamente, la introducción de la búsqueda "cambio climático" arroja diversos resultados según la personalidad del solicitante de información: a algunas personas, les presenta dicho fenómeno como algo inútil, mientras que a otras les invita a concienciarse sobre ello.

Así las cosas, los menores crecen condicionados por un sistema que puede mostrarles la información de manera sesgada, resaltando algunas informaciones en detrimento de otras. La conducta descrita, genera una realidad diferente para cada uno de los menores usuario de redes sociales. Así, la red social distorsiona la realidad a la que cada menor de edad de su servicio tiene acceso[582], incidiendo esta conducta de manera especialmente negativa en su desarrollo personal, puesto que, de manera acertada manifiesta GARRIGA DOMINGUEZ que el uso de perfiles puede determinar la información a la que las personas van a poder acceder, limitando así su derecho a recibir información veraz (art. 20.1.d) CE)[583]. Consciente del importante riesgo que esta conducta implica, el Parlamento Europeo aboga por fomentar la libertad de los medios de información y el pluralismo, forzando a estas tecnologías a no limitar o discriminar el acceso a un entorno mediático pluralista[584]. Asimismo, La Carta de Derechos Digitales

[581] *Guidelines 8/2020 of European Data Protection Board on the targeting of social media users*, Version 2.0, adopted on 2 september 2020, p. 6.

[582] Para mayor profundización sobre el filtro burbuja véase PARISIER, E., *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos*, Madrid, Taurus, 2017, p. 18.

[583] GARRIGA DOMINGUEZ, A., "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea", *op. cit.*, p. 136. Así lo afirma también de manera más reciente en "Decisiones automatizadas basadas en algoritmos y protección de datos personales", en TOMÁS MALLEN, B., GARCÍA MAHAMUT, R., y PAUNER CHULVI, C., (Editores), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español*, *op. cit.*, p. 340.

[584] Considerando 13) de la Recomendación del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no

española reconoce el derecho a recibir libremente información veraz, para lo que obliga a los prestadores de servicios digitales a adoptar protocolos que garanticen a los usuarios su derecho a recibir información en tales condiciones[585].

En otro orden de consideraciones, los métodos de análisis de datos del *big data* e IA aumentan el riesgo de discriminación y exclusión de los colectivos más vulnerables de personas de la oferta de determinados productos o de determinadas informaciones. En efecto, el análisis de datos masivos puede discriminar directa o indirectamente a determinado grupo de personas que cumplan criterios específicos, por ejemplo, no mostrándoles determinadas ofertas de trabajo, ofertas crediticias sobre préstamos, etc. [586]. Baste como muestra, que los algoritmos se diseñan por seres humanos que, de manera voluntaria o involuntaria, pueden introducir en los sistemas que programan los prejuicios y estereotipos sobre determinados grupos sociales, de modo que, los algoritmos no se dedican más que reproducir y evidenciar en mayor entidad dicha discriminación[587]. Además, no se debe olvidar que los datos que nutren y entrenan al algoritmo, también pueden encontrarse sesgados.

En relación con el sesgo y discriminación que los algoritmos pueden causar, resulta destacable el informe de la Comisión francesa de protección de datos (CNIL), sobre los Algoritmos: prevenir la automatización de la discriminación, trabajo a través del cual la comisión francesa explica la discriminación a la que los algoritmos pueden

discriminación, seguridad y aplicación de la ley, Diario Oficial de la Unión Europea, C 263/10, de 25 de julio de 2018.

[585] Para su logro, los protocolos a adoptar por el responsble deberán, de manera transparente, informar al usuario sobres si se han elaborado sin intervención humana, si se han clasificado o priorizado por el proveedor mediante técnicas de perfilado o equivalentes o si poseen carácter publicitario. Carta de Derechos Digitales aprobada por el Gobierno de España. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022).

[586] Efectivamente, de acuerdo con ENISA, la información recabada por las redes sociales, además de para personalizar la experiencia en la plataforma, puede emplearse para discriminar (a través de los precios, estableciendo que determinados productos no se oferten a quien, de su información personal se deduzca que, no posee posibilidades económicas para consumirlos, etc.) EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, *Security Issues and Recommendations for Online Social Networks*, núm. 1, de octubre 2007 p. 9.

[587] En ese sentido, el Gobierno de los Estados Unidos emplea el sistema denominado COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions)* para la concesión o denegación de la libertad condicional. Dicho sistema, alimentado por una gran base de datos, infiere las posibilidades de reincidencia de los presos cuya libertad condicional se solicita. Sin embargo, el devenir de los años demostró que los presos de raza negra, siempre recibían una tasa de reincidencia superior a la que debería. Esto es, la reincidencia que ocurría en la práctica, siempre resultaba menor a la pronosticada por el programa. Por el contrario, los presos de raza blanca, recibían una tasa de reincidencia menor a la que les correspondía. Véase la Sentencia por la que se juzga el algoritmo que emplea el sistema COMPAS de la Corte Suprema de Wisconsin, de 13 de julio de 2016, *State of Wisconsin vs. Eric L. Loomis*, Caso núm. 2015AP157-CR.

conducir. Así, entre los diversos ejemplos prácticos de discriminación que visibiliza, destaca que es posible que un algoritmo programado para reclutar personal nuevo detecte que las mujeres ocupan determinados cargos, frecuentemente de menos responsabilidad y peor remunerados, reproduciendo estos sesgos e incluso acentuándolos[588]. Ciertamente, cabe la posibilidad de que el algoritmo llegue a inferir que no deben seleccionarse mujeres para dicho nuevo puesto al no reclutar históricamente mujeres para el mismo. En el caso de menores de edad, el algoritmo puede llegar a excluir a menores en función al centro educativo al que asisten o el lugar en el que radica su residencia. Queda en evidencia así, que estos sistemas pueden vulnerar el derecho fundamental a la igualdad consagrado en el art. 14 de la CE.

Más aún, los algoritmos poseen la capacidad de inferir informaciones de carácter sensible de aquellos datos proporcionados por los usuarios que no revisten tal condición. En efecto, las técnicas de análisis masivos de datos poseen la capacidad de inferir todo tipo de informaciones relativas al usuario, incluso aquellas que revelan datos de carácter sensible como la orientación religiosa, raza o etnia, entre otros[589], y tomar, consecuentemente, decisiones en base a ellas. Por ello, estas técnicas de tratamiento de datos ponen en riesgo los esfuerzos de la UE por articular la normativa en materia de protección de datos personales como protectora de la igualdad y la no discriminación a través de la prohibición de tratamiento de datos pertenecientes a categorías especiales (art. 9 RGPD). La razón nuclear de prohibir el tratamiento de datos pertenecientes a categorías especiales, reside en evitar la concurrencia de situaciones en las que se trate de manera diferente a un sujeto por su pertenencia a un determinado grupo en riesgo de exclusión[590]. Ahora bien, la inferencia de esta información sensible tras la aplicación del

[588] Informe la Comisión francesa de protección de datos (CNIL) sobre *Algorithmes: prévenir l´automatisation des discriminations*, 2020. Obtenido de: https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_algorithmes_access_0.pdf (última consulta el 1 de septiembre de 2022), p. 7

[589] Sobre este aspecto resulta ilustrativo el ejemplo proporcionado por el Grupo de Trabajo 29 cuando dispone que un estudio combinó los "me gusta" de Facebook con información limitada procedente de encuestas y halló que los investigadores predijeron con exactitud la orientación sexual de un usuario varón en el 88% de los casos; el origen étnico de un usuario en el 95% de los casos y; la ideología u orientación religiosa en el 82% de estos. Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 17.

[590] En esa línea, el Reglamento (UE), 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE de servicios digitales, Diario Oficial de la Unión Europea, L 277/1, de 27 de octubre de 2022, prevé prohibir en su art. 28.2 la presentación de anuncios basada en la elaboración de perfiles utilizando categorías especiales de datos personales.

algoritmo a información que no posee tal condición, se presenta como un nuevo riesgo del que proteger a estos colectivos vulnerables, dado que, estas técnicas pueden tomar decisiones basadas en dichos datos sobre raza, etnia, orientación política, etc., que han sido inferidos.

Por otra parte, la muestra de determinadas ofertas o publicidad a un grupo señalado de personas y no a otro, reduce considerablemente la libertad de elección que los individuos poseen en un mercado libre, así como la igualdad de oportunidades[591]. Véase que la inclusión de una persona en un concreto perfil al que se le atribuyen una suerte de comportamientos futuros, ocasiona que se le excluya de serle mostrada el resto de información que, sin embargo, será compartida con personas que cumplan los criterios para ello. De conformidad con el Grupo del Artículo 29, esta técnica puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren. Consecuentemente, además de socavar la libertad de las personas a la hora de elegir ciertos productos o determinados servicios tal y como señala el mencionado organismo[592], este comportamiento atenta contra el derecho a la libertad constitucionalmente reconocido en el art. 17 de la CE.

A mayor abundamiento, estos sistemas de toma de decisiones basados en grandes volúmenes de información tienden a adoptar decisiones sesgadas o incluso erróneas cuando deben decidir sobre cuestiones de realidad social. Véase que resulta complejo convertir en variables medibles todos aquellos aspectos de la realidad social relevantes en orden a adoptar una decisión, de modo que, las personas encargadas de la programación de los algoritmos, pueden obviar algunas variables, introduciendo sesgos al sistema. Consecuentemente, el resultado del cálculo puede arrojar decisiones parciales, no ajustadas plenamente a la realidad. Así, por ejemplo, tal y como ilustra SORIANO ARNANZ, es probable que concurra una correlación entre la compra de una freidora y

[591] En ese sentido, la plataforma de contenidos audiovisuales Netflix, no permite al usuario explorar el catálogo completo de sus contenidos, obligando a este a elegir entre las recomendaciones que la aplicación propone. Sin embargo, el usuario cree que, al tratarse de una plataforma bajo demanda, elige entre la serie o película que realmente desea visualizar. Nada más lejos de ello, el usuario no posee la completa libertad de elección, ya que solamente se le muestran una serie de contenidos "personalizados" bajo criterios que desconoce. Para la ampliación de la información véase CASTILLO, C., La oferta y la demanda del contenido audiovisual en la era de los datos masivos, 2018. Obtenido de: https://chato.cl/papers/castillo_2018_oferta_disponiblidad_contenido_audiovisual-ES.pdf (última consulta 12 de enero de 2022).

[592] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 6.

los malos hábitos alimenticios de la persona que la adquiere. Ahora bien, también puede ocurrir que la compra de dicha freidora se trate de un regalo, en cuyo caso, el algoritmo puede conducir a una errónea decisión al tildar a un futuro cliente de seguro médico como persona con hábitos no saludables y aumentar su prima[593].

En términos similares, resultan interesantes las aportaciones de LLANEZA GONZÁLEZ cuando afirma que los algoritmos toman decisiones por correlación en vez de por causalidad, lo que en la práctica se traduce en que pueden llegar a atribuir un mal resultado a individuos que, por ejemplo, adquieren productos en tiendas en las que los clientes que consumen habitualmente en ellas poseen malos resultados de solvencia económica. Sin embargo, la veracidad de dichos datos queda cuestionada considerablemente, pues nada prueba que dicha persona en particular sufra problemas de solvencia económica por el simple acto de consumir en dicho comercio. Al contrario, se discrimina a dichas personas por compartir algunos factores circunstanciales con personas no solventes[594]. Consciente de esta problemática, la UE se propone con acierto la transparencia de este tipo de publicidad, previendo imponer a las plataformas sociales el deber de explicar a los usuarios la razón o razones por las que han resultado excluidos de determinada publicidad (art. 27del Reglamento 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales).

Íntimamente ligado con las consideraciones expuestas, tal resulta el deseo de las compañías privadas de recabar, cada vez con mayor agresividad, un mayor volumen de datos personales para su posterior análisis predictivo, que han desarrollado técnicas basadas en la monitorización del comportamiento de los usuarios tanto en sus páginas web o plataformas, como fuera de ellas[595]. Todo ello, ha derivado en un constante control *online* que el usuario no siempre advierte, a pesar de que, ha llegado un momento en el que incluso los mensajes privados resultan susceptibles de emplearse con fines comerciales. Esta realidad se presenta a modo de preocupación, dado que, los mensajes privados como emails o mensajería instantánea, deberían quedar al amparo del art. 18.3

[593] SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *op. cit.*, p. 91.
[594] LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.*, p. 129.
[595] Política de privacidad de Instagram, https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse (última consulta el 21 de septiembre de 2022), p. 6.

CE que propugna la garantía del secreto de las comunicaciones[596]. Sin embargo, dicha salvaguarda no opera de modo eficaz en la circunstancia descrita, en el sentido que, se permite a operadores privados analizar su contenido con fines meramente económicos que bajo ningún concepto deberían suponer razón suficiente para ello[597].

Así las cosas, las redes sociales corren el riesgo de convertirse en herramientas muy eficaces para controlar a la población. Sobre este punto, resulta de interés, por su estrecha relación con el control al que se somete a los usuarios de redes sociales, recordar el panóptico de Betham, en el que el vigilante de la prisión, el manicomio, los hospitales, etc., puede observar cualquier rincón de dichas instituciones sin ser visto a cambio por las personas sometidas a control[598]. Ahora bien, si bien es cierto que la sociedad digital actual puede identificarse con una sociedad de control en la que prácticamente la totalidad de los comportamientos se analizan, la diferencia principal entre el panóptico de Bentham y el digital reside en que, mientras que en el primero el individuo es consciente de la presencia del vigilante, en el segundo, las personas se creen en libertad. De este modo, las propias personas desvelan su información personal y privada sin ser realmente conscientes del escrutinio al que dicha información se somete. Todo ello conduce a lo que BYUNG-CHUL identifica como una sociedad de transparencia[599].

No obstante, el verdadero problema reside en que, dicho control lo poseen empresas privadas como Google, Apple o Amazon, las cuales adoptan conductas monopolísticas en el mercado a causa de la circunstancia descrita. Más no se trata solo de

[596] Así, El TC manifiesta que el secreto de las comunicaciones también alcanza a aquellas que se efectúen a través del uso de la informática en su Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre de 2012, Boletín Oficial del Estado, de 22 de enero de 2013, núm. 19, en el contexto de la intervención empresarial de comunicaciones electrónicas de personas trabajadoras.

[597] En efecto, empresas como Google reconocen que analizan el contenido de los emails enviados y recibidos a través de la plataforma Gmail con fines publicitarios y de mercadotecnia. Concretamente, los desarrolladores de software analizan los contenidos de los correos electrónicos con la finalidad de conocer las prácticas de los usuarios. En consecuencia, los anuncios se pueden personalizar en virtud de las palabras empleadas en un correo electrónico. LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.*, pp. 97-98.

[598] BENTHAM, J., *The Panopticon Writings,* Editor Miran Bozovic, Londres, 1995. Sin embargo, la obra original data de 1791.

[599] BYUNG-CHUL, H., *La sociedad de la transparencia,* Barcelona, Herder, 2013, p. 90. De igual modo, LLANEZA GONZÁLEZ compara el control al que los proveedores TIC someten a los usuarios con la instalación en 1673 por el jesuita Atanasio Kircher de lo que este denominó "estatua citofónica", cuyo fin residía en espiar conversaciones cotidianas en la plaza y transmitirlas a la oligarquía italiana del siglo XVII. Este pionero sistema de escucha, se trató de un método temprano de extracción de información para las élites, ya que, las personas en la calle no poseían ninguna indicación de que sus conversaciones se canalizaban a aquellas personas que instrumentarían ese conocimiento en beneficio de su poder o riqueza. Por tanto, a nadie parecía preocuparle una estatua instalada en la plaza, pues no se percibía la misma como un instrumento de escucha, sino como un elemento decorativo. LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. op. cit.*, p. 53.

ello, de conformidad con SORIANO ARNANZ, estas compañías operan en espacios que forman parte esencial de la vida diaria de muchas personas, y como propietarias de dichas plataformas, toman decisiones que pueden poseer un impacto en las personas que interactúan con los algoritmos que diseñan[600]. Tanto es así que, las redes sociales ya han servido de herramienta para controlar y manipular a la población y socavar su derecho a la libertad consagrado en el art. 17 CE. Baste como muestra el escándalo denominado Cambridge Analityca en el que se vio envuelto Facebook en la campaña a las elecciones de Estados Unidos del año 2016 cuando la plataforma facilitó más de 50 millones de perfiles a la empresa Cambridge Analityca con el objetivo de influenciar el comportamiento de los votantes estadounidenses[601]. Por lo tanto, compartimos las palabras de PÉREZ LUÑO cuando afirma que nos encontramos ante el riesgo de que se produzca el más implacable fenómeno de control y manipulación que pueda imaginarse[602].

En definitiva, el modo de funcionar y tratar los datos personales de estas plataformas no ha tomado en consideración a los menores en su diseño[603]. Ha quedado claro, que los riesgos a los que la población se enfrenta revisten gravedad como consecuencia del uso que estas compañías realizan con los datos personales de los usuarios. En esta realidad, millones de usuarios menores de edad cuya personalidad se

---

[600] SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *op. cit.*, p. 99.

[601] La empresa británica Cambridge Analityca recolectó más de 50 millones de perfiles de usuarios de Facebook a través de un test de personalidad insertado por esta empresa en la plataforma y que los usuarios de esta contestaban. Al proceder a la cumplimentación de dicho cuestionario, los usuarios autorizaban a Cambridge Analityca el acceso a sus datos del perfil, así como al de las amistades de estos. Con esta información, la empresa británica creaba el perfil de cada votante por medio de algoritmos diseñados por científicos de los datos. La finalidad de dicha recolecta y tratamiento, residía en influenciar y cambiar de forma invisible e imperceptible para el usuario de Facebook, el voto en las elecciones presidenciales de 2016 de EEUU en las que resultó victorioso Donald Trump. De este modo, se pudo influenciar y cambiar el voto de millones de personas no a través de técnicas de persuasión, sino por medio del dominio informativo. La empresa conocía de antemano a qué tipo de mensajes resultaría susceptible cada usuario, la forma de entregarlo para su mayor efecto, los temas que podrían provocar dicho cambio de orientación, el contenido y el tono del mensaje para resultar más efectivo, etc. Para mayor información, véase el siguiente enlace: https://www.xataka.com/privacidad/el-escandalo-de-cambridge-analytica-resume-todo-lo-que-esta-terriblemente-mal-con-facebook (última consulta el 28 de octubre de 2021).

[602] PEREZ LUÑO, A.E., "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", *Anuario de Derechos Humanos*, 1986-1987, núm. 4, p. 269.

[603] De modo similar se manifiesta el Comité de Derechos del Niño en la Observación general núm. 25, de 2 de marzo de 2021, en su apartado 12 cuando afirma que el entorno digital no se diseñó, en principio, para los niños. Obtenido de: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12 (última consulta el 2 de febrero de 2023)

encuentra en pleno desarrollo y formación se enfrentan a una herramienta que puede condicionar por completo su tránsito a la madurez[604]. El propio CEPD advierte que el *big data* puede afectar a la formación de las preferencias e intereses de los menores, incidiendo estos comportamientos de manera especialmente lesiva sobre su autonomía y desarrollo[605].

De conformidad con lo expuesto, los algoritmos y la elaboración de perfiles sobre datos cuya titularidad recae en los menores de edad, pueden conducir a las futuras generaciones a asimilar conductas irreversibles como: no acceder a una información veraz y plural, crecer en un ambiente de manipulación digital que les impida formar su personalidad de manera libre o, en definitiva, no poseer una igualdad de oportunidades para forjar su futuro[606].

3. RESPUESTA NORMATIVA A LAS TÉCNICAS DE ANÁLISIS MASIVO DE DATOS EN EL MARCO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Muchos de los potenciales riesgos causados por el empleo de algoritmos se generan como consecuencia directa de la recogida y procesamiento a gran escala de datos personales. Por tanto, este se constituye como un tratamiento de datos personales al que deberá aplicarse la normativa sobre protección de datos personales.

Así, el Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, ya mostraba su preocupación en el año 1999 por todos los tipos de operaciones de tratamiento informático que se llevaran a cabo en Internet a través de software y hardware sin conocimiento del interesado, y por

---

[604] En efecto, de conformidad con RALLO LOMBARTE el uso abusivo de la tecnología por los menores tiende a modificar sus pautas de comportamiento personal y su modelo de relacionarse personalmente, lo que dificulta un adecuado modelo de desarrollo de su personalidad. RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales, op. cit.*, p. 34.

[605] *Guidelines 8/2020 of European Data Protection Board on the targeting of social media users*, Version 2.0, adopted on 2 september 2020, p. 7.

[606] Así, destaca con acierto el Comité de Derechos del Niño que, […] los sistemas automatizados o los sistemas de filtrado de información no se utilicen para afectar o influenciar el comportamiento o las emociones de los niños ni para limitar sus oportunidades y desarrollo. Observación general número 25, del Comité de los derechos del niño, de 2 de marzo de 2021, relativa a los derechos de los niños en relación con el entorno digital. Obtenido de: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12 (última consulta el 2 de febrero de 2023).

consiguiente, de manera invisible para el mismo[607]. Sin embargo, si bien podemos considerar el art. 15 de la Directiva 95/46/CE como el precedente en la regulación de fenómenos como las decisiones automatizadas y elaboración de perfiles, no ha sido hasta varias décadas después, cuando por medio de la entrada en vigor RGPD el ordenamiento jurídico europeo ha consolidado en su articulado normativa dirigida a fenómenos como el *big data* y la IA.

A pesar de ello, si bien el RGPD no ha pasado por alto el tratamiento de datos masivo, el rápido desarrollo de las técnicas de tratamiento basadas en este fenómeno, dificultan de manera notoria la posibilidad de las personas interesadas de ejercer un control eficaz sobre sus datos personales. En ese sentido, la complejidad de los procesos de tratamiento de datos personales, la opacidad de las herramientas empleadas para ello, el análisis inferido de datos, entre otros, parecen colisionar con los pilares sobre los que se asienta el tradicional derecho a la protección de los datos personales.

3.1. La cuestionada eficacia del consentimiento del interesado como condición de licitud para el tratamiento de datos personales mediante tecnologías *big data* e inteligencia artificial

De la lectura del RGPD se puede constatar que el legislador europeo introduce una serie de previsiones, que si bien su adopción no responde directamente a proporcionar una regulación al *big data* e IA, resultan de aplicación a las mismas[608]. Como se verá, muchas de los preceptos del RGPD, presentan una manifiesta incompatibilidad con este nuevo fenómeno de análisis de grandes volúmenes de datos personales que los proveedores de redes sociales y anunciantes practican[609].

---

[607] Recomendación 1/1999 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware aprobado por el Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, de 23 de febrero de 1999, DG XV C 5093/98/final WP 17.

[608] Efectivamente, la Directiva 95/46/CE, acogía principios, normas y garantías que como identifica HERRÁN ORTIZ se fundamentaban sobre el concepto de tratamiento de datos estático y no dinámico ni en conexión. Esto es, los ficheros se consideraban estancos y reservados. "Datos personales de salud, investigación científica, y tecnología *big data*. De la necesidad de un marco normativo propio en la UE", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, Madrid, Dykinson, 2021, p. 207. Ahora bien, debemos añadir que, el RGPD toma conciencia de los nuevos paradigmas en el tratamiento de datos que el *big data* y la IA ofrecen.

[609] ARMADA VILLAVERDE, M.E., Y LÓPEZ BUSTABAD, I.J., "El Reglamento General de Protección de Datos ante el fenómeno del "Big Data", *op. cit.*, p. 2.

Así, la base jurídica del consentimiento (art. 6.1.a) RGPD) que tradicionalmente se considera piedra angular en la concesión al interesado de un control efectivo sobre sus datos personales, no parece garantía suficiente cuando se refiere a consentir el tratamiento para la personalización de la experiencia del usuario en una red social. Ello se debe a que, aunque el consentimiento fuera recabado, la complejidad de los tratamientos que el *big data* e IA permiten, colisionan frontalmente con las tradicionales premisas del consentimiento del interesado, como quedará de manifiesto.

A este respecto, la prestación del consentimiento libre, expreso e informado se posiciona como una de las vías principales que la legislación emplea en orden a proporcionar a todo individuo un control razonable sobre los datos que le conciernen; sin embargo, esta autonomía en la gestión de los datos personales no ha de entenderse como sinónimo de un sistema efectivo de protección por defecto. Tal y como señalan OLIVER-LALANA y MUÑOZ SORO, poseer el control sobre la información personal en un mundo basado en el almacenamiento y cruce de datos, resulta imposible. Este contexto, presenta graves impedimentos para que los individuos puedan controlar sus datos en un entorno globalizado donde las técnicas de intercambio, perfilado y minería de dados resultan cada vez más sofisticadas e invisibles[610].

Efectivamente, las personas usuarias de redes sociales, no toman conciencia de que el registro en la plataforma de su elección, autoriza a la red social al rastreo de todas sus acciones con el fin de incidir en la toma de sus decisiones. Incluso aunque no concurra un registro, como veremos posteriormente, dicho rastreo deviene posible. Más aún, queda comprobado que esta nueva tecnología propicia una vigilancia integral, así como una reconstrucción de todas las facetas de la vida de una persona sin que esta advierta dicha circunstancia. En consecuencia, los menores de edad, como sujetos especialmente vulnerables, crecen en un entorno que somete a control sus acciones hasta límites insospechados sin que perciban dicho comportamiento.

En tales circunstancias, fundamentar el control de la información sobre el consentimiento como informado y válidamente emitido resulta complejo. Las personas

[610] OLIVER-LALANA, D., Y MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J., (Coordinador), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Cizur Menor, Aranzadi, 2013, p. 163. Comparte dicha opinión MORENTE PARRA cuando afirma que, con la llegada del *big data*, la obtención del consentimiento tal y como se ha conocido hasta la fecha se torna imposible. MORENTE PARRA "El Big Data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", *op. cit.*, p. 248.

usuarias, más si son menores de edad, no pueden ejercer un control sobre sus datos personales ante unos riesgos que no conocen o de los que no se les informa con claridad. Así, los proveedores de redes sociales deben asumir que aunque los usuarios muestren sus preferencias, gustos o acciones en su plataforma, ello no legitima que sin un consentimiento válido, puedan utilizar dicha información con fines publicitarios[611].

Puede pensarse que la clave de potenciar dicho control sobre la información personal se halla en proporcionar al usuario la información necesaria para que éste emita un consentimiento informado. Ahora bien, en el entorno de la IA, la elaboración de perfiles y la toma de decisiones automatizadas, resulta imprescindible que dicha información incluya la lógica aplicada de los tratamientos que estas empresas realizan sobre datos de las personas usuarias a efectos de cumplir el principio de transparencia (art. 5.1.a RGPD). Sin embargo, las políticas de privacidad de redes sociales no facilitan dicha información. Tal y como proponen ARMADA VILLAVERDE y LÓPEZ BUSTABAD, las políticas de privacidad deberían exponer la lógica empleada en los algoritmos que se utilizan para determinar las predicciones y correlaciones derivadas de esos datos, dado que, la opacidad de los métodos de análisis y reutilización de la información, dificultan considerablemente la comprensión del usuario sobre los tratamientos practicados sobre sus datos[612].

En relación con lo expuesto, el Tribunal distrito de La Haya (*Rechtbank Den Haag*), ha dictado el 5 de febrero de 2020 la primera sentencia conocida en Europa que declara ilegal un algoritmo empleado por el Gobierno de los Países Bajos para evaluar el riesgo de fraude a la Seguridad Social o a Hacienda por parte de los ciudadanos[613]. Principalmente, el tribunal neerlandés declara la falta de transparencia del algoritmo,

[611] GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.,* p. 129.

[612] ARMADA VILLAVERDE, M.E., Y LÓPEZ BUSTABAD, I.J., "El Reglamento General de Protección de Datos ante el fenómeno del "Big Data", *op. cit.,* pp. 10-11.

[613] Véase Sentencia del Tribunal del distrito de La Haya, de 5 de febrero de 2020, *Rechtbank Den Haag*/ (*Sentencia SyRI*), C-09-550982-HA ZA 18-388. En el pronunciamiento señalado, el Gobierno neerlandés emplea un instrumento legal denominado Sistema de Indicación de Riesgos (SyRI) para prevenir y combatir el fraude en el campo de la Seguridad Social y los esquemas relacionados con los ingresos, las contribuciones fiscales y de las leyes laborales. Este sistema, se basa en la asignación de un nivel de riesgo a que una determinada persona cometa fraude a los ingresos públicos, en función de una serie de parámetros analizados y relacionados entre sí. Para dicho cometido, el sistema se vale de un algoritmo que procesa una gran cantidad de datos de los ciudadanos tales como, nombre, residencia, fecha de nacimiento, datos fiscales, datos comerciales, historial de cumplimiento de las leyes y reglamentos, becas recibidas, subsidios recibidos, nivel de endeudamiento, etc. El fin último, reside en asignar un nivel de riesgo de cometer fraude a cada una de las personas analizadas por el sistema.

dado que, el gobierno holandés no ha publicado el tipo de algoritmo empleado en el modelo de riesgo, ni proporcionado información sobre el método de análisis de riesgos aplicado. Además, continúa el tribunal disponiendo que la normativa reguladora del algoritmo no prevé ninguna obligación de informar a las personas cuyos datos se tratan, de modo que, no cabe esperar que éstas conozcan que sus datos se emplean para la finalidad perseguida por el Gobierno de Países Bajos en la detección del fraude fiscal. Por último, sienta el órgano jurisdiccional, que tampoco resulta posible verificar cómo se ha procedido al diseño del árbol de decisión que emplea el algoritmo, por lo que la persona afectada difícilmente puede defenderse contra la elaboración del informe de riesgo, pues se desconoce el modo de su elaboración.

De todos modos, esta información sobre la lógica aplicada puede alcanzar una complejidad técnica muy avanzada, en la que incluso sus desarrolladores prevén una manifiesta dificultad en especificar los detalles de dichos tratamientos. En consecuencia, la falta de transparencia de los sistemas algorítmicos, dificulta e incluso imposibilita el control general de la legalidad de los programas empleados en la toma de decisiones automatizadas[614]. Así, la falta de transparencia, tanto en la ausencia de advertencia al usuario de la práctica de esta toma de decisiones, como en el modo en el que estas se adoptan a través de algoritmos, conduce a una imposibilidad por parte del usuario de protegerse de estas a través del consentimiento informado.

Sin embargo, esta dificultad no debe traducirse en una absoluta opacidad a la hora de informar sobre la práctica de estos tratamientos ni servir de excusa para no satisfacer dicha información al interesado. En caso de que el responsable del tratamiento advierta una imposibilidad manifiesta en orden a explicar la lógica aplicada de los algoritmos empleados para los fines previstos, deberá abstenerse de dicho tratamiento.

Aunque estos nuevos tratamientos de datos practicados por proveedores de redes sociales basados en parámetros del *big data* e IA, informaran sobre dicha lógica aplicada, aparecen nuevos escollos a efectos de considerar el consentimiento como garantía de control de la información personal. Al hilo de lo expuesto por COTINO HUESO, consentir informadamente sobre unas finalidades de uso de datos que no se conocen ni sospechan siquiera, o en su defecto, no se comprenden, conducen a un consentimiento

[614] SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *op. cit.*, p. 94.

simbolista[615]. Más no se trata tan solo de ello, esta nueva tecnología, alberga la posibilidad de transformar la información generando nuevos datos personales de los datos primitivos, lo que dificulta notoriamente que las empresas especifiquen en sus políticas de datos las futuras finalidades de uso de esos datos. Sobre estos nuevos datos inferidos, los responsables del tratamiento deberían recabar un nuevo consentimiento si los mismos se emplean para fines distintos a los inicialmente consentidos. Ahora bien, para salvar dicho obstáculo, justifican su tratamiento mediante el principio del interés legítimo, sin que ello resulte correcto, tal y como veremos posteriormente.

Por si ello no fuera suficiente, de conformidad con ARMADA VILLAVERDE y LOPEZ BUSTABAD muchas empresas-entre las que se encuentran los proveedores de redes sociales- supeditan el consentimiento al tratamiento de datos personales para finalidades que no guardan relación con la prestación de sus servicios[616]. En efecto, sirva como ejemplo, que las redes sociales acostumbran a combinar información de terceros con la de su plataforma para fines distintos a los iniciales sin consentimiento del usuario[617]. Efectivamente, los proveedores de redes sociales reutilizan información y la emplean para fines distintos de los consentidos inicialmente sin recabar nuevamente el consentimiento del interesado para estas nuevas finalidades. Ciertamente, el *big data* recopila informaciones de fuentes y orígenes diversos, de modo que, a priori, no cabe la posibilidad de informar al interesado sobre cuestiones que los propios responsables del tratamiento desconocen en ese momento.

En definitiva, estas manifestaciones nos conducen a afirmar que el *big data* e IA también inciden sobre el principio de la limitación de la finalidad (art. 5.1.b) RGPD), en el sentido que, el uso transformativo de la información personal, conduce a la prestación de un consentimiento sobre el que no se ofrece una relación detallada y específica de las potenciales finalidades para los que los datos se tratarán en un futuro[618].

---

615 COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *op. cit.,* p. 145.

616 ARMADA VILLAVERDE, M.E., Y LÓPEZ BUSTABAD, I.J., "El Reglamento General de Protección de Datos ante el fenómeno del "Big Data", *op. cit.,* p. 9.

617 *Guidelines 8/2020 of European Data Protection Board on the targeting of social media users*, Version 2.0, adopted on 2 september 2020, p. 7.

618 Véase que las finalidades del principio de limitación de la finalidad pueden considerarse dos: por una parte, los datos personales deben recogerse para las finalidades determinadas, explícitas y legítimas previstas; por otra parte, los datos personales no se tratarán posteriormente de manera incompatible con los fines señalados. TRONCOSO REIGADA, A., "Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)", *op. cit.,* p. 859.

Consecuentemente, los tratamientos futuros de dicha información, no poseen acomodo en ninguna base legal exigida por el RGPD. De conformidad con GIL GONZÁLEZ, estas técnicas, se apoyan en la reutilización datos que se obtuvieron para una primera finalidad, otorgándole otra nueva[619]. A lo que debemos añadir que sin un consentimiento nuevo recabado. Conscientes de dicha circunstancia, los proveedores de redes sociales emplean cláusulas vagas e imprecisas cuyo fin reside en mantener abierta la puerta a dichos futuros tratamientos de datos personales[620].

El riesgo que los tratamientos de datos masivos generan sobre información de usuarios se agrava considerablemente cuando los menores manejan redes sociales. Véase que, en primera instancia, los proveedores de redes sociales no informan con claridad sobre la práctica de estos tratamientos de datos sobre la información de los usuarios. A lo que se debe agregar, que la creciente sofisticación de los tratamientos y la proliferación de decisiones automatizadas, dificultan que una persona pueda conocer el verdadero destino de su información, más aún, si esta es menor. De modo que, en el caso de este colectivo, el consentimiento en ningún caso asegura el control de la información personal.

Por otra parte, las personas reacias a otorgar un consentimiento, pueden sufrir una exclusión de un amplio abanico de servicios de la sociedad de la información. Así, por ejemplo, la negativa a la prestación del consentimiento en el ámbito de redes sociales, puede generar aislamiento en el menor de edad o incluso problemas para integrarse en la sociedad ante la expansión en el uso de estas plataformas. Ello nos permite plantear, si jurídicamente el consentimiento prestado por el menor se configura como un consentimiento que goza de la libertad exigida por la normativa sobre protección de datos personales (Considerando 32 RGPD). El generalizado uso de estos servicios entre los más jóvenes, propugna una mayor sensación de inevitabilidad de la pérdida de privacidad, dado que, al crecer inmiscuidos en este nuevo mundo, han acabado por interiorizar y normalizar conductas contrarias a su privacidad.

Definitivamente, las condiciones y garantías actuales en las que el consentimiento se desenvuelve, no otorgan al menor el control de los datos personales cuando sus datos

[619] GIL GONZÁLEZ, E., "Big Data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?", *op. cit.*, p. 2.
[620] Sirva como ejemplo de vaguedad la siguiente cláusula obtenida de la Política de privacidad de Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse (última consulta el 22 de octubre de 2021), p. 17. "Usamos la información que recogemos para ofrecerte una experiencia personalizada, incluidos anuncios, además de los otros fines que se detallan más adelante".

se someten a análisis masivos basados en parámetros de *big data* e IA. La falta de transparencia en las políticas de privacidad encaminadas a informar al usuario en las que no informan con claridad de la práctica de este tipo de tratamientos, la imposibilidad de establecer las finalidades de tratamiento por parte de los proveedores, la posibilidad de generar nuevos datos inferidos de la información compartida primitivamente para la consecución de finalidades diferentes a las consentidas, se consideran algunas de las circunstancias que influyen decisivamente en la dificultad de establecer garantías sobre el tratamiento masivo de datos personales.

En definitiva, los pilares legales tradicionales sobre los que se sustenta la protección de datos personales resultan ineficaces en este nuevo escenario de tratamiento de datos personales proporcionado por las técnicas derivadas del *big data* e IA. Gran parte de los principios consagrados en la normativa sobre protección de datos personales resultan sistémicamente vulnerados por aquellos responsables del tratamiento que las practican.

3.2. De la recopilación a gran escala de datos personales del menor internauta y las tensiones que esta genera con el principio de minimización de los datos

El art. 5.1.c) del RGPD dispone que los datos personales tratados habrán de resultar adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se someten a tratamiento, esto es, nos referimos a lo que el texto europeo califica como "minimización de los datos". En esencia, consiste en que los datos sometidos a tratamiento resulten adecuados, pertinentes y no excesivos. Este principio, llevado a términos prácticos se fundamenta en la minimización de datos a lo largo de todas las etapas del tratamiento: recogida, uso, conservación y difusión según dispone la AEPD[621]. En concreto, el principio de minimización de los datos se proyecta sobre dos dimensiones del tratamiento de datos: por un lado, sobre la extensión y categorías de datos a recopilar en orden a evitar una recopilación indiscriminada de datos; por otro lado, sobre el plazo de conservación de estos datos, cuestión sobre la que incidiremos en el capítulo siguiente del presente estudio.

[621] Guía de privacidad desde el diseño de la AEPD, de octubre de 2019. Obtenido de https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf , p. 8.

Así las cosas, la lectura de dicho principio conduce a reflexionar sobre si los proveedores de redes sociales tratan una cantidad de datos proporcionada y acorde al servicio que prestan o si, por el contrario, recopilan un volumen ingente de información desproporcionada en relación a los fines del tratamiento alegados. Nos preguntamos así, sobre la adecuación de este sistema de recogida y análisis masivo de información al principio de minimización de los datos.

Sin embargo, de manera previa a valorar dicha adecuación, creemos conveniente ilustrar toda aquella información que las redes sociales más empleadas por los menores recopilan. Así, Instagram y Facebook dividen en tres grupos la información que tratan[622]:

En primer lugar, recopilan información sobre las conductas del usuario en su plataforma, como el contenido que este comparte, las comunicaciones que el usuario envía, así como la fecha de creación de un archivo, el lugar en el que se ha tomado una determinada fotografía, el contenido de los mensajes enviados por chat, e incluso el contenido que el usuario visualiza a través de la cámara. En esta misma categoría, recopila información sobre las personas, páginas, cuentas, *hashtags*, personas y grupos con los que más interactúa el usuario. Asimismo, Instagram y Facebook monitorizan el uso que las personas usuarias realizan en su plataforma. Así, recopilan información sobre el modo en el que las personas emplean sus redes sociales, los tipos de contenidos que estas visualizan, las funciones que más emplean, las acciones llevadas a cabo, personas o cuentas con las que interactúa el usuario, hora, frecuencia y duración de las actividades, como, por ejemplo, registrar cuándo el usuario utiliza la red social, cuándo la utilizó por última vez y todo tipo de contenido visualizado por este. Continúa la política de privacidad afirmando que, tratan la información sobre las transacciones que se efectúan en la plataforma como las compras efectuadas en juegos o donaciones. Por último, en este grupo de datos, también recaban información sobre la actividad de otros usuarios y la información que proporcionan sobre otros usuarios como, por ejemplo, fotografías o comentarios que otros usuarios realizan sobre la persona usuaria[623].

[622] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse , (última consulta el 21 de septiembre de 2022).
[623] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse , apartado ¿Qué información recogemos?, (última consulta el 21 de septiembre de 2022), pp. 3-4.

En segundo lugar, las mencionadas plataformas recopilan todo tipo de información sobre el dispositivo a través del cual el usuario accede a la red social. En efecto, recaban información sobre los móviles, televisiones *online*, ordenadores, etc., a través de los que los usuarios acceden a sus plataformas. Concretamente, recaban las características del dispositivo tales como, la información sobre el sistema operativo, la versión de *hardware* y *software*, el nivel de carga de la batería, la potencia de la señal, el espacio de almacenamiento disponible, el tipo de navegador, los tipos y nombres de aplicaciones o archivos, y los *plugins*. Continúa la política de privacidad estableciendo que, recopilan las operaciones realizadas con el terminal como operaciones y los comportamientos realizados en el dispositivo, como poner una ventana en primer o segundo plano o los movimientos del ratón. Además, también recopilan las señales del dispositivo como, por ejemplo, señales de Bluetooth e información sobre balizas, torres de telefonía móvil y puntos de acceso a redes wifi cercanos. Por si la información enumerada no fuera suficiente, también compilan información sobre la red y conexiones empleadas como: el nombre del operador de telefonía móvil o proveedor de Internet, el idioma, la zona horaria, el número de teléfono móvil, la dirección IP, la velocidad de la conexión y, en algunos casos, información sobre otros dispositivos que se encuentran cerca o están en la red del dispositivo[624].

Por último, también tratan la información que sus socios poseen sobre las personas usuarias. Ciertamente, la política de privacidad del Grupo Meta establece que estos socios proporcionan información sobre las actividades que el usuario realiza fuera de la plataforma, incluidos datos sobre el dispositivo que utilizas, los sitios web que visita, las compras que efectúa, los anuncios que visualiza y la manera en que emplea sus servicios, tanto si este posee una cuenta de Facebook se ha iniciado sesión en ella, como en caso contrario[625].

Por otra parte, redes sociales cuya popularidad está en auge desde 2020 entre la juventud como TikTok, también recopilan un volumen considerable de información[626].

---

[624] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse , apartado ¿Qué información recogemos?, (última consulta el 21 de septiembre de 2022) , pp-5-6.

[625] Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#2-HowDoWeUse, apartado ¿Qué información recogemos? (última consulta el 21 de septiembre de 2022), pp. 6-7.

[626] Tal y como dispone el "Informe anual sobre Aplicaciones y menores: un año atrapados detrás de las pantallas", *Qustodio*, Año 2020. Obtenido de https://qweb.cdn.prismic.io/qweb/10de139a-cb1c-488e-

Así las cosas, recaban datos sobre el perfil del usuario, el comportamiento que este lleva a cabo en la plataforma como el uso que este hace de la red social, incluida la frecuencia con la que utiliza la plataforma y cómo interactúa con el contenido que se le muestra, los anuncios que ve, los vídeos que visiona, los problemas que detenta, el contenido que le gusta, el contenido que guarda en favoritos, las palabras que busca y los usuarios a los que sigue. Así mismo, también trata la información sobre los seguidores del usuario, los «me gusta» que recibe y las respuestas al contenido que el usuario comparte.

Al igual que Instagram y Facebook, TikTok también recaba los mensajes que el usuario envía y recibe además de recopilar información de terceros que la persona usuaria comparte. En ese sentido, sus socios comerciales entre los que se encuentran, tanto Facebook como Instagram, pueden compartir con la plataforma información recabada por estos. Idéntico comportamiento pueden llevar a cabo los anunciantes y proveedores de medición de TikTok. Al igual que en el caso de Instagram y Facebook, TikTok recaba todo tipo de información sobre el terminal utilizado para acceder a la plataforma, ajustes, conexiones, etc., por último, también compilan la información sobre las compras efectuadas en la plataforma[627].

Queda demostrado así, que algunas de las redes sociales más habituales entre los más jóvenes, compendian y tratan información a gran escala sobre las personas usuarias[628]. Antes bien, no debe preocupar exclusivamente que los tratamientos de datos de *big data* e IA se realicen sobre elevados volúmenes de datos, sino que, además, este fenómeno, combina información de múltiples fuentes y busca la inferencia y creación de nuevos datos en base a los datos primitivos recabados. Por ello, a nuestro juicio, esta conducta puede impactar con este principio, dado que, la técnica sirve a la creación de nuevas informaciones personales.

---

b0e9-f5becb01f32f_Informe+anual+de+Qustodio+2020+Informe+sobre+los+h%C3%A1bitos+digitales+de+los+menores_ES.pdf (última consulta el 4 de mayo de 2021) los meses de marzo y abril de 2020 coronaron a TikTok como el rey de las rede sociales con el mayor porcentaje de menores usándolo en España, Reino Unido y EE.UU.

627 Para mayor información, véase la política de privacidad de TikTok en el siguiente enlace: https://www.tiktok.com/legal/privacy-policy?lang=es#pp-eea (última consulta 27 de abril de 2021)

628 Resulta sorprendente que, sin embargo, el Grupo Meta afirme en su política de privacidad que se proponen crear experiencias personalizadas que aporten valor sin comprometer la privacidad de los usuarios. Véase la Política de privacidad obtenida de la página de registro de la red social Instagram: https://mbasic.facebook.com/privacy/policy/printable/#18.4-LegitimateInterestsWeRely , apartado sobre ¿Cómo usamos tu información (última fecha de consulta el 21 de septiembre de 2022).

Antes bien, recabar muchos datos no se considera sinónimo de incumplir el principio de minimización de los datos automáticamente. Efectivamente, el RGPD apunta que el responsable debe, por defecto, tratar únicamente los datos estrictamente necesarios para cumplir el fin lícito establecido. Así las cosas, se debe valorar que las redes sociales han sufrido una metamorfosis en su cometido principal desde su irrupción inicial en el año 2008. Mientras que anteriormente sí que destinaban sus herramientas a proporcionar al usuario un entorno virtual en el que chatear, comentar y subir fotografías, en la actualidad su principal servicio no se corresponde con el descrito a pesar de mantener ciertas connotaciones de dicha actividad.

Efectivamente, las redes sociales han centrado su servicio en "personalizar la experiencia" al usuario, lo que se configura como una actividad que solamente podrá funcionar ante la combinación masiva de datos personales recabados de diversas fuentes a saber: la información proporcionada por el usuario de modo activo, aquella recabada de modo pasivo de su comportamiento, así como los datos de diversas fuentes que estos algoritmos poseen la capacidad de recopilar. A nuestro juicio, resulta cuestionable, que mientras que el cumplimiento del principio de minimización de los datos exige una recogida limitada de los datos acorde al fin lícito establecido, uno de estos fines requiera de una recogida masiva de datos personales.

En ese sentido, el considerando 39 RGPD dispone que los datos personales deben ser adecuados, pertinentes y limitados "a lo necesario" para los fines para los que sean tratados. Así las cosas, no resulta suficiente que el tratamiento se considere lícito, leal, transparente y para unas finalidades determinadas, explícitas y legítimas, sino que, además, habrán de resultar los datos personales objeto de tratamiento, adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que se tratan. Efectivamente, debe concurrir una adecuación entre los datos recabados y la finalidad de tratamiento declarada. Por ello, se debe someter a análisis la finalidad o finalidades declaradas, pues ésta o éstas determinarán la pertinencia o no sobre el volumen de datos recopilados. Véase que puede ocurrir que la recopilación de determinados datos personales supere el juicio de adecuación para una finalidad, mientras que no para otras.

En esta labor, resultan de verdadero interés las aportaciones de TRONCOSO REIGADA cuando afirma que, los parámetros tradicionales del principio de proporcionalidad pueden alumbrar en qué situaciones los datos pueden recibir el

calificativo de excesivos. Precisamente, habrán de ponderarse los bienes y derechos constitucionales en conflicto, para determinar si la injerencia en el derecho a la protección de datos personales resulta equilibrada por derivarse más beneficios de su práctica para el interés general que perjuicios para el derecho a la protección de datos personales. En esencia, se trata de determinar si la intromisión se justifica en aras de lograr un bien mayor[629].

A nuestro juicio, la recogida masiva de datos personales con fines de personalización y mercadotecnia directa en redes sociales no supera el juicio de proporcionalidad. Por cuanto que, los beneficios a alcanzar no sirven al interés general, más bien todo lo contrario, responden a intereses particulares de un número limitado de grandes compañías. En definitiva, cabe cuestionarse la adecuación, pertinencia y "limitación a lo necesario" de la recogida masiva de datos con los fines descritos[630].

Este comportamiento, a su vez, puede generar fricciones con el principio de exactitud de los datos instaurado por el art. 5.1. letra d) RGPD, dado que la exactitud de estos nuevos datos dependerá en gran medida de la calidad de los datos subyacentes empleados para la elaboración del perfil. Esto es, el empleo de datos inexactos en la elaboración del perfil o en el proceso de decisión automatizada, conducirá a un perfil o decisión defectuosa[631]. Conviene recordar sobre este punto, que la información recabada por los proveedores de redes sociales puede resultar parcial o incompleta, lo que, sin duda puede conducir a la inferencia de conclusiones poco acertadas por parte del algoritmo que genera el perfil. En efecto, la información compartida en Internet y redes sociales, no reviste calidad en su totalidad, por tanto, un gran volumen de datos, no garantiza inferencias de datos de mayor calidad. Así, consideramos que los proveedores de redes

[629] TRONCOSO REIGADA, A., "Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)", *op. cit.*, pp. 873-886.

[630] Sobre este extremo, resulta esclarecedora la recomendación realizada por la AEPD en su Guía de privacidad desde el diseño cuando dispone que, en ocasiones la asimetría de la información en la que una de las partes involucrada en una transacción (en este caso el proveedor de redes sociales), posee más o mejor información sobre la otra (el interesado), genera desconfianza entre las partes. Así, el organismo propone que para evitar este patrón se debe proceder a minimizar la cantidad y tipo de datos obtenidos del usuario requeridos para el propósito perseguido y establecer políticas claras y concisas fácilmente comprensibles por el usuario en orden a reducir el desequilibrio entre ambas partes. Sin embargo, en el contexto de las redes sociales, los usuarios apenas conocen una dirección con la que contactar con el responsable, mientras que el proveedor de redes sociales conoce de manera realmente minuciosa detalles personales e incluso íntimos de los usuarios. Guía de privacidad desde el diseño de la AEPD, de octubre de 2019. Obtenido de: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf , p. 41.

[631] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, pp. 12-13.

sociales recopilan un volumen injustificado de datos en relación a los fines para los que estos se tratan (personalización de la experiencia).

A su vez, la implementación de tratamientos basados en el análisis de datos masivos no ha recibido un diseño de tal modo que respete la protección de datos desde el diseño y por defecto (art. 25 RGPD). Así, el CEPD dispone en las Directrices 4/2019, sobre protección de datos desde el diseño y por defecto citada previamente que, en el momento de determinar los medios del tratamiento, el responsable debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados[632]. De este modo, a la hora de diseñar estos nuevos tratamientos masivos de datos, es cierto que la disponibilidad de un excelso volumen de datos se antoja necesaria para la consecución de dicha finalidad. Sin embargo, parece contradictorio que, mientras que el RGPD se inclina por la mínima recogida de datos posible para cada finalidad, paralelamente se haya desarrollado un análisis masivo de datos basado en enormes cantidades de datos con fines de personalización de los servicios y publicidad.

Por ello, consideramos que la privacidad desde el diseño no se ha respetado por los proveedores de redes sociales al implementar mecanismos de control de comportamiento de los usuarios o la inferencia de nuevos datos. Para los casos en los que esta técnica ya fuera empleada, recordemos que el responsable debe reevaluar las operaciones de tratamiento en orden a continuar garantizando la protección de datos personales. Así, deberá instarse a los proveedores a que revisen estas técnicas de tratamientos de datos por resultar especialmente lesivas para los derechos y libertades de las personas usuarias tal y como ha quedado evidenciado en apartados precedentes.

Así las cosas, la implementación de estas técnicas obedece a un modelo de negocio cada vez más intrusivo con los datos personales de los usuarios, tanto los que estos han compartido, como los que no. Debemos advertir que los menores crecen en un contexto que no garantiza la protección de su información, se considere esta de carácter personal o no, ya que el *big data* e IA poseen la capacidad de convertir en dato personal aquellas informaciones que no revisten dicho carácter. Conscientes del ataque que supone para la privacidad la recopilación desproporcionada de datos personales, la empresa Apple ha limitado a redes sociales como Whatsapp, Facebook e Instagram, el acceso a la

[632] Directrices 4/2019, del Comité Europeo de Protección de Datos sobre protección de datos desde el diseño y por defecto, de 20 de octubre de 2020, p. 11.

fototeca completa del terminal móvil de sus usuarios[633]. Ahora, recaerá sobre el usuario la decisión de seleccionar manualmente a qué fotografías proporciona acceso a las redes sociales. Si bien esta medida merece una valoración positiva, consideramos debería extenderse a otros ámbitos en los que, la recopilación continúa resultando excesiva y puede desvelar información privada y sensible sobre menores de edad, como, por ejemplo, mitigar el monitoreo constante de los usuarios.

El RGPD, consciente de las tensiones descritas, propone la solución relativa a la anonimización y pseudonimización de los datos personales disponiendo en el Considerando 26, que los principios de protección de datos no deben aplicarse a la información anónima, esto es, a la información que no guarde relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no pueda resultar identificable o deje de poseer tal carácter tras la aplicación de la técnica descrita. Consecuentemente, el RGPD no afecta al tratamiento de información previamente anonimizada. Efectivamente, tal y como dispone GIL MEMBRADO, las cautelas establecidas por la normativa sobre protección de datos personales, no se aplican a la información anónima[634].

Así las cosas, una definición conceptual de la anonimización proporcionada por el Grupo de Trabajo 29, podría consistir en la eliminación de los datos personales los elementos suficientes para que no pueda identificarse al interesado[635]. La pseudonimización, por su parte, se entiende como un conjunto de datos que no pueden atribuirse a una persona interesada sin información adicional. Esto es, requiere que dicha información adicional figure por separado y garantice que esta no se emplee para lograr identificar a una persona física identificada o identificable[636].

Las empresas han escudado en estas técnicas de anonimización el tratamiento masivo de datos personales por sistemas de *big data* e IA, alegando que los mismos

[633] En una de las actualizaciones del sistema operativo de Apple, la compañía ha limitado el acceso a la galería de imágenes de los terminales de los usuarios del teléfono móvil a las aplicaciones instaladas como Instagram, Facebook, etc. Ahora, los usuarios deberán seleccionar aquellas fotografías a las que deseen conceder acceso a las aplicaciones, sin que se permita un acceso a la completa galería de imágenes por defecto. [fuente propia]

[634] GIL MEMBRADO, C., "Autonomía y tratamiento de datos personales de salud en tiempo de pandemia", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, *op. cit.*, p. 154.

[635] Dictamen 5/2014, del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre técnicas de anonimización, de 10 de abril de 2014, WP 216, pp. 5-6.

[636] Definiciones de la AEPD en torno a la pseudonimización de los datos. Obtenido de: https://www.aepd.es/es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion , (última consulta el 19 de diciembre de 2022).

funcionaban con datos totalmente anonimizados. Asimismo, constituye una creencia generalizada de los interesados, que los datos que los proveedores de redes sociales tratan, no pueden llegar a identificarles. Véase que de tomar por válido dicho argumento, las fricciones expuestas en las líneas precedentes no tendrían cabida al no resultar aplicable la normativa sobre protección de datos personales a mentada información.

Ahora bien, el *big data* y la IA dificultan considerablemente aceptar la anonimización como presupuesto válido para alegar la falta de aplicabilidad de la normativa sobre protección de datos personales, en el sentido que, esta técnica puede re-identificar a las personas sin gran impedimento[637]. En efecto, los datos anónimos pueden volver a cruzarse para re-identificar a los usuarios. Véase que las técnicas de tratamientos de datos masivos pueden identificar a una persona desde la base de datos inicialmente anónimos. Pero no solo eso, también puede inferir nuevas informaciones de datos inicialmente anónimos[638]. Realmente, se ha demostrado que la generación de un conjunto de datos verdaderamente anónimo a partir de un voluminoso conjunto de datos personales, no constituye un propósito sencillo. La razón reside en que estos deben tratarse de tal manera que no puedan destinarse para identificar a una persona física mediante un conjunto de medios que puedan emplearse razonablemente por el responsable del tratamiento o terceros. Además, el tratamiento por el que los datos personales resultan anonimizados debe poseer carácter irreversible. Esto es, la técnica de anominización ha de resultar análogamente permanente al borrado de dichos datos[639].

Sentado cuanto antecede, el *big data* y la IA imposibilitan que, con carácter irreversible, no puedan atribuirse determinados datos personales a una persona interesada[640]. Prácticamente cualquier solución de anonimización eficaz, que debe abogar

---

[637] Considerando 7 de la Recomendación del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, Diario Oficial de la Unión Europea, C 263/10, de 25 de julio de 2018.

[638] En efecto, los datos anonimizados pueden emplearse para enriquecer perfiles existentes de personas creando nuevos problemas para la efectiva protección de los datos personales. Dictamen 5/2014, del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre técnicas de anonimización, de 10 de abril de 2014, WP 216, p. 4.

[639] Véase mismo Dictamen 5/2014, del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre técnicas de anonimización, p. 6.

[640] De conformidad con las palabras manifestadas por RICHARD MARTINEZ MARTINEZ, en el III Congreso de buen gobierno y transparencia de la Comunitat Valenciana, celebrado los días 5 y 6 de septiembre de 2018, "La anonimización es imposible". Obtenido de: https://www.youtube.com/watch?v=EwwecCrJKfg&list=PLMqWVbmUv8Thcv7QFKfHfUYT8f1fogdkG&index=8 (última consulta el 1 de marzo de 2022).

por impedir a cualquier sujeto identificar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos e inferir cualquier tipo de información a partir de dicho conjunto, deviene imposible cuando los datos anónimos se someten a tratamiento por técnicas de *big data* e IA[641]. Precisamente, la elaboración de perfiles puede poner en peligro el anonimato de los datos previamente anonimizados. En definitiva, esta nueva tecnología de tratamiento de datos, resulta un verdadero obstáculo para la salvaguarda de los datos personales de los interesados, ya que la anonimización no constituye protección suficiente para su privacidad. Esta nueva posibilidad de desanonimizar los datos que ya no revestían carácter personal, unida al resto de riegos que estas técnicas de análisis masivos implican sobre la privacidad de los usuarios de redes sociales nos lleva a compartir la reflexión de GARRIGA DOMÍNGUEZ: en este nuevo escenario, se debería reformular el concepto de dato personal, puesto que a pesar de que los datos parezcan invisibles o impersonales, prácticamente cualquier tipo de dato puede emplearse para localizar personas algorítmicamente[642]. En ese sentido, incluso la Carta de Derechos Digitales española citada en apartados anteriores, se refiere a la protección de datos, mientras que en versiones anteriores, aludía a la protección de datos personales[643].

Por todo lo expuesto, el principio de responsabilidad proactiva (art. 5.2. RGPD) que debe guiar la totalidad de los tratamientos de datos personales no logra su fin cuando se refiere a tratamientos masivos de datos personales. Mientras que el responsable del tratamiento debe poder demostrar que cumple con la normativa sobre protección de datos personales, estos proveedores de servicios continúan desarrollando nuevas técnicas de tratamiento de un modo alejado los principios que inspiran el RGPD[644]. En este contexto,

[641] Sirva como ejemplo, que la plataforma Netflix llevó a cabo un experimento de reidentificación sobre la base de datos de clientes formada por más de 100 millones de valoraciones de unas 1800 películas en una escala del 1 al 5 por parte de 500.000 usuarios. La empresa publicó esta base de datos tras anonimizarla con arreglo a sus directrices internas sobre privacidad. Los resultados del estudio arrojaron que se podía identificar de manera unívoca el 99% de los registros de usuarios en el conjunto de datos empleando 8 valoraciones y fechas con errores de 14 días a modo de criterio de selección. NARAYANAN, A., Y SHMATIKOV, V., "Robust de-anonymization of large sparse datasets", *Security and Privacy*, 2008, IEEE Symposium, pp. 111-125.

[642] GARRIGA DOMINGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data y de la Computación ubicua, op. cit.*, p. 36.

[643] RAMÓN FERNÁNDEZ, F., "Protección de menores y educación en el entorno digital (X y XVII)", en COTINO HUESO, L., (Coordinador), *La Carta de Derechos Digitales,* Valencia, Tirant lo Blanch, 2022, p. 156.

[644] Así, continuamos identificando situaciones en las que los proveedores de redes sociales incumplen reiteradamente de manera grave el principio de responsabilidad proactiva al protagonizar comportamientos contrarios a la salvaguarda de la privacidad de las personas usuarias. Baste como muestra que la plataforma Facebook ha resultado sancionada con un total de 550 millones de dólares al someter a tratamiento sin el consentimiento expreso preceptivo datos biométricos de usuarios del Estado de Illinois. Concretamente, el reconocimiento facial se empleaba en fotografías de los usuarios con fines de realizar a futuro sugerencias

difícilmente pueden demostrar que los tratamientos de datos personales que practican se encuentren guiados por el cumplimiento de la normativa de protección de datos personales.

3.3. El RGPD ante la elaboración de perfiles de personalidad del menor y la toma de decisiones automatizadas en redes sociales

La sociedad actual asiste al desarrollo de una nueva era digital en la que el análisis masivo de datos personales conduce a una toma de decisiones en las que el factor humano cada vez se encuentra más ausente. Así las cosas, las decisiones automatizadas y la elaboración de perfiles conforman una parte integral de los procesos *big data* e IA. Cada vez con mayor frecuencia, muchas de las decisiones tomadas en diversos ámbitos no se preceden por la intervención humana, sino que, la decisión se ha adoptado tras un análisis de datos que clasifican a las personas en un determinado grupo al que se atribuyen unos comportamientos futuros (elaboración de perfil).

Concretamente, el RGPD aborda tres posibles formas de elaborar perfiles en el art. 22: en primer lugar, la elaboración de perfiles sin que estos se empleen para la toma de decisiones; en segundo lugar, las decisiones basadas en la elaboración de perfiles, esto es, aquellas en las que una persona decide si aprueba determinada decisión sobre la base de un perfil elaborado mediante tratamiento automatizado de datos personales; en tercer lugar, las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que producen efectos jurídicos en el interesado o le afectan significativamente de un modo similar.

Preocupado por el impacto de estas conductas sobre los derechos y libertades de las personas, el legislador europeo introduce en el RGPD nuevas facultades cuya titularidad recaerá sobre los interesados en orden a garantizar el control de sus datos personales en este nuevo ámbito (art. 22 RGPD). El Considerando 71 del RGPD acoge, por una parte, la definición sobre la elaboración de perfiles; por otra parte, ejemplos tendentes a ilustrar lo que debe entenderse por una decisión automatizada. A tenor de lo expuesto en este considerando, puede considerarse un ejemplo de decisión automatizada

---

de etiquetado de personas que aparecieran en las fotografías compartidas. CANTANTE NATASHA y MIKE ISAAC., "Facebook to pay 500 million to settle facial recognition suit", *The new York Times*, January 29 of 2020. Obtenido de: https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html (última consulta el 2 de noviembre de 2021).

la denegación automática de una solicitud de crédito en línea o los servicios de contratación en la red en los que no interviene ningún tipo de intervención humana. Por otra parte, la elaboración de perfiles, se refiere a un tipo de procesamiento consistente en cualquier forma de tratamiento de datos personales que evalúe aspectos personales relativos a una persona física, en particular, para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, y que conduce generalmente a decisiones automatizadas. Tal y como dispone ROMEO CASABONA, la elaboración de un perfil puede depurar determinados aspectos o manifestaciones de la personalidad de las personas, incluso cabe realizar predicciones sobre su comportamiento previsible[645].

No obstante, no debe caerse en el frecuente error de confundir la elaboración de perfiles con la adopción de decisiones individuales automatizadas. Efectivamente, ambas técnicas obedecen a intereses diferentes. Por un lado, hemos tenido ocasión de señalar que la elaboración de un perfil conlleva la creación de nuevos datos personales no facilitados directamente por el interesado con el fin de predecir su comportamiento futuro. Por otro lado, las decisiones individuales automatizadas suponen la adopción de una concreta decisión en la que no existe intervención humana, pudiendo esta basarse en la previa elaboración de un perfil o no[646].

Sentado cuanto antecede, la normativa europea dispone que los responsables del tratamiento, pueden elaborar perfiles y adoptar decisiones automatizadas siempre que cumplan todos los principios y dispongan de unas bases jurídicas adecuadas para el tratamiento. En cambio, para las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, resultará de obligado cumplimiento a su vez el art. 22.1 RGPD, al que nos referiremos posteriormente.

Así, los proveedores de redes sociales podrán aplicar este tipo de tratamiento cuando este se acomode a alguna de las bases legales del art. 6 RGPD. No obstante, los

[645] ROMEO CASABONA, C.M., "Elaboración de perfiles (comentario al artículo 4.4 RGPD)", TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Civitas, Madrid, 2021, p. 609.
[646] A modo de ejemplo, mostrar anuncios a un usuario cuya dirección IP se localice en determinada ciudad, supondría la adopción de una decisión automática, pero en la que, sin embargo, no se ha elaborado un perfil. Por el contrario, si durante un período de tiempo se procediera a monitorizar los hábitos de navegación de este, en orden a determinar qué tipo de comida prefiere, la inclusión de esta publicidad sí conllevaría la elaboración de un perfil.

proveedores de redes sociales más habituales -entre los que podemos destacan Instagram o Facebook- acostumbran a escoger bases legales inadecuadas para el tratamiento de datos que aparejan técnicas de *big data* e IA. En orden a resultar más específicos, estas plataformas tienden a justificar el tratamiento de los datos personales argumentando la personalización de sus servicios (lo que incluye el análisis del comportamiento dentro y fuera de la red social, la información compartida por el usuario y generalmente la elaboración de perfiles de estos) como presupuesto indispensable para la ejecución del contrato, así como para la consecución de un interés legítimo por parte de la plataforma[647].

Cabe señalar que el CEPD confirma en las Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, que el seguimiento y elaboración de perfiles de usuarios no pueden sustentarse sobre la base de la ejecución del contrato o prestación del servicio, dado que, el seguimiento y comparación de las características y conductas de los usuarios con fines de publicidad dirigida a otras personas, no resultan necesarios desde el punto de vista objetivo para la ejecución del contrato del que el usuario es parte[648]. Ciertamente, para la prestación del servicio, el proveedor de la red social debe poner a disposición del usuario de un entorno *online* para que éste socialice y se comunique, pero ello no lleva implícito que la elaboración de perfiles con fines de mercadotecnia, que solamente interesan al proveedor revistan carácter necesario para la prestación del servicio[649].

---

[647] Política de privacidad de Instagram/Facebook obtenido de la página web: https://mbasic.facebook.com/privacy/policy/printable/#18.2-PerformanceOfAContract (última consulta el 22 de septiembre de 2022), p, 60 y ss.

[648] Considerando 56 de las Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, p. 17.

[649] Así, volvemos a incidir en la sanción impuesta por la autoridad irlandesa de protección de datos personales (*Data Protection Commission of Ireland*) al Grupo Meta, el pasado 4 de enero de 2023, siguiendo la decisión vinculante del CEPD que fue consultado en este caso al amparo del art. 60 RGPD. Ya que, en esta, se sanciona al Grupo meta por justificar los tratamientos de datos personales con fines de mercadotecnia directa sobre la base legal de la ejecución del contrato. En efecto, señala el organismo que esta funcionalidad no resulta indispensable para la ejecución del contrato o la prestación del servicio que oferta el Grupo Meta en sus servicios de Facebook e Instagram. En consecuencia, el tratamiento de datos es ilícito al contravenir el art. 6 RGPD. Véase el apartado 32 de la decisión del CEPD, *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)*, de 5 de diciembre de 2022. Obtenido de: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf (última consulta el 30 de enero de 2023), p. 12.

Por lo tanto, pudiera pensarse que la elaboración de perfiles con fines de mercadotecnia, responde a intereses legítimos de las plataformas al amparo del Considerando 47 del RGPD[650]. En ese sentido, el Grupo de Trabajo del Artículo 29 define el interés legítimo como el fundamento jurídico que permite el tratamiento necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero al que se comuniquen los datos siempre que no prevalezcan los derechos y libertades fundamentales de los interesados que requieran protección[651]. Tal y como se desprende de dicha definición, con antelación, deberán sopesarse y someterse a juicio de ponderación, por una parte, los intereses del responsable, por otra parte, los derechos y libertades en juego de los interesados.

No obstante, el Grupo de trabajo del Artículo 29 advirtió en ese mismo Dictamen que resultaba difícil para los responsables del tratamiento justificar la utilización de intereses legítimos como base jurídica para las prácticas intrusivas basadas en la elaboración de perfiles y seguimiento con fines de mercadotecnia o publicidad[652]. Así, si bien es cierto que el interés legítimo puede constituir una base legal legítima para fines de publicidad o mercadotecnia directa tal y como dispone el Considerando 47 del RGPD, ello no significa, tal y como señala la AEPD, que los responsables del tratamiento puedan remitirse al mismo como fundamento jurídico en orden a supervisar de manera indebida las actividades en línea y fuera de línea de sus clientes, combinar enormes cantidades de datos sobre ellos provenientes de diferentes fuentes- que fueran inicialmente recopilados en otros contextos y con fines diferentes- y crear perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento, sin un mecanismo viable de oposición, y por no mencionar la ausencia de un consentimiento informado. Tratándose de

[650] Sobre este particular cabe apuntar, además, que el legislador español al transponer el art. 7 (f) de la Directiva 95/46/CE a través de los arts. 30 de la LOPD y 45 del Reglamento 1720/2007 por el que se desarrollaba esta, creó una presunción *iure et de iure* respecto a la no prevalencia de los derechos de los interesados frente al interés legítimo del responsable. En definitiva, el marketing directo se constituía como una de las excepciones que eludiendo el consentimiento del interesado permitían al responsable aducir un interés legítimo en el tratamiento. Para mayor detalle consúltese GÁLLEGO HIGUERAS, G.F., Y GARCÍA RODRÍGUEZ, P., "Tratamiento de datos en el ámbito publicitario (Comentario al art. 23 LOPDGDD)", TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, p. 3703-3706.

[651] Dictamen 6/2014 del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de abril de 2014, WP 217, p. 5-6.

[652] Dictamen 6/2014 del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de abril de 2014, WP 217, p. 55.

elaboración de perfiles, continua la AEPD sentando que resulta probable que dicha actividad represente una intromisión importante en la privacidad del cliente, prevaleciendo en este supuesto los derechos e intereses del usuario sobre el interés del responsable del tratamiento[653].

En efecto, el tratamiento de datos personales que prevea la elaboración de perfiles en el contexto de redes sociales, no puede sustentarse sobre la base legal del interés legítimo en todo caso. Ello se debe a que, el usuario no debe soportar, por defecto, una recopilación de un gran volumen de datos personales, que no obedece a la puesta a disposición de este de un entorno en el que socializar, sino a intereses que solamente satisfacen al proveedor de red social[654].

De conformidad con GÁLLEGO HIGUERAS y GARCÍA RODRÍGUEZ, los perfilados menos invasivos prácticamente con toda certeza podrán justificarse en el interés legítimo; en cambio, cuando el perfilado se acompañe de un análisis muy exhaustivo de las características de los individuos, incorpore múltiples aspectos de la personalidad de aquellos o se complete con fuentes externas, el consentimiento constituirá previsiblemente la base de legitimación aplicable[655]. En esa línea también se pronuncia AVIÑÓ BELENGUER, pues dispone que, si bien se permite la base del interés legítimo para los casos de envío de comunicaciones publicitarias a los clientes de una empresa (bajo determinadas circunstancias), esta no prevalecerá cuando para ello se requiera de la elaboración de perfiles exhaustivos del interesado por medio de la combinación de diversas fuentes de información[656].

---

[653] Consúltese al respecto el Informe 0017/2019 de la AEPD, de 16 de junio de 2020, p. 23. El citado informe resuelve la consulta planteada por un centro comercial sobre la posibilidad de instalar un sistema de "Wifi-Tracking", cuyo fin reside en conocer los recorridos y tránsitos realizados por los clientes para posteriores acciones de mercadotecnia.

[654] En efecto, para la puesta a disposición del usuario de un entorno en el que socializar simplemente- en el que no se requieren más que los datos de registro – al constituir un servicio imprescindible para la prestación del servicio, no se precisa del consentimiento y el tratamiento podrá sustentarse sobre la base legal de la ejecución del contrato o prestación del servicio. Sin embargo, en el caso de la personalización de los servicios-finalidad para la que se requiere de un elevado volumen de datos- tal y como ha quedado de manifiesto, la base legal sobre la que el tratamiento debe sustentarse es el consentimiento del usuario.

[655] GÁLLEGO HIGUERAS, G.F., Y GARCÍA RODRÍGUEZ, P., "Tratamiento de datos en el ámbito publicitario (Comentario al art. 23 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, *op. cit.*, p. 3730.

[656] AVIÑÓ BELENGUER, D., "El uso de cookies de publicidad comportamental desde la óptica de la protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2020, núm. 56, p. 32.

En definitiva, si bien el interés legítimo podría considerarse un fundamento jurídico válido para los fines de mercadotecnia directa del responsable, en el contexto de redes sociales, el tratamiento a practicar, consideran dicha base legal como totalmente desaconsejada para la legitimación del tratamiento[657]. Por ello, no coincidimos con ARENAS RAMIRO cuando afirma que la finalidad del marketing directo se puede considerar un interés legítimo del responsable[658], ya que pudiera pensarse que no caben excepciones como la recientemente aducida, esto es, que el tratamiento suponga una gran intromisión en los intereses y derechos del interesado[659].

Ciertamente, tal y como señala el Grupo de Trabajo del Artículo 29 en el Dictamen 6/2014, esta base legal no debe emplearse como "último recurso" para aquellas

[657] En ese sentido, resulta ilustrativa la Sentencia del Tribunal de Justicia de la UE, de 29 de julio de 2019, *Fashion ID,* Asunto C-40/17, apartado 95, cuando el Tribunal afirma que, para poder tratar los datos conforme a un interés legítimo en el contexto de la publicidad en redes sociales *online*, deben cumplirse tres condiciones de manera cumulativa, a saber: en primer lugar, la persecución de un interés legítimo en el tratamiento por parte del proveedor de la red social o por terceros anunciantes en este caso; en segundo lugar; que el tratamiento resulte necesario para alcanzar esos intereses legítimos; por último, que dicho legítimo interés no anule intereses subjetivos o afecte a derechos y libertades fundamentales. Así, es posible que constituya interés legítimo de la red social aumentar sus ingresos por medio de ofrecer a los anunciantes un espacio donde publicitarse. No obstante, dicha circunstancia no conduce automáticamente a considerar que concurre un interés legítimo, pues han de cumplirse igualmente el resto de condiciones señaladas. En concreto, ha de justificarse una necesidad de tratamiento a efectos de alcanzar dicho interés legítimo, lo que lleva a considerar que se trata de la técnica menos invasiva para lograr dicho fin. Por último, se debe ponderar que dicho interés legítimo no anule los derechos y libertades fundamentales de los interesados: es en este aspecto donde, el interés legítimo tanto del proveedor de la red social como de los anunciantes debe ceder ante los derechos y libertades fundamentales de los interesados. Las consideraciones expuestas, nos permiten afirmar la imposibilidad de aplicar la base legal del interés legítimo en este contexto. Esta se trata a su vez la interpretación realizada por el CEPD *Guidelines 8/2020 on the targeting of social media users*, Version 2.0, adopted on 2 september 2020, pp. 15-16. Asimismo, en virtud de lo expuesto por las Directrices 2/2019, del CEPD sobre sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados citada anteriormente en la presente investigación, la publicidad comportamental y la personalización de servicios en el contexto descrito, no pueden ampararse en la base legal 6.1.b RGPD como requisito indispensable para la ejecución del contrato, pp. 16-17.

[658] ARENAS RAMIRO, M., "El derecho de oposición (comentario al artículo 21 RGPD y al artículo 18 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 1710. ÁLVAREZ CARO, también se pronuncia en términos similares, afirmando que el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado sobre la base legal del interés legítimo. ÁLVAREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en RECIO GAYO, M., Y PIÑAR MAÑAS, J.L., (Directores) *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad,* Madrid, Reus, 2016, p. 236.

[659] Sobre este particular, merece traer a colación las palabras de GÁLLEGO HIGUERAS, G.F., Y GARCÍA RODRÍGUEZ, P., "Tratamiento de datos en el ámbito publicitario (Comentario al art. 23 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.*, p. 3703 cuando señala que, ya no es posible afirmar que los datos personales para marketing directo queden amparados "sí o sí" en el supuesto del art. 6.1.f) RGPD.

situaciones raras o imprevistas o como una última posibilidad cuando el tratamiento no puede sustentarse sobre las restantes bases legales de tratamiento[660].

Sentado cuanto antecede, estas plataformas deberán recabar el consentimiento del usuario para la elaboración de estos perfiles. En ese sentido, el Grupo de Trabajo del Artículo 29, dispone en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, que los responsables que pretendan basarse en el consentimiento como base para la elaboración de perfiles, deberán demostrar que las personas interesadas entienden con exactitud qué tipo de tratamiento consienten[661].

Ahora bien, ha quedado de manifiesto que el consentimiento en el contexto del *big data* e IA acusa un marcado carácter simbolista, especialmente si se presta por un menor de edad. Puesto que, se debe denunciar, por una parte, la falta de transparencia más que evidente en la advertencia a los usuarios sobre la práctica de este tipo de tratamiento, pues los proveedores de redes sociales no informan en sus políticas de privacidad de la lógica subyacente de esta práctica[662]; por otra parte, lo ilusorio que resulta el consentimiento del menor a la práctica de los mismos, pues en ningún caso alcanza a comprender la magnitud del tratamiento ni las consecuencias que conlleva para su privacidad. Por todo ello, la configuración actual del consentimiento tampoco constituye una base legal adecuada en este contexto.

Todavía cabe señalar, que para el caso de las decisiones exclusivamente automatizadas en las que no interviene el factor humano, habrá de cumplirse, además, el art. 22.1. RGPD. El citado precepto dispone que todo interesado tendrá derecho a no resultar objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles que produzca efectos jurídicos sobre este o le afecte significativamente de modo similar.

---

[660]Dictamen 6/2014 del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de abril de 2014, WP 217, p. 11.

[661] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 14.

[662] De la lectura completa de la Política de privacidad de Facebook e Instagram, se deduce vagamente la práctica de tratamientos basados en la elaboración de perfiles, pero no se explica su lógica subyacente. Política de privacidad de Instagram/Facebook obtenido de la web: https://mbasic.facebook.com/privacy/policy/printable/#18.2-PerformanceOfAContract (última consulta el 21 de septiembre de 2022).

Quizás la mayor dificultad reside en acreditar que ciertas decisiones individuales automatizadas pueden causar efectos significativos similares a la producción de efectos jurídicos en el ámbito publicitario de las redes sociales. No obstante, el Grupo de Trabajo del Artículo 29 afirma que, si bien con carácter general la publicidad basada en la elaboración de perfiles no poseerá un efecto significativo y análogo a los efectos jurídicos, en algunos casos, ciertas decisiones de la índole señalada pueden ocasionar efectos similares a los jurídicos dependiendo de las circunstancias particulares de cada caso. Así, en orden a determinar si este tipo de decisiones pueden llegar a producir efectos jurídicos similares a los jurídicos, y por ende, resultarles de aplicación el art. 22.1 RPGD, habrán de valorarse los siguientes factores, a saber: el nivel de intrusismo en la privacidad de los usuarios durante el proceso de elaboración de perfiles, incluido el nivel de seguimiento de las personas en diferentes sitios webs, dispositivos y servicios; las expectativas y deseos de las personas afectadas al emplear estos; la forma en la que se presenta el anuncio; y por último, el uso de conocimientos sobre las vulnerabilidades de los interesados[663].

De este modo, cabe decir que los perfiles que los proveedores de redes sociales pueden construir, alcanzan un nivel de precisión y detalle elevado. Ello se debe a que combinan diversas fuentes de datos disponibles tales como, aquellos que los usuarios comparten, pero también los que responden a hábitos de su navegación, e incluso datos disponibles en Internet sobre la reseñada persona. Esto es, todos los datos pasivos que se recopilan sobre el usuario sin que este advierta dicha circunstancia. En definitiva, el nivel de intrusismo en este contexto resulta máximo pues los proveedores de redes sociales, monitorean y rastrean constantemente la actividad del interesado cuando interacciona con sus servicios e incluso fuera de ellos, con el objetivo de enriquecer la elaboración de perfiles sobre estos con la señalada información.

Por otra parte, los proveedores de redes sociales conocen de las vulnerabilidades de los menores, sin embargo, al no verificar la edad de los mismos al acceder a sus plataformas, muchos de los servicios ofertados no deberían dirigirse a un público especialmente vulnerable como los menores de edad. Incluso el propio Grupo de Trabajo del Artículo 29 reconoce, que un tratamiento que carece de impacto sobre las personas en

[663] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 24.

general, puede ocasionar un efecto significativo en determinados grupos de la sociedad como grupos minoritarios, adultos vulnerables o niños[664]. En efecto, tal y como dispone RUBÍ PUIG, cuando las decisiones individuales automatizadas llegan a afectar a todos los miembros de un grupo social, el impacto global de las mismas puede resultar significativo[665]. Con todo, siguiendo a AVIÑÓ BELENGUER, consideramos que a las decisiones individuales automatizadas basadas en dirigir publicidad comportamental a las personas usuarias de redes sociales debe resultarles de aplicación el art. 22.1. RGPD[666].

Ahora bien, no se puede negar que el art. 22.2 RGPD regula tres excepciones a la prohibición de esta práctica que permiten la adopción de decisiones individuales automatizadas, a saber: que la elaboración de estos resulte necesaria para la ejecución del contrato o la prestación del servicio, que este comportamiento se encuentre autorizado por el derecho de la UE o Estado miembro; y, por último, que concurra un consentimiento expreso del interesado, en este caso usuario de la red social.

Sin embargo, la elaboración de perfiles no resulta necesaria para la prestación del servicio por parte de los proveedores de redes sociales, este puede desarrollarse sin los servicios de mercadotecnia para los que emplean esta técnica, de modo que, a nuestro parecer, no debe justificarse dicho tratamiento de datos por medio del art. 22.2. letra a). Por otra parte, resultan igualmente aplicables en este caso las consideraciones sobre la falta de garantías del consentimiento en este supuesto recientemente expuestas, esto es, los proveedores de redes sociales no informan claramente en sus políticas de privacidad sobre la elaboración de perfiles; y por ende, tampoco comparten la lógica aplicada de dichos tratamientos[667]. Definitivamente, la elaboración de perfiles practicada por los

[664] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 25.

[665] RUBÍ PUIG, A., "Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores", *Revista de educación y derecho*, 2021, núm. 24, pp. 14-15.

[666] En efecto, el autor sostiene que una vez elaborados los perfiles publicitarios de los usuarios, los anunciantes podrán dirigir de manera automatizada (por medio de una decisión automatizada) al equipo rastreado la publicidad *online* que coincida con los gustos e intereses deducidos de dicho rastreo y análisis. AVIÑÓ BELENGUER, D., "El uso de cookies de publicidad comportamental desde la óptica de la protección de datos", *op. cit.*, p. 3.

[667] Concretamente, los arts. 13.1.f), 14.2.g) y 15.1.h) exigen informar al interesado sobre la práctica de decisiones automatizadas, así como el ofrecimiento de información sobre la lógica aplicada de dicho tratamiento, además de proporcionar información sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Sin embargo, la falta de transparencia al ocultar dicha práctica colisiona con el art. 5.1.a) RGPD. De acuerdo con ello se muestra SANCHO VILLA, D., "Las decisiones individuales automatizadas, incluida la elaboración de perfiles (comentario al artículo 22 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley*

proveedores de redes sociales con el fin de adoptar decisiones individuales automatizadas, no posee acomodo legal en la normativa sobre protección de datos personales vigente.

En ese sentido, la AEPD ha impuesto sanciones de importe elevado a la banca por elaborar perfiles sin el consentimiento del interesado con el fin de valorar su solvencia crediticia[668]. Si bien en el presente supuesto el banco informaba sobre la finalidad consistente en la elaboración de perfiles, no recababa el consentimiento del interesado para su práctica. En el caso de los proveedores de redes sociales, la situación reviste mayor gravedad, pues los usuarios no pueden prestar un consentimiento sobre una finalidad del tratamiento de la que no se informa, y por tanto, no pueden consentir[669]. REDUNDANTE MAL REDACTADO A lo que debemos añadir, que también imposibilita que se oponga a un tratamiento sobre el que no se le informa (art. 21 RGPD).

Por otra parte, el art. 22.4 RGPD prohíbe la elaboración de perfiles sobre categorías especiales de datos personales (art. 9 RGPD); ahora bien, hemos señalado anteriormente que estas técnicas poseen la capacidad de inferir datos especiales, de aquellos datos que no revisten dicho carácter. En suma, estos nuevos datos inferidos de carácter especial se tratan sin el consentimiento, ni el conocimiento del usuario.

Orgánica de Protección de datos personales y Garantía de los Derechos digitales, Madrid, Civitas, 2021, pp. 1725-1745. En ese sentido, la Carta de Derechos Digitales aprobada por el Gobierno Español, a pesar de su carácter no normativo, alumbra dichos principios. Concretamente, el art. 5.2 dispone que el responsable del tratamiento debe informar explícitamente al interesado sobre la finalidad de localización, el perfilado o la decisión automatizada y sobre el ejercicio del derecho de oposición; y además, presentarlos al margen de cualquier otra información. Carta de Derechos Digitales del Gobierno de España. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022), p. 10.

[668] Véase el Procedimiento Sancionador PS/00500/2020. Obtenido de: https://www.aepd.es/es/documento/ps-00500-2020.pdf (última consulta el 5 de enero de 2023) en el que la AEPD sanciona a CAIXABANK con una multa de 3.000.000 de euros por elaborar perfiles sin el consentimiento del interesado con el fin de valorar la solvencia crediticia de este y proceder a la oferta de determinados productos financieros. En concreto, el interesado reclamante solamente mantuvo una relación puntual con el banco para valorar la contratación de determinados productos, esto es, no recibe la consideración de cliente de este, ni finalmente contrata ningún producto con la sucursal. Por tanto, denuncia que en ningún momento llegó a consentir que se empleara dicha información para la elaboración de perfiles.

[669] Sirva como ejemplo, que el Grupo Meta (antiguo Grupo Facebook) no informa claramente en sus políticas de privacidad sobre la práctica consistente en la elaboración de perfiles (a pesar de resultar una mención obligatoria en aras de cumplir con la concurrencia de un consentimiento informado) cuando su propio CEO Mark Zuckerberg reconoció en las dos series de respuestas escritas a preguntas en la reunión entre líderes de los grupos políticos del Parlamento Europeo y este, que practican perfiles con fines de personalización de sus productos. Véase al respecto el set de respuestas de dicha reunión obtenido de https://www.europarl.europa.eu/resources/library/media/20180604RES04911/20180604RES04911.pdf , p. 10. (última consulta el 5 de noviembre de 2021). En consecuencia, la lógica aplicada de dicha elaboración de perfiles tampoco se informa.

En otro orden de ideas, el Considerando 71 del RGPD, acoge un principio de especial valor en la presente tesis doctoral pues, dispone que este tipo de decisiones no deben afectar al menor[670].

Aun así, el Grupo de Trabajo del Artículo 29 matiza dicha negativa en sus Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 en cuanto que reconoce que el art. 22 del RGPD no impide a los responsables del tratamiento tomar decisiones basadas exclusivamente en el tratamiento automatizado acerca de los niños. De todos modos, sí dispone que las decisiones sometidas a los parámetros expuestos pueden influir en las elecciones y en el comportamiento de los menores, dependiendo de la naturaleza de las elecciones y los comportamientos en cuestión. Así, el órgano consultivo europeo, consciente de que los niños representan un grupo vulnerable de la sociedad, insta a las organizaciones a abstenerse en general de elaborar perfiles sobre menores con fines de mercadotecnia. Ello se debe, principalmente, a que los menores pueden mostrarse especialmente susceptibles en el entorno en línea y pueden verse influenciados con mayor facilidad por la publicidad comportamental[671]. Así, por ejemplo, la elaboración de perfiles puede emplearse para dirigirse a jugadores que, según el algoritmo diseñado por la plataforma resulten más propensos a gastar dinero en los juegos, así como para ofrecer más publicidad personalizada sobre el juego. Dada la edad y falta de madurez de los niños, estos pueden no comprender la motivación latente detrás de este tipo de mercadotecnia, así como sus lesivas consecuencias.

Más aún, el Considerando 38 del RGPD propugna una protección jurídica específica de los datos personales del menor, ya que estos pueden resultar menos conscientes de los riegos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Así, dicha protección específica ha de aplicarse, en particular, a la utilización de datos personales de los niños con fines de mercadotecnia o elaboración de perfiles de personalidad, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a estos. Lejos de lo expuesto, el modelo de negocio diseñado e instaurado por los proveedores de redes sociales continúa

[670] Considerando 71 «Tal medida no debe afectar a un menor».
[671] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, pp. 31-32.

basándose en la toma de decisiones de este tipo independientemente de la edad del usuario.

Además, en el caso de usuarios menores de edad, la eficaz protección ante esta nueva técnica de procesamiento de datos se torna harto compleja ante la más que manifiesta falta de madurez del menor para prestar un consentimiento informado. Así, a la falta de transparencia por parte de los proveedores de redes sociales, habría que añadir la imposibilidad por parte de este colectivo de comprender el alcance y lógica aplicada de este tratamiento. En consecuencia, el consentimiento del menor no ha de resultar presupuesto válido para consentir el tratamiento de datos para la elaboración de perfiles o adopción de decisiones individuales automatizadas. El menor no puede ejercer un control efectivo sobre sus datos personales en un entorno técnicamente complejo en el tratamiento de datos que, además, puede resultar de gran riesgo para su desarrollo personal y formación de su personalidad dada la evidente capacidad que estas técnicas poseen para incidir sobre sus decisiones y llegar a manipular su comportamiento.

A mayor abundamiento, la Carta de Derechos Digitales citada anteriormente, en su disposición 10.3 sobre protección de las personas menores de edad en el entorno digital, afirma que se prohíben los tratamientos de la información de menores de edad orientados a establecer perfiles de personalidad en entornos digitales. Asimismo, el mismo precepto establece que devendrán ilícitas las prácticas de perfilado susceptibles de manipular o perturbar la voluntad de los menores, y en particular, la publicidad basada en este tipo de técnicas[672]. Así, queda de manifiesto que los proveedores de redes sociales deben abstenerse de la elaboración de perfiles de menores de edad para la personalización de la publicidad, afirmación con la que nos mostramos acordes[673]. Sin embargo, la carta no posee valor jurídico[674].

En ese sentido, cabe afirmar que, el Gobierno de California ha aprobado de forma pionera una norma- la *California Age-Appropriate Design Code Act* (Ley del Código de Diseño Adecuado a la Edad)- cuyo fin reside en proteger la privacidad de menores de 18

[672] Véase, la Carta de Derechos Digitales del Gobierno de España. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022), p. 13.
[673] Mas dicha consideración, ya se estableció por el Grupo de Trabajo del Artículo 29 en 2013 en su Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes, de 27 de febrero de 2013, WP 202, p. 32.
[674] Idénticas manifestaciones pueden proferirse de la Declaración Europea de los Derechos y Principios Digitales para la Década Digital. Diario Oficial de la Unión Europea, de 23 de enero de 2023, C 23/1, p. 8.

años que empleen servicios en línea. Así, la norma impone a los proveedores de redes sociales el deber de anteponer el interés del menor frente a sus propios intereses, forzándoles a tomar medidas como abstenerse de elaborar perfiles concernientes a menores de edad con fines de publicidad y mercadotecnia directa[675].

En esa línea, el Reglamento 2022/2065 relativo a un mercado único de servicios digitales aprobado por el Parlamento Europeo, también se decanta por prohibir el perfilado de menores en su art. 28[676]. Si bien se constituye como una decisión que alabamos, surge nuevamente la necesidad de adoptar mecanismos que verifiquen la verdadera edad del menor cuando se registra en una plataforma social, ya que, de lo contrario, corre el riesgo de convertirse en una medida carente de aplicabilidad, pues al no caber la posibilidad de restringir una función del sistema si no se conoce la edad del usuario. Por ello, no comprendemos que el Considerando 71 afirme que esta obligación no debe incentivar en los prestadores de plataformas en línea la captura de la edad del destinatario del servicio antes del uso. Ya que, precisamente el art. 8 RGPD exige verificar la edad del menor para la emisión de un consentimiento válido. Algo que solamente podrá ocurrir si la edad se verifica por lo menos, de manera simultánea a la prestación del consentimiento.

Así, no caben dudas de que la tenencia del legislador reside en restringir la práctica de estos tratamientos sobre información personal de menores. Como no podía ser de otro modo, convenimos con que se debe prohibir a los proveedores de redes sociales elaborar perfiles y adoptar decisiones automatizadas exclusivamente basadas en estos cuando el usuario de la plataforma sea menor de edad[677]. Ahora bien, el RGPD debe acoger dicha prohibición en su articulado, pues si bien el Considerando 71 aconseja no

---

675 Véase la noticia en Diario La Ley, de 1 de septiembre de 2022. Obtenido de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAGXMMQvCQAyG4V_jLV3Sq4MON7UODhWH7nK95DBYkiOlQv-9dRGK3_jx8DJiuF0AwNenbY17k82sEjx4D2eonSjS0LVhEaTMQvglnNdO07AWCjlOMzkaVV-70uNXSIVDT7LcjSVxidPx0MT9sRn8N1erYtXySIZklJ76Aezw_vauAAAAWKE (última consulta el 5 de octubre de 2022).

676 En esa misma línea, el Comité de Derechos del Niño, dispone en el apartado 42 de su Observación general núm. 25, de 2 de marzo de 2021, que los Estados partes deben prohibir por ley la elaboración de perfiles o la selección de niños de cualquier edad con fines comerciales.

677 Especialmente si se parte de que algunas redes sociales no recaban el consentimiento preceptivo de los representantes legales para practicar estos tratamientos sobre información personal de menores de 14 años. A modo de ejemplo, la red social Musica.Ly (posteriormente TikTok) fue sancionada en 2019 por recabar y utilizar con fines comerciales datos personales de menores de 13 años sin recabar el consentimiento de sus representantes legales. GARCIA GARNICA, M.C., "Datos personales y menores de edad", en GONZÁLEZ PACANOWSKA, I., (Coordinadora) *Protección de datos personales*, *op. cit.*, p. 166.

llevar a cabo este tipo de tratamientos sobre información personal de menores, sus preceptos no se decantan por prohibirlos, al igual que el CEPD, que tampoco ha interpretado una prohibición del perfilado de información concerniente a jóvenes tal y como se ha manifestado anteriormente. Además, evitando este tipo de prácticas sobre menores de edad, se procederá a la protección de los mismos en el tránsito hacia su madurez de una técnica particularmente lesiva para su desarrollo y derechos fundamentales, pero sin privarle del universo *online* al que se encuentra acostumbrado.

4. MONITORIZACIÓN DEL COMPORTAMIENTO DEL MENOR EN REDES SOCIALES A TRAVÉS DE LAS *COOKIES* CON FINES DE PUBLICIDAD COMPORTAMENTAL. LA INSUFICIENCIA DE LA NORMATIVA EUROPEA

La regulación del fenómeno *big data* e IA no se lleva a cabo exclusivamente por la normativa sobre protección de datos personales. En efecto, una de sus múltiples aplicaciones prácticas, como resulta la publicidad comportamental, empleada con el cometido de rastrear el comportamiento *online* de los usuarios- a través de las *cookies*- se regula en cuerpos normativos diferentes al RGPD[678]. Sin embargo, procede conceder un apartado a su estudio, pues se trata de otra técnica para recabar datos que nutre los sistemas de *big data* e IA.

4.1. La personalización de la publicidad basada en el análisis del comportamiento de los usuarios de redes sociales. Nuevas técnicas para la recopilación de datos personales

Los anunciantes de bienes y servicios siempre han tratado de hacer llegar sus mensajes del modo más eficiente posible al público potencialmente interesado. A tal fin, las empresas anunciantes se han decantado por los canales que consideran idóneos en orden a alcanzar la máxima audiencia. Sin embargo, en las últimas décadas, la red ha desplazado buena parte de la audiencia desde los medios de comunicación tradicionales hasta el contexto *online*. En consecuencia, los anunciantes dirigen su atención a Internet,

[678] Tal y como se ha señalado previamente, su regulación se acomete por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores (en adelante, Directiva 2009/136/CE) . Por otra parte, no debemos pasar por alto que, dicha regulación posee acomodo en la norma destinada a la transposición de los textos citados en el Estado español mediante la LSSIE.

ya que, esta herramienta en general y las redes sociales en particular, abren nuevas posibilidades de promoción tanto en la oferta de bienes y servicios, como en el impulso de la imagen de marca.

De este modo, los proveedores de redes sociales y anunciantes han desarrollado nuevas técnicas de marketing, cada vez, con un mayor grado de personalización. A día de hoy, resulta habitual el rastreo de la actividad de los usuarios en Internet a efectos de ofrecerles, con carácter posterior, la publicidad que mejor se acomode a los intereses inferidos de su comportamiento en la red. Esta técnica, que recibe el nombre de publicidad comportamental *online*, se fundamenta en el conocimiento de los hábitos de comportamiento del consumidor en la red con el propósito de ofrecer a éste publicidad personalizada.

Así, el Grupo de Trabajo del Artículo 29 define la publicidad comportamental (*behavioural advertising*) como la publicidad basada en la observación continuada del comportamiento de los individuos que busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento[679].

De dicha definición se desprende que, mientras que la publicidad contextual y la publicidad segmentada se refieren a instantáneas de lo que los usuarios visualizan o llevan a cabo en Internet, la publicidad comportamental puede proporcionar a los anunciantes una imagen muy detallada y precisa sobre la vida en línea del usuario (qué páginas visita, qué anuncios le gustan, cuánto tiempo transcurre en cada página web, etc.). Así las cosas, la recopilación de dichos hábitos de navegación se emplea para la creación de perfiles de cada uno de los usuarios, con el fin de publicitarles bienes y servicios acomodados a sus intereses inferidos de la elaboración de dichos perfiles. Sin embargo, el usuario no habitúa a tomar conciencia sobre esta práctica cuando navega por la red o es usuario de una aplicación en línea, o si lo hace, no conoce su alcance.

Supuesto lo anterior, cabe preguntarse el modo en el que se recaban los hábitos de navegación del usuario en la red. En ese sentido, la técnica de rastreo más empleada

[679] Dictamen 2/2010 Grupo de Trabajo de protección de datos del Artículo 29 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 5.

se corresponde con las *cookies* de rastreo[680]. Estas, se pueden definir como pequeños ficheros de texto alfanuméricos generados por las páginas web que se visitan y que se almacenan en el dispositivo del usuario para su posterior recuperación y lectura de datos recabados[681]. Así, el proveedor de redes de publicidad coloca la *cookie* en el dispositivo del usuario la primera vez que visita un sitio de Internet que exhibe un anuncio de su red. Posteriormente, la *cookie* permitirá al proveedor de publicidad reconocer a un antiguo visitante que vuelve a dicho sitio o visita cualquier otro espacio asociado al proveedor de la red de publicidad. De la reiteración de visitas, el proveedor de la red de publicidad construirá un perfil del visitante que se empleará para diseñar publicidad personalizada.

Concretamente, la técnica de rastreo para la realización de publicidad comportamental se estructura del siguiente modo la luz de lo señalado por PÉREZ BES: inicialmente, el usuario accede a la red a través de un navegador, seguido del acceso a una determinada página web o aplicación que, si forma parte de una red de publicidad, el servidor de esta le enviará e instalará una *cookie* al navegador que el usuario emplea. Seguidamente, el servidor creará un fichero vinculado con la *cookie* instalada en el terminal del usuario en el que la *cookie* incluirá información de la navegación del usuario. Así, de la lectura de dicha *cookie* el servidor de publicidad conocerá paulatinamente los gustos, hábitos y preferencias del usuario. Por último, en virtud de la información recabada, se procederá a la elaboración de un perfil que permita al proveedor de publicidad ofrecer al usuario una publicidad adaptada a este, alineando la información mostrada con sus deseos y necesidades inferidas de la información recabada por la *cookie*[682].

De este modo, la instalación de la *cookie* por parte del proveedor de la red de publicidad, constituye un paso indispensable en orden a recabar los hábitos y comportamiento *online* de las personas usuarias. De su instalación depende la recopilación de datos detallados y precisos sobre los hábitos y gustos de las personas usuarias. Por otra parte, tal y como señala NAVAS NAVARRO, esta técnica también permite, a su vez, una gestión más eficiente de los espacios publicitarios que aparecen en

[680] El término *cookie* apareció por primera vez en 1979 cuando se crea un programa llamado *Fortune cookie*, para el sistema operativo UNIX. Su cometido residía -emulando las galletas de la suerte chinas- en extraer una cita aleatoria para el usuario de una gran base de datos. HOLMES DAWN, E., *Big data: una breve introducción, op. cit.,* p. 91.
[681] APARICIO SALOM, J., Y SANFULGENCIO TOMÉ, S., "El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos", *Revista Aranzadi Doctrinal,* 2014, núm. 11, p. 1.
[682] PÉREZ BES, F., *La publicidad comportamental online, op. cit.*, pp. 24-25.

cada página web, pues los mismos aparecerán personalizados conforme a los gustos y las preferencias de cada específico usuario[683].

Así las cosas, las redes sociales se constituyen como aquel servicio que pone a disposición de los anunciantes un espacio que les permita analizar el comportamiento, gustos y preferencias de los usuarios. Pero no solo eso, las redes sociales además de someter a tratamiento los datos activos y pasivos que los usuarios comparten en su plataforma, también se han propuesto rastrear los hábitos *online* de sus usuarios en orden a personalizar su experiencia en la plataforma. En efecto, los proveedores de redes sociales personalizan sus plataformas y las ajustan a los gustos y preferencias de cada específico usuario, a raíz de los datos almacenados y tratados por medio de las *cookies* instaladas en los terminales de estos.

Con todo, la técnica de rastreo descrita resulta especialmente intrusiva en la privacidad de las personas ya que la creación de estos perfiles tan precisos sobre los usuarios, en la mayoría de los casos implica el tratamiento de datos de carácter personal. Por ello, esta práctica no puede realizarse al margen del derecho a la protección de datos personales.

4.2. La transparencia y el consentimiento previo como garantías jurídicas fundamentales para la instalación de *cookies* con fines de publicidad comportamental

En el año 2009, la UE visibilizó nuevamente su preocupación por los riesgos que el empleo de *cookies* implicaba, tanto para para la intimidad de las personas usuarias de Internet, como para la protección de sus datos personales[684]. Tanto es así que, en ese mismo año, se modificó la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas en orden a dotar de mayor seguridad a los usuarios de estos servicios en el espacio europeo.

[683] NAVAS NAVARRO, S., *La personalidad virtual del usuario en Internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*, Valencia, Tirant lo Blanch, 2015, p. 68.

[684] Desde la vigencia de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, el Considerando 24 ya advertía de la información de los equipos y terminales de los usuarios pertenecía a la esfera privada de los usuarios.

Ello se debe a que, si bien esta técnica nació con un carácter principalmente técnico, consistente en facilitar la prestación del servicio al usuario de Internet, el paso del tiempo evidenció que la instalación de una *cookie* en un dispositivo permitía conseguir utilidades diferentes a la expuesta entre las que destaca la publicidad comportamental[685]. Así, la instalación y lectura de la *cookie,* permite comprender mejor el perfil de cada usuario, lo que garantiza al anunciante la producción de una publicidad verdaderamente personalizada. No obstante, el riesgo para la privacidad resulta patente, dado que el objetivo de la *cookie* se orienta a detectar los gustos y las preferencias del usuario por medio de la observación continuada de sus hábitos de navegación en la red[686].

En consecuencia, el art. 5.3 de la Directiva 2002/58/CE modificada en 2009 quedaba redactado de tal modo que se garantizase que el almacenamiento de información o la lectura de la información ya almacenada en un equipo o terminal de un usuario solamente pudiera practicarse en caso de que este hubiera sido provisto de información clara y completa sobre los fines de dicho tratamiento; pero, además, el usuario también hubiera otorgado un consentimiento al tratamiento de dicha información. Se añadía así en 2009 la preceptividad del consentimiento, que hasta ese entonces no resultaba obligatorio. Con la finalidad de adaptar la normativa nacional mediante la que se traspuso la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, el art. 22.2 de la LSSIE también fue dotado de una nueva redacción a efectos de transponer los nuevos postulados de la Directiva[687].

De la lectura de las señaladas normativas, se desprende que, la misma resulta aplicable a dispositivos de almacenamiento y recuperación de datos personales en cualquiera de los equipos terminales de los destinatarios. Así, las *cookies* se constituyen como mecanismos eficaces para propiciar el almacenamiento y lectura posterior de la

[685] Así, afirma FAQUER RIUTORT que la instalación de *cookies* ya no persigue únicamente mejorar la prestación del servicio, sino que va más allá, pues busca comprender mejor el perfil de los distintos usuarios desde la huella que estos generan con el fin de mejorar los sitios web, aplicaciones productos, servicios y anuncios. FLAQUER RIUTORT, J., "La función publicitaria de las cookies: mecanismos de prevención y cautela en el Derecho español", *THEMIS-Revista de Derecho,* enero-junio 2021, núm. 79, pp. 128-129.
[686] FLAQUER RIUTORT, J., "Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy)", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2018, núm. 47, pp. 4-5.
[687] La transposición de la Directiva se llevó a cabo por medio del por medio del Real Decreto-Ley 13/2012, de 30 de marzo por el que se transponen las directivas en materia de electricidad y gas y en materia de comunicaciones electrónicas y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctricos y gasista, Boletín Oficial del Estado, de 31 de marzo de 2012, núm. 78.

información recabada por esta en los terminales (móviles, ordenadores, *tablets*) en los que se instala; ya que el cometido de este fichero instalado en los terminales reside en proporcionar acceso remoto a la detallada información sobre las vicisitudes de la navegación almacenada en los dispositivos del usuario[688].

No obstante, no todas las *cookies* precisan del consentimiento del interesado. Efectivamente, en virtud de lo manifestado por la AEPD, solamente las *cookies* de análisis y publicidad comportamental precisarían del consentimiento del usuario[689]. Por el contrario, las *cookies* técnicas no requieren del consentimiento, a saber: las *cookies* de entrada de usuario; las de autenticación o identificación del usuario de sesión; las de seguridad del usuario; las de sesión de reproductor de multimedia; las de sesión para equilibrar la carga; las de personalización de interfaz del usuario; y por último, las de complemento o *plug-in* para intercambiar contenidos sociales[690].

Ahora bien, la información recopilada por medio de la instalación y posterior lectura de esta, puede practicarse sobre datos cuyo carácter resulta personal. Es habitual que la lectura de *cookies* facilite la recopilación de datos como cuentas de correo electrónico, nombres, apellidos, etc. Pese a ello, también se pueden recabar datos cuya consideración de dato de carácter personal puede pasar inadvertido. En ese sentido, el Grupo de Trabajo del Artículo 29 ha afirmado que, el fin de la lectura de dichos datos reside en la elaboración de perfiles basados en las características personales de los usuarios para influenciar su comportamiento, para lo que frecuentemente se recurre a vincular la información del usuario proporcionada en la fase de registro. De modo que, en el caso descrito, la normativa sobre protección de datos personales resultaría aplicable. Por otra parte, idéntica conclusión ha alcanzado el organismo europeo sobre la consideración de la dirección IP de los terminales como dato personal[691]. De esta manera,

[688] Sin embargo, en la actualidad, esta tecnología ha sido superada por otras técnicas más avanzadas que al igual que las *cookies*, obtienen la huella digital de los dispositivos de los usuarios. Nos referimos así a las *canvas fingerprinting*, *webRTC* o *audio fingerprint* a las que la Directiva 2002/58/CE resulta de igual aplicación al poseer un cometido idéntico a las *cookies* (almacenar información sobre los dispositivos de los usuarios para su posterior lectura con un alto grado de intrusismo).

[689] Guía sobre el uso de las cookies de la AEPD, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta 1 de julio de 2021), pp. 11-12. Ello se debe a que estas, poseen un carácter permanente, y en muchas ocasiones se instalan por terceros.

[690] Dictamen 4/2012 del Grupo de trabajo del Artículo 29, sobre la exención del requisito de consentimiento de cookies, de 7 de junio de 2012, WP 194, pp. 6-10.

[691] Dictamen 2/2010 del Grupo de Trabajo de protección de datos del Artículo 29 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 10.

la *cookie* almacena y trata la dirección IP, que permite aislar a un usuario del resto, aun desconociendo su identidad, lo que permite identificar a una persona aisladamente de las demás; y en el caso de las *cookies*, atribuirle un haz de informaciones sobre sus hábitos que facilitan la personalización de la publicidad.

La propia AEPD tuvo ocasión en el año 2003 de pronunciarse sobre la consideración de la dirección IP como dato de carácter personal a través del Informe 327/2003, en el que afirma que por medio de la dirección IP cabe la posibilidad de que se termine identificando al usuario (especialmente en los casos en los que se emplean técnicas invisibles para el usuario como las *cookies* y minería de datos). Por ello, las direcciones IP se consideran datos de carácter personal a las que habrá de aplicarse la normativa sobre protección de datos personales[692]. En ese sentido, recordemos que también el TS ha calificado las direcciones IP como datos personales, ya que contienen información concerniente a personas físicas identificadas o identificables[693]. Este criterio ha sido igualmente sostenido por el TJUE al afirmar que todos los proveedores de servicios de medios en línea pueden llegar a identificar a las personas físicas a través de las direcciones IP. Es más, a día de hoy, la identificación de una persona física resulta posible por medio de datos de búsquedas, webs visitadas y hábitos *online* de este, de modo que, resulta más actualizado referirse a lo que el TJUE califica de "doctrina del perfil"[694]. A decir verdad, las técnicas tan avanzadas de *big data* e IA permiten una identificación de las personas incluso sin la necesidad de recabar la dirección IP. En definitiva, la probabilidad de tratar datos personales al cruzar los datos disponibles resulta evidente.

Véase que el propio RGPD toma conciencia de ello en el Considerando 30 cuando dispone que las personas físicas pueden asociarse a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de Internet, identificadores de sesión en forma de *cookies* u otros

[692] Para mayor detalle, consultar el Informe 327/2003 de la AEPD sobre el carácter de dato personal de la dirección IP. Obtenido de: https://www.aepd.es/es/documento/2003-0327.pdf (última fecha de consulta el 1 de julio de 2021).
[693] Consúltese al respecto la Sentencia del Tribunal Supremo 3896/2014, Sala 1ª de lo Civil, de 3 de octubre de 2014 (rec. 6153/2011) FJ 4º y la Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de octubre de 2016, *Patrick Breyer y Bundesrepublik Deutschland*, Asunto C-582/14, aptdos. 47 a 49.
[694] Sentencia del Tribunal de Justicia de la Unión Europea, de 21 de diciembre de 2016, *Tele2 Sverige AB y Post-och telesty- relsen y Secretary of State for the Home Departament y otros*, Asuntos acumulados C-203/15 y C-698/15, aptdo. 99 y Sentencia del Tribunal de Justicia de la Unión Europea, de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros*, Asuntos acumulados C-293/12 y C-594/12, aptdo. 27.

identificadores. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden empelarse para la elaboración de perfiles de las personas físicas e identificarlas. En definitiva, en un contexto de *big data* e IA, gran parte de las instalaciones y posteriores lecturas de *cookies* supondrán el tratamiento de datos de carácter personal, por lo que, la normativa sobre protección de datos personales gozará, igualmente, de plena aplicabilidad.

Así las cosas, cuando la utilización de una *cookie* conlleva el tratamiento de datos personales, los responsables del tratamiento deberán cumplir las exigencias adicionales establecidas por la normativa sobre protección de datos personales. Lo destacado hasta ahora, nos conduce a visibilizar que en el marco normativo aplicable a la publicidad comportamental convergen dos normativas a saber: la Directiva 2009/136/CE por la que se modifica la 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y la normativa sobre protección de datos personales[695].

Sentado cuanto antecede, el art. 5.3 de la Directiva 2009 /136/CE y el art. 22.2 LSSIE prevén dos obligaciones principales con el fin de garantizar al usuario el poder de controlar sus datos de navegación. Por un lado, en tanto en cuanto los usuarios no acostumbran a conocer el alcance de la técnica practicada, la normativa regula el deber de informar al usuario sobre el empleo de *cookies*, así como de la finalidad de tratamiento por medio de las mismas que, a su vez, deberá cumplir con las exigencias de los arts. 12 y 13 RGPD. Por otro lado, debe concederse un consentimiento expreso por parte del usuario y con carácter previo la instalación de las *cookies* en los dispositivos de los usuarios que concuerde, asimismo con el arts. 4.11 y 6.1.a) RGPD. Esto es, a rasgos generales, el usuario debe poder conocer el empleo de dicha técnica, así como el alcance

[695] No obstante, resulta preciso realizar una serie de consideraciones al respecto. En primer lugar, la normativa sobre protección de datos personales se aplicará al empleo de *cookies* o instrumentos similares cuando la Directiva 2009 /136/CE no prevea disposiciones específicas para garantizar la protección de derechos y libertades fundamentales. Efectivamente, la *lex specialis* primará sobre la *lex generalis*; en segundo lugar, la aplicación de la normativa sobre protección de datos personales incluye la aplicabilidad de las obligaciones del responsable del tratamiento y los derechos de las personas. Así las cosas, el empleo de *cookies* con fines de publicidad comportamental deberá ajustarse, por una parte, a lo establecido en el art. 5.3 de la Directiva 2009 /136/CE; por otra parte, resultarán igualmente aplicables las disposiciones del RGPD. Véase el Considerando 10 de la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), Diario Oficial de la Unión Europea, L 108/51, de 24 de abril de 2002 modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE.

y objetivos de la misma, al tiempo de consentir el uso de la misma sobre sus dispositivos de manera previa a su práctica.

Así las cosas, la determinación sobre la información a proporcionar al usuario, así como el modo en el consentimiento debe prestarse, constituyen cuestiones prejudiciales resueltas por el TJUE en la Sentencia, de 1 de octubre de 2019[696]. En concreto, el TJUE afirma que, a pesar de que la Directiva 2002/58/CE no contiene indicación alguna sobre el modo en que debe prestarse el consentimiento a la instalación de la *cookie*, estima que de la interpretación literal del art. 5.3 de la señalada normativa, se deduce que es precisa una acción del usuario. Es más, el Considerando 17 de la propia Directiva 2002/58/CE citada anteriormente, dispone que el consentimiento del usuario debe corresponderse con el consentimiento que prevé la normativa sobre protección de datos personales (en la actualidad el RGPD). Por lo tanto, el consentimiento ha de configurarse como una manifestación de voluntad libre, específica, informada e inequívoca del interesado, que ha de adoptar la forma de declaración o una clara acción afirmativa[697]. Así, en la autorización al almacenamiento de información o acceso a la misma mediante la instalación de una *cookie* por medio de una casilla marcada por defecto, no puede considerarse un consentimiento válido que reúna las señaladas características.

El Grupo de Trabajo del Artículo 29 ya en el año 2010 informaba de manera más específica y concreta sobre las características del consentimiento del usuario para la instalación de *cookies* con fines de publicidad comportamental citada en reiteradas ocasiones del presente estudio. Como resultado, el organismo europeo apuntaba que el consentimiento ha de presentar un carácter previo, esto es, ha de recabarse antes de proceder a la instalación de la *cookie* siempre que se haya informado de manera clara y sencilla al usuario sobre la identidad, fines y cualesquiera otras informaciones necesarias

[696] Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de octubre de 2019, *Planet49*, Asunto C-673/17. La Sentencia señalada resuelve la cuestión prejudicial planteada por el Bundesgerichtshof (Tribunal Supremo de lo Civil y Penal alemán) en el seno del procedimiento iniciado por la Federación alemana de consumidores contra la empresa Planet49. Esta última, organizó un juego con fines promocionales en el dominio de Internet www.dein-macbook.de el 24 de septiembre de 2013, en el que los internautas debían introducir su nombre y dirección, así como marcar una casilla para consentir el tratamiento de datos personales y otra que, marcada previamente, consentía la instalación de una *cookie* en el dispositivo de los usuarios. En ese sentido, el TS alemán se preguntaba sobre la interpretación del art. 5.3 de la Directiva 2002/58/CE en lo referente al modo de prestar el consentimiento para su validez, así como si el tiempo durante el cual las *cookies* se encontrarían activas ha de considerarse una información obligatoria en orden a cumplir el deber de información exigido para la prestación de un consentimiento informado.

[697] El CEPD también afirma en sus Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020, citado en ocasiones anteriores, que las condiciones para la obtención de un consentimiento válido establecidas en el RGPD resultan de aplicación en las situaciones que entran en el ámbito de aplicación de la Directiva sobre privacidad y comunicaciones electrónicas, p. 11.

para garantizar un tratamiento leal. Por otra parte, incluso disponía que no puede considerarse consentimiento válido la configuración del navegador que, por defecto, permita la instalación de *cookies* y requiera de la acción del usuario para desactivar dicha función.

El organismo europeo muestra igual rechazo por las técnicas que conceden al usuario el derecho a excluir voluntariamente este tipo de publicidad, en tanto en cuanto, este en muchas ocasiones no conoce el modo en el que puede ejercitar dicho derecho, y lo que consideramos de mayor relevancia, se diseña como un sistema que se basa en la inacción del usuario para la instalación de la *cookie*, debiendo el usuario rechazar su instalación una vez ya ha ocurrido. Sin lugar a dudas, esta técnica no resulta compatible con las premisas instauradas por la Directiva. Por último, se decanta por los mecanismos de aceptación previa del usuario, en los que debe probarse un acto explícito del usuario que exprese su consentimiento antes de que se envíe la *cookie* al dispositivo[698].

Volviendo a la Sentencia del TJUE señalada, el tribunal europeo afirma que la Directiva 2002/58/CE igualmente guarda silencio sobre la información que ha de proporcionarse al usuario a la hora de solicitar su consentimiento en la instalación de la *cookie*. Así, en orden a garantizar una información clara y completa sobre la instalación de la *cookie*, esta debe determinar las consecuencias del consentimiento de manera comprensible y suficientemente detallada. De suerte que, además de identificar a las entidades que recopilarán dicha información y las finalidades para las que se recabará, habrán de facilitarse cualesquiera otras informaciones en la medida que dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado. En el caso que se resuelve mediante la Sentencia citada, la

[698] Las señaladas Directrices del CEPD 5/2020, obligaron a la AEPD a cambiar su doctrina sobre el modo de prestar el consentimiento a la instalación de las *cookies*. Efectivamente, la AEPD aceptaba como válida la función "seguir navegando" del usuario como forma de prestar el consentimiento por parte de los usuarios para su instalación. Sin embargo, tras las Directrices del organismo europeo, así como la sentencia del TJUE sobre el asunto *Planet 49* citada recientemente, este mecanismo debía descartarse. Para más detalle, véase RODRÍGUEZ DUARTE, L., "Cookies: consentimiento, su revocación y Reglamento E-privacy", *Derecho Digital e Innovación (La Ley Digital)*, tercer trimestre 2020, núm. 6, p. 5. A mayor abundamiento, la AEPD se posicionaba como el único organismo defensor de este mecanismo, ya que, las guías de países europeos homólogas, mostraban su rechazo a este modo de otorgar el consentimiento. Véanse así, la Guía de la CNIL francesa, de 4 de julio de 2019, *Délibération núm. 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif).* Obtenido de: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337 (última consulta el 8 de febrero de 2023); o la Guía sobre *cookies* de la Conferencia de Autoridades Independientes de protección de datos de los gobiernos federales y estatal alemán, de marzo de 2019. Obtenida de: 20190405_oh_tmg.pdf (datenschutzkonferenz-online.de) (última consulta el 8 de febrero de 2023).

información relativa al tiempo durante el cual las *cookies* se encontrarán activas responde a la exigencia de un tratamiento de datos leal, dado que un período prolongado o incluso ilimitado de rastreo implica la recogida de numerosos datos sobre los hábitos de navegación del usuario.

Resulta evidente, que la Sentencia del TJUE no muestra un grado elevado de detalle sobre la información concreta que ha de proporcionarse al usuario, de modo que, consideramos conveniente añadir que la AEPD detalla en la referida Guía sobre el uso de *cookies*[699], tanto la información que mínimamente debe recibir el usuario como el modo en el que ha de mostrarse dicha información. En este sentido, con la Guía de la AEPD como base, la información que habrán de facilitar, en nuestro caso, las redes sociales *online* como editores, así como el modo en el que habrán de compartirla con el usuario presenta una serie de deficiencias de entidad relevante cuyo detalle se expone como sigue en el presente estudio. A estos efectos, informa la AEPD que, los editores deberán incluir la siguiente información de conformidad con lo dispuesto en el art. 13 RGPD[700]:

En primer lugar, deberán ofrecer una definición de las *cookies*, así como la función genérica de estas. Es cierto que, las redes sociales acostumbran a proporcionar dicha definición, aunque por ejemplo, en el caso de la red social Instagram, se define con vaguedad la función para la que estas sirven[701]. En cambio, podemos hallar redes sociales como TikTok que, por el contrario, sí definen correctamente y aclaran en mayor medida la función genérica de esta técnica[702].

En segundo lugar, establece la AEPD que los editores habrán de informar sobre los tipos de *cookies*, así como la finalidad de cada una de ellas. Lamentablemente, sobre este extremo, gran parte de las políticas de *cookies* de redes sociales, entre las que destaca, por ejemplo, la política de privacidad del Grupo Meta, no realizan un esfuerzo suficiente en determinar cada una de las finalidades aparejada a la *cookie* correspondiente. En tal sentido, la red social se limita a expresar genéricamente alguna de las finalidades para las que dicha técnica se emplea, pero en ningún caso dispone la finalidad para cada una de

[699] Guía sobre el uso de las cookiesde la AEPD, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta 30 de junio de 2021)
[700] Guía sobre el uso de las cookies de la AEPD, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta el 30 de junio de 2021), pp. 15-22.
[701] Política de privacidad de la red social Instagram: https://help.instagram.com/1896641480634370?ref=ig (última consulta el 10 de enero de 2023).
[702] Política de privacidad de la red social TikTok: https://www.tiktok.com/legal/tiktok-website-cookies-policy?lang=es (última consulta 30 de junio de 2021).

las múltiples *cookies* empleadas. Es más, tampoco establecen cada uno de los tipos de *cookies* empleadas por la plataforma. Consecuentemente, el consentimiento prestado por el usuario en estas circunstancias, no se constituye como un consentimiento prestado para cada una de las finalidades de tratamiento (arts. 5 y 13 RGPD) de modo que, carece de validez. Por el contrario, destacando nuevamente la política de privacidad de la red social TikTok, esta sí que aclara cada una de las *cookies* empleadas por la plataforma, así como la finalidad o el destino de uso de cada una de ellas. Por ello, modelos como el de la red social TikTok podrían resultar de utilidad para el resto de proveedores de redes sociales a efectos de adaptar sus políticas de *cookies* a los postulados del RGPD.

En tercer lugar, las plataformas deberán identificar quién utilizará las *cookies* en caso de que no se empleen exclusivamente por el editor. La totalidad de las redes sociales nutren sus ingresos de la publicidad que muestran en sus espacios, para lo que se emplean técnicas de publicidad comportamental a través de las *cookies* de rastreo, por ello, resulta habitual que también empleen *cookies* de terceros. Esto es, terceros colaboradores podrán acceder a la información almacenada en la *cookie* previamente instalada en los dispositivos de los usuarios. En este caso, la AEPD afirma, que se deberá informar al usuario de dicha circunstancia, además de brindar la posibilidad de conocer a los terceros que accederán a la información de sus dispositivos. Preocupa considerablemente que las redes sociales no acostumbran a informar sobre la identidad de estas terceras entidades, de modo que, el usuario no posee la capacidad de conocer quién accederá a información tan detallada como sus gustos o hábitos de navegación, ocasionando ello una pérdida acusada de control sobre sus datos personales. A mayor abundamiento, acertadamente señala APARICIO SALOM, que se constituye esta como una tarea prácticamente imposible, ocasionada, por una parte, por el elevado número de terceros colaboradores; por otra parte, por la imposibilidad del proveedor de prever de antemano los mismos[703].

En cuarto lugar, la política de *cookies* deberá proveerse de la información para aceptar, denegar o revocar el consentimiento. Si bien es cierto que este aspecto tiende a informarse, el mecanismo ofrecido por los proveedores de redes sociales para la puesta en práctica de la revocación dista considerablemente del proporcionado para consentir la instalación. Principalmente, el usuario debe acudir a los ajustes de su navegador para

[703] APARICIO SALOM, J., Y SANFULGENCIO TOMÉ, S., "El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos", *op, cit*, p. 17.

retirar el consentimiento previamente concedido al darse de alta en la red social. A nuestro juicio, esta dificultad provoca no en pocas ocasiones el desistimiento por parte del usuario en la revocación del consentimiento.

Por último, debemos señalar tres menciones de crucial relevancia en las políticas de *cookies* al fin de garantizar al usuario un poder de control sobre sus datos, no se articulan en las políticas de *cookies* de las redes sociales, a saber: no advierten sobre la transferencia de datos a otros países de los datos recabados por las *cookies*, tampoco informan sobre la elaboración de perfiles con los datos recabados, conducta que, deviene indispensable para el correcto funcionamiento de la publicidad comportamental, tal y como ha quedado claro en apartados precedentes; y por último, algunas de las plataformas no advierten sobre el plazo de conservación de cada una de las *cookies* empleadas[704].

Sobre este último aspecto, recordemos que un plazo indefinido puede resultar contrario a un tratamiento leal de datos personales tal y como dispuso el TJUE en el asunto *Planet49* citada con anterioridad[705]. Efectivamente, no informar al usuario sobre el plazo en el que la *cookie* permanecerá instalada almacenando información sobre los hábitos de navegación del usuario, colisiona con el art. 13.1 apartado a) del RGPD que exige facilitar al interesado la información sobre el plazo durante el cual se conservarán los datos personales en aras de garantizar un tratamiento leal.

A propósito del plazo, también conviene señalar que los usuarios con el tiempo pueden olvidar que su actividad se somete a control por parte de los proveedores de servicios *online*. Por consiguiente, el Grupo de Trabajo del Artículo 29 establece que los proveedores de este tipo de servicios deben buscar el modo de informar periódicamente a las personas de este rastreo. Para dicho cometido, nos parece de especial interés la iniciativa impulsada por el organismo europeo consistente en añadir un icono que alertara a los usuarios que un proveedor de servicios se encuentra controlando sus búsquedas para enviar publicidad a medida. De este modo, el usuario podría no solo recordar dicha

[704] Sirva como ejemplo, que la política de privacidad de Instagram dispone que "El tiempo que una cookie permanece en un ordenador o dispositivo varía en función de si se trata de una cookie permanente o de sesión. Las cookies de sesión sólo permanecen en tu dispositivo hasta que finalices tu navegación. Sin embargo, las permanentes se conservan en el ordenador o dispositivo móvil hasta que caducan o se eliminan". Obtenido de la Política de privacidad de la red social Instagram: https://help.instagram.com/1896641480634370?ref=ig (última consulta el 10 de enero de 2023).
[705] Segunda cuestión prejudicial de la Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de octubre de 2019, (caso *Planet49*).

circunstancia, sino también valorar si desea continuar prestando su consentimiento, o por el contrario, revocarlo[706].

En otro orden de consideraciones, la AEPD también se ha manifestado sobre el modo en el que la información debe mostrarse en las políticas de *cookies*[707]. Así, al igual que para el caso de las políticas de privacidad, la información debe resultar concisa, transparente e inteligible. Sobre este aspecto, hemos de puntualizar una serie de consideraciones. En primer lugar, las comunicaciones de políticas de *cookies* habrán de mostrarse de modo sucinto para evitar la fatiga o el cansancio y desistimiento del usuario de su lectura. Es cierto que, políticas de *cookies* se configuran con mayor brevedad que las políticas de privacidad; no obstante, los principales problemas se presentan con el grado de transparencia e inteligibilidad, habida cuenta de que en las redes sociales prolifera la participación de menores de edad, el lenguaje empleado no se acomoda al grado de conocimiento que estos pueden poseer[708].

Con todo, se puede apreciar que las carencias que presentan las políticas de *cookies* resultan similares a las que sufren las políticas de privacidad. En consecuencia, en orden a no resultar reiterativos, como propuestas de mejora remitimos a las consideraciones realizadas sobre las políticas de privacidad en capítulos precedentes de la presente investigación.

En otro orden de ideas, ha quedado de manifiesto que el consentimiento a la instalación de las *cookies* ha de consistir una clara acción afirmativa por parte del usuario. Pese a ello, los mecanismos de obtención del consentimiento válidos pueden resultar variados dependiendo del tipo de página o aplicación de que se trate según dispone la AEPD[709]. Sin embargo, el presente estudio se centra en aquellas modalidades que pueden

[706] Dictamen 2/2010 del Grupo de trabajo del Artículo 29 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 20.

[707] Guía sobre el uso de las cookies de la AEPD, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta el 30 de junio de 2021), pp. 17-22.

[708] Recuérdese que al amparo del considerando 70 las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020, el responsable del tratamiento habrá de valorar el público que proporciona datos a su organización. Por ejemplo, en el caso de audiencias menores de edad, el lenguaje debe resultar comprensible para dicho grupo.

[709] Guía sobre el uso de las cookies de la AEPD, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta el 30 de junio de 2021), p. 25.

resultar de utilidad para los proveedores de redes sociales por encontrarse en directa relación con el objeto de la presente tesis doctoral.

Así las cosas, redes sociales como Instagram, al momento del registro, solamente contemplan la posibilidad de aceptar las *cookies* para permitir continuar con la fase de registro. Cierto es que informan sobre el modo en el que las *cookies* pueden eliminarse a través del navegador; sin embargo, no conceden al usuario la posibilidad de elegir la aceptación o rechazo de instalación de *cookies* previo al registro[710]. Consecuentemente, el consentimiento carece de la libertad requerida por el RGPD, en el sentido que, genera en los usuarios la percepción de que deben aceptar las *cookies* para poder continuar con el alta en el servicio[711]. A mayor abundamiento, la plataforma no permite descargar la política de privacidad sin la aceptación de la política de *cookies*. Sobre este particular, el Supervisor Europeo de Protección de Datos, considera que no debe condicionarse a los individuos el acceso a los espacios web, forzándolos a consentir el rastreo de sus actividades *online*[712]. En efecto, el propio CEPD ha sentado que, únicamente en determinados supuestos se justifica que el rechazo de las *cookies* pueda aparejar la privación de la utilización del servicio. Ello podrá ocurrir siempre que se informe adecuadamente al respecto al usuario y además se le ofrezca una alternativa de acceso sin necesidad de aceptar el uso de las *cookies*, que deberá ofrecerse de manera genuinamente equivalente al servicio prestado mediante el empleo de estas[713]. Como cabe esperar, los proveedores de redes sociales no ofrecen alternativa alguna.

Por todo lo expuesto, el consentimiento actual a la instalación de *cookies* y dispositivos similares, carece de validez conforme a las normativas que le resultan de aplicación a saber: de un lado la Directiva 2009 /136/CE sobre privacidad, de otro lado,

[710] Sin embargo, recordemos que este modo de prestar el consentimiento ha sido descartado por el Grupo de Trabajo del Artículo 29 en su Dictamen 2/2010 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 7.

[711] Es más, los propios proveedores de redes sociales advierten en las políticas de *cookies* que el funcionamiento del servicio no resultará el mismo en caso de rechazar la instalación de estas. Ello acrecienta en el usuario la sensación de obligatoriedad en la prestación del consentimiento. Si bien es cierto que la conducta descrita no se identifica con lo que el CEPD califica como "*cookie walls*" en su Dictamen 5/2020 citado en reiteradas ocasiones- consistente en denegar el acceso al servicio en caso de rechazo de las *cookies*- el modelo diseñado por los proveedores de redes sociales continúa produciendo un efecto similar en el usuario a la hora de prestar el consentimiento.

[712] Opinión 6/2017 del Supervisor Europeo de Protección de Datos, sobre la propuesta de regulación sobre la privacidad y comunicaciones electrónicas (e-privacy), de 24 de abril de 2017. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf (última consulta el 8 de febrero de 2023), pp. 21-22.

[713] Directrices del Grupo de Trabajo del Artículo 29, sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259 modificadas por las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020.

el RGPD. cambio, tal y como señala CABALLERO TRENADO, el consentimiento constituye una base fundamental para la licitud de la instalación de *cookies* que debe configurarse con carácter previo a la instalación del archivo y de modo respetuoso con el RGPD[714].

Concretamente, los mayores obstáculos se presentan con la adaptación de los principios de transparencia y consentimiento instaurados por la normativa europea vigente en lo que se refiere a la protección de datos personales. Fundamentalmente, las políticas de *cookies* carecen de la transparencia exigida por el RGPD, además, la información proporcionada por muchas de estas plataformas, no cumple con los requerimientos mínimos exigidos. Finalmente, el modo de recabar el consentimiento de varios de los proveedores de redes sociales, tampoco cumple con los postulados de la normativa vigente en aras de considerar el mismo válido. En definitiva, se debe imponer a los proveedores de redes sociales y demás agentes implicados, el cumplimiento de la normativa en relación a la instalación y posterior lectura de *cookies*, de lo contrario, se permite una evidente intromisión en la privacidad de las personas usuarias de estos servicios.

4.3. A propósito de una nueva regulación en el empleo de *cookies*: la propuesta del Reglamento comunitario sobre privacidad y las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (e-privacy)

Consciente de las carencias que presenta la normativa actual sobre la instalación y posterior lectura de *cookies* en orden a garantizar la intimidad y la protección de datos personales de los usuarios, el 1 de octubre de 2017 la Comisión Europea da a conocer la primera Propuesta de Reglamento sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)[715].

[714] CABALLERO TRENADO, L., "*Cookies* y consentimiento", *Revista Crítica de Derecho Inmobiliario,* 2020, núm.781, p. 3234.

[715] Propuesta de Reglamento de la Comisión Europea sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), de 1 de octubre de 2017, COM (2017) 10 final.

Así, la Exposición de motivos de la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas, señala que la norma relativa al consentimiento destinada a proteger la confidencialidad de los equipos terminales, no ha logrado alcanzar sus objetivos por cuanto que los usuarios finales pueden acceder a la instalación de *cookies* de rastreo sin comprender lo que ello significa, e incluso en algunos casos, pueden verse expuestos a *cookies* instaladas sin su consentimiento. Por ello, la Comisión Europea propone una nueva regulación para el uso de *cookies* y tecnologías similares por medio de los arts. 8 a 11 del texto.

Si bien es cierto que el legislador europeo procura subsanar varias de las carencias de las que ha adolecido la normativa sobre *cookies* en este texto, no todas las novedades propuestas podían calificarse de loables, a nuestro juicio[716]. En concreto, a pesar de que el consentimiento continúa posicionándose como eje central que permite el empleo de la técnica de rastreo a través de las *cookies*, el modo de configurar el mismo propuesto por la Comisión Europea difiere considerablemente del vigente hasta la fecha[717].

En ese sentido, la Propuesta de Reglamento sobre privacidad y comunicaciones electrónicas apuesta por un sistema en el que, a partir de la configuración del navegador, el usuario pueda elegir el grado de rastreo que se encuentra dispuesto a tolerar sin verse expuesto de manera continua a la aparición de advertencias sobre la aceptación de la política de *cookies* en cada sesión[718]. En esencia, los programas deberían ofrecerse al usuario, con la configuración, por defecto, con el grado de privacidad más alto posible en lo que respecta a la instalación y posterior lectura de dispositivos de rastreo como las *cookies*, sin perjuicio de que el usuario pueda modificar dicha configuración en cualquier momento a una más permisiva con la instalación de *cookies*.

Ahora bien, este modo de configurar el consentimiento presenta nuevas dificultades en la práctica. Ciertamente, creemos que los usuarios a la hora de reconfigurar el navegador o el programa para permitir la instalación de *cookies*, pueden no resultar plenamente conscientes del alcance del rastreo que implica la instalación de

[716] Destacan positivamente los esfuerzos por imponer una clara acción afirmativa del usuario como consentimiento válido o dotar de mayor claridad las exenciones al consentimiento.
[717] Es más, tal y como afirma ORTÍZ LÓPEZ, las características y forma de recabar el consentimiento se han constituido como uno de los debates más intensos en el desarrollo de las propuestas. ORTÍZ LÓPEZ, P., "El Reglamento de e-privacy", *Diario La Ley*, 2021, núm. 8, p. 4.
[718] El considerando 23 de la propuesta del Reglamento e-privacy dispone que los usuarios deberán elegir entre distintos niveles de privacidad, desde el nivel más elevado (por ejemplo, no aceptar nunca *cookies*) hasta el nivel más bajo (por ejemplo, aceptar *cookies* siempre), pasando por el nivel intermedio (por ejemplo, rechazar *cookies* de terceros o solo aceptar *cookies* de origen).

una *cookie*, especialmente en los casos en los que la obtención de dicha información deviene imprescindible ante la gratuidad de los servicios digitales. Precisamente, para que dicho modo de prestar el consentimiento se considere idóneo conforme a la normativa sobre protección de datos personales, la información proporcionada por los proveedores ha de configurarse de modo completo y claro, no opaco como acostumbra a resultar.

Por otra parte, a la posible falta de acierto en la elección de la configuración del navegador, se debe agregar que los usuarios no acostumbran a cambiar los ajustes de privacidad con carácter posterior a la instalación de las aplicaciones o navegadores; de este modo, es posible que incluso olvide que dicha instalación se lleva a cabo sobre su información, incumpliendo este modo de prestar el consentimiento la lealtad requerida en el tratamiento de datos personales. Por ello, habrán de desarrollarse mecanismos para la prestación del consentimiento que adviertan al usuario de que su actividad se somete a control[719]. Es más, el propio Grupo de Trabajo del Artículo 29 ya tuvo ocasión de rechazar este tipo de consentimiento a través de la configuración del navegador en su Dictamen 2/2010 sobre publicidad comportamental, citado en reiteradas ocasiones[720]. Ciertamente, este modo de recabar el consentimiento no respeta el art. 4.11 RGPD.

En adición a lo expuesto, una elección de privacidad excesivamente preservadora de la privacidad, puede acabar por perjudicar la principal fuente de financiación de los contenidos y servicios digitales. Adviértase que, muchas de las *cookies* empleadas en la actualidad a efectos de rastrear los gustos y hábitos de los usuarios con fines de publicidad comportamental, quedarían vetadas por medio de la configuración del navegador, acarreando una considerable disminución de los ingresos publicitarios. Precisamente esta circunstancia, genera desconfianza sobre la verdadera implementación de opciones de configuración de privacidad realmente garantistas con la intimidad y datos personales por parte de las empresas que basan su rentabilidad en este negocio[721].

De conformidad con FLAQUER RIUTORT, la solución propuesta por la Comisión Europea beneficiaría únicamente a grandes compañías como Google, Amazon,

[719] Sobre este punto recordemos que puede considerarse una buena práctica insertar un icono en la publicidad que advierta al usuario de que su actividad está siendo sometida a rastreo o que informe a este del motivo por el que dicho anuncio le es mostrado.

[720] Dictamen 2/2010 Grupo de Trabajo de protección de datos del Artículo 29 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171, p. 15.

[721] Justamente por ello, la mayoría de navegadores configura, por defecto, sus servicios para aceptar *cookies*. AVIÑÓ BELENGUER, D., "El uso de cookies de publicidad comportamental desde la óptica de la protección de datos", *op. cit.*, p. 19.

Facebook y Apple, por cuanto que estas disponen de una mayor facilidad para recabar el consentimiento de sus usuarios, y acceder a sus datos personales sin necesidad de depender de la instalación de *cookies* en sus dispositivos[722]. En efecto, estas empresas privadas poseen la capacidad de seguir aplicando la técnica del *big data* e IA en sus estrategias publicitarias sin necesidad de emplear las *cookies* como medio de recogida de datos para desvelar los hábitos y gustos de los usuarios. Consecuentemente, la novedad introducida por la Comisión Europea[723], consideramos que agravaría en mayor medida los riesgos para la privacidad de los usuarios de redes sociales, pues estos proveedores de redes sociales, al verse como principales recabadores de información personal en este nuevo contexto, desarrollarían técnicas más precisas e intrusivas en orden a continuar recabando y compartiendo datos personales y hábitos de sus usuarios con fines lucrativos.

En definitiva, si bien encontramos voces doctrinales, entre las que destaca POLO ROCA, que alaban la propuesta de Reglamento en relación a las novedades que prevé respecto al consentimiento, no compartimos dicho parecer por las razones expuestas anteriormente[724]. La manera en la que propone configurar la solicitud del consentimiento, así como el incumplimiento reiterado de las obligaciones al respecto por los responsables de la instalación de dichos dispositivos, refuerzan dicha desconfianza, ya que supondría confiar en la buena fe de una industria cuyo interés en muchas ocasiones resulta contrario a los derechos y libertades fundamentales de los usuarios.

Por otra parte, la Propuesta de reglamento no menciona el consentimiento a la instalación de *cookies* o dispositivos similares otorgado por menores de edad. Es cierto que, el texto somete las exigencias del consentimiento al RGPD; sin embargo, consideramos que una mención al consentimiento de la instalación y posterior acceso a la *cookie* cuando el dispositivo es titularidad de un menor de edad o en aquellas webs orientadas a usuarios jóvenes, resultaba necesaria[725]. Ello se debe, principalmente, a que

[722] FLAQUER RIUTORT, J., "Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy), *op. cit.*, p. 32.
[723] En ese sentido, la Comisión Europea vuelve a fomentar la prestación del consentimiento por medio del navegador en el Informe sobre la Propuesta de Reglamento de la Comisión Europea sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), de 20 de octubre de 2017. Obtenido de: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_ES.html (última consulta el 18 de abril de 2013).
[724] POLO ROCA, A., "Geolocalización, motores de búsqueda y cookies: tres grandes retos para la protección de datos", *Revista jurídica de Castilla y León,* 2020, núm. 52, p. 182.
[725] Véase que el art. 9.1 de la Propuesta de Reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy), dispone que serán de aplicación las condiciones previstas en los

este nuevo sistema no arroja claridad a la hora de verificar la edad del menor, lo que imposibilita considerar válidos los consentimientos emitidos por personas cuya edad no supere los 14 años de edad. Idéntica conclusión podríamos aplicar a la configuración del navegador por personas que no alcancen la edad descrita, en el sentido que, estas no poseen la madurez suficiente para comprender el alcance del empleo de dicha práctica sobre su información personal.

Además, la verificación de la edad en el presente supuesto adquiere especial relevancia, por cuanto que tanto el CEPD como la AEPD recomiendan a los editores abstenerse de la instalación de *cookies* de publicidad comportamental dados los patentes riesgos que esta técnica puede conllevar en menores[726]. Por el contrario, la nueva normativa tampoco prevé una solución que permita una aplicabilidad efectiva de dichas restricciones cuando el usuario es un menor de edad. Consecuentemente, los menores resultan víctimas de estas técnicas intrusivas en la privacidad a diario cuando acceden a redes sociales. Queda de manifiesto pues, que la verificación de la verdadera edad del menor se posiciona como una necesidad de primer orden a efectos de garantizar la salvaguarda de sus datos con fines de publicidad comportamental. Solamente en caso de poder autentificar la edad del menor, podrán impedirse este tipo de prácticas sobre datos y hábitos de navegación de usuarios vulnerables. En definitiva, estimamos que, habida cuenta de los riesgos que genera para la privacidad del menor el empleo de esta técnica de rastreo con fines comerciales, debería prohibirse la instalación de *cookies* en todo momento cuando el titular del dispositivo no alcance la mayoría de edad.

5. EL TRATAMIENTO DE DATOS PERSONALES EN REDES SOCIALES A PARTIR DE LA INTELIGENCIA ARTIFICIAL. UN NUEVO DESAFÍO LEGISLATIVO

Parece que la práctica de tratamientos de datos basados en sistemas de *big data* e IA se ha establecido con carácter permanente en el presente siglo. En efecto, la llegada

arts. 4.11 y 7 del RGPD relativas al consentimiento. Sin embargo, no se remite al art. 8 RGPD sobre las condiciones del consentimiento prestado por menores de edad.

[726] Dichas conclusiones se alcanzan por el CEPD en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a efectos del RGPD citado en reiteradas ocasiones, así como por la AEPD en la Guía sobre el uso de las cookies, de julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta el 30 de junio de 2021), p. 28.

de la IA ha revolucionado de un modo sin precedentes el modo de otorgar valor a los datos disponibles en la actualidad. En paralelo, la irrupción de sistemas basados en IA, ha generado nuevos riesgos para los derechos fundamentales de las personas. Si bien es cierto que el empleo de estos sistemas resulta beneficioso para la sociedad, su desarrollo e implementación han de redundar, en todo caso, en beneficio de la humanidad.

5.1. Los principios y valores que deben inspirar el desarrollo de la IA

Así las cosas, parece el momento oportuno para encauzar una reflexión, desde una perspectiva jurídico-ética, sobre el diseño, despliegue y funcionamiento de estos sistemas. Dado que nadie cuestiona los innumerables beneficios que la IA aporta en diversos sectores económicos, su aplicación ha de guiarse por el máximo respeto a los derechos de las personas a las que la señalada técnica sirve. Como hemos comprobado, las prácticas actuales no siempre priorizan correctamente la premisa señalada, lamentablemente.

De este modo, sobre esta cuestión ha de recordarse que la posibilidad de que la técnica permita la práctica de determinados tratamientos, no conlleva implícito que su implementación obedezca a razonamientos éticos. En ocasiones, determinadas decisiones deben presidirse, no desde el deseo exclusivo de potenciar el avance tecnológico, sino desde la defensa de los derechos fundamentales de la persona. Desde la misma aparición de Internet, el ser humano ya supo anticipar que el empleo de dicha herramienta podría constituir un riesgo para los derechos de las personas. Ahora, varias décadas después, dicha aseveración cobra especial relevancia cuando se trata de dotar de razonamiento lógico y autónomo a aparatos tecnológicos que se alimentan de grandes bancos de datos. Conformes con BELLOTO GÓMEZ, la ética debe resultar necesaria en la IA al igual que lo es en las personas[727].

Las anteriores afirmaciones, nos conducen a abordar la necesidad de garantizar sistemas de IA fiables y respetuosos con los derechos fundamentales. En esta línea, resultan de obligada mención las Directrices éticas para una IA fiable elaboradas por un grupo de expertos independiente constituido por la Comisión Europea publicadas el 8 de

[727] BELLOTO GÓMEZ, J.M., "Explicabilidad e inteligencia artificial responsable. Recomendaciones "aterrizadas" al día a día de las empresas", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial,* Valencia, Tirant lo Blanch, 2022, p. 201.

abril de 2019[728]. El señalado trabajo sienta como objetivo promover una IA fiable, para lo que propone el cumplimiento de tres componentes al fin de lograr un marco para una IA con la fiabilidad deseada, a saber: la IA ha de resultar lícita, esto es, debe cumplir las leyes y reglamentos aplicables; de igual modo debe ser ética, en el sentido que, habrá de respetar los principios y valores éticos implicados; por último, deberá gozar de robustez desde el punto de vista técnico, así como social, dado que a pesar de la intención positiva de sus objetivos, la IA puede provocar perjuicios en la sociedad.

Concretamente, la licitud de los sistemas de IA debe garantizar el cumplimiento de las normas implicadas. Así, el respeto de las normas jurídicamente vinculantes a escala europea, nacional e internacional se erige como el punto de partida para el logro de una IA ética y jurídicamente responsable. Es decir, los sistemas de IA deben respetar la normativa implicada en su desarrollo y aplicación, además de garantizar el respeto de los derechos fundamentales de las personas. Precisamente, los sistemas de IA deben respetar la dignidad humana, lo que conlleva que todas las personas han de recibir un trato respetuoso y no aquel que los trate como objetos filtrables, ordenables, condicionables e incluso manipulables[729]. Asimismo, deberán asegurar la libertad individual, evitando la vigilancia injustificada, el engaño y la manipulación; por otra parte, la IA debe respetar la democracia, justicia y Estado de Derecho, no debiendo socavar los procesos democráticos al fin de garantizar a las personas su libertad de elección y toma de decisiones; seguidamente, debe propugnar la igualdad, no discriminación y solidaridad, evitando sesgos injustos en la sociedad; por último, debe garantizar el respeto máximo a los derechos de los ciudadanos[730]. En cambio, tal y como se ha trabajado en el presente trabajo de investigación, abundan ejemplos en los que se ponen en entredicho los derechos fundamentales más elementales consagrados constitucionalmente en las normativas de los Estados.

---

[728] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico Social Europeo y al Comité de las Regiones, sobre Inteligencia artificial para Europa, COM (2018) 237 final.

[729] Recuérdese en este punto el programa COMPAS o el escándalo electoral protagonizado por la compañía Cambridge Analytica. Véanse pies de página 585 y 599 respectivamente.

[730] De modo semejante apunta la OCDE en la Recomendación del Consejo sobre Inteligencia Artificial, de 22 de mayo de 2019, OCDE/JURÍDICO/0449, p. 3 que los actores de IA deben respetar el Estado de derecho, los derechos humanos y los valores democráticos durante todo el ciclo de vida del sistema de IA. Estos incluyen libertad, dignidad y autonomía, *privacidad y protección de datos*, no discriminación e igualdad, diversidad, equidad, justicia social y derechos laborales reconocidos internacionalmente. [la cursiva es nuestra].

En efecto, determinados sistemas de IA implementados en la actualidad no valoran suficientemente el respeto a las premisas expuestas. Efectivamente, habida cuenta que, en las redes sociales, como en muchos ámbitos que emplean IA, los datos resultan un componente indispensable para el funcionamiento de la IA, el respeto al derecho fundamental a la protección de datos personales, debería constituirse como la primera obligación a cumplir por los proveedores de redes sociales. De igual modo, la normativa sobre la instalación de *cookies* estudiada con anterioridad, también debería cumplirse. En cambio, los proveedores de redes sociales no priorizan el respeto a la protección de datos personales en sus modelos de negocio.

Asimismo, el respeto de los derechos fundamentales, debe acompañarse en este campo por normas éticas que, pese a no resultar jurídicamente vinculantes, devienen cruciales en orden a garantizar la fiabilidad de los sistemas de IA. Al hilo de lo expuesto por el Supervisor Europeo de Protección de datos, en el entorno digital actual, no es suficiente con respetar la ley, sino que se debe tener presente la dimensión ética en el tratamiento de datos[731]. De esta suerte, los sistemas de IA deben asegurar el respeto de cuatro principios éticos que han de consolidarse como imperativos éticos que los profesionales de IA deberán esforzarse en observar, a saber: los sistemas de IA respetarán la autonomía humana, prevendrán el daño, resultarán equitativos y, por último, habrán de resultar explicables[732].

En definitiva, mientras que una IA fiable requiere del respeto a los principios éticos implicados, los proveedores de redes sociales no han practicado la reflexión ética necesaria para su garantía, priorizando a tal efecto el desarrollo de sistemas de IA que solamente benefician sus intereses, principalmente económicos, en detrimento de los derechos más elementales de los usuarios de sus servicios. Como muestra de ello, Mark Zuckerberg, fundador de Facebook y propietario de Instagram, Facebook y WhatsApp, afirmó que su compañía no se consideraba una empresa ética, pero afirmaba que sí que cumplían las normas[733]. Sin embargo, ha quedado demostrado en la presente

[731] Dictamen 4/2015 del Supervisor Europeo de Protección de Datos sobre Hacia una nueva ética digital. Datos, dignidad y tecnología, de 11 septiembre de 2015. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf (última consulta el 26 de enero de 2013).
[732] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico Social Europeo y al Comité de las Regiones, sobre Inteligencia artificial para Europa, COM (2018) 237 final.
[733] La literalidad de la frase del Mark Zuckerberg reza como sigue: "Nosotros no necesariamente somos éticos, pero somos legales". Véase en "Hay que enseñar a los límites de la tecnología y pensamiento

investigación que la prioridad de las plataformas no reside en el cumplimiento de la normativa sobre protección de datos personales, a lo que debemos añadir, que el respeto a los principios éticos que deben guiar su negocio carecen igualmente de prioridad en sus negocios, tal y como afirma su fundador[734].

5.2. La explicabilidad y auditabilidad como presupuestos indispensables para una IA lícita

No obstante, todavía resulta posible revertir la situación. Ciertamente, se debe concienciar y forzar a los desarrolladores de sistemas de IA a que el cumplimiento de la normativa implicada se erija como el punto de partida de una IA fiable. Recordemos que, la acumulación de información y el *big data* se consideran dos elementos que han permitido en los últimos años el desarrollo efectivo de la IA[735], de modo que, el cumplimiento riguroso de la normativa sobre protección de datos personales resulta la primera obligación que los desarrolladores deben cumplir. De conformidad con la Autoridad Catalana de Protección de Datos, el uso de la IA debe compatibilizarse con el RGPD[736]. Sobre este particular, los proveedores de redes sociales deben encauzar una reflexión profunda en la que, desde el compromiso, conduzcan sus sistemas de IA a un desarrollo que cohoneste con el cumplimiento efectivo de la normativa sobre protección de datos personales.

Íntimamente relacionado con el cumplimiento de la normativa sobre protección de datos personales, debe exigirse a los desarrolladores de sistemas de IA a que cumplan

crítico", *Autoridad Catalana de Protección de Datos. Inteligencia Artificial: decisiones automatizadas en Cataluña.* Obtenido de: https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf (última consulta el 12 de enero de 2022), p. 84.

[734] En ese sentido, resultan de verdadero interés las palabras de LLANO ALONSO cuando afirma que confiar en los principios y valores éticos y las deontología profesional vigentes pueden ser suficientes para asegurar el correcto desarrollo, despliegue y uso de la IA, es parecido a hacer un acto de fe habida cuenta de las campañas de lavado de imagen ética que han protagonizado algunas de las grandes compañías como Google para encubrir su mala praxis, llegando incluso a despedir a aquellas personas encargas de liderar los proyectos acorde a estándares éticos. LLANO ALONSO, F., "Ética de la inteligencia artificial en el marco de la Unión Europea", en VARONA VILAR, S (Editor), *Justicia algorítmica y neuroderecho: una mirada multidiscipilinar*, Valencia, Tirant lo Blanch, 2021, p. 125.

[735] COTINO HUESO, L., "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho", *Revista General de Derecho Administrativo*, 2019, núm. 50, p. 7.

[736] Informe de la AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS sobre la Inteligencia Artificial: decisiones automatizadas en Cataluña. Obtenido de: https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf (última consulta el 12 de enero de 2022), p. 12.

con el derecho de información de los interesados (explicabilidad)[737]. En efecto, los arts. 13.2.f), 14.2.g) y 15.1.h) RGPD obligan a los responsables del tratamiento a proporcionar información significativa sobre la lógica aplicada del tratamiento, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Esto es, los responsables deben explicar los procesos técnicos, así como las decisiones asociadas al sistema de IA para que estas resulten comprensibles por las personas. Se presenta esta como una premisa básica en orden a que las personas que interactúan con los sistemas de IA puedan defenderse ante las eventuales decisiones adoptadas por este[738].

Únicamente un contexto en el que fluya la información podrá generar mayor confianza en las personas sobre el empleo de sistemas de IA, así como garantizar un absoluto respeto de los derechos fundamentales[739]. En efecto, acertadamente señala BELLOTO GÓMEZ que la explicabilidad se constituye como la base sobre la que se construye la confianza en esta tecnología[740]. No obstante, la tarea se presenta ardua, dado que la práctica habitual consiste hasta la fecha en no informar a los usuarios sobre el empleo de este tipo de sistemas en redes sociales. A pesar de ello, a nuestro juicio, los sistemas de IA solo se tornarán más fiables, cuando entre otras obligaciones, los desarrolladores de los mismos comprendan la relevancia de los principios recientemente expuestos, y con especial mimo, por encontrarse en relación con la privacidad, el principio de explicabilidad. Pese a ello, reconocemos que, cumplir con la transparencia requerida en el contexto de la IA resulta complejo. Ello se debe a que, los propios programadores de algoritmos no alcanzan a conocer aquellas variables que conducen al

[737] En efecto, los arts. 13.2.f), 14.2.g) y 15.1.h) RGPD obligan a los responsables del tratamiento a proporcionar información significativa sobre la lógica aplicada del tratamiento, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

[738] Resulta ilustrativo que, en el año 2007, Adrian Fenty, alcalde de Washington D.C., con el fin de corregir la situación de las escuelas deficientes de la ciudad, encargó a la Rectora en centros educativos de primaria y secundaria Michelle Rhee el desarrollo e implementación de una herramienta de evaluación del personal docente llamada IMPACT, cuyo fin residía en evaluar de modo objetivo al profesorado y prescindir de aquellos que no alcanzaran ciertos estándares. Principalmente se pensaba que el algoritmo podría valorar al personal docente al margen de amistades o subjetivismos. Así las cosas, entre los profesores despedidos, se encontraba Sarah Wysocki, una maestra tremendamente apreciada, tanto por el resto del profesorado, como alumnos y progenitores. Esta, preocupada por la puntuación obtenida por la aplicación, decidió solicitar una explicación para la que no obtuvo respuesta, pues el algoritmo diseñado era de "caja negra", esto es, no cabe la posibilidad de conocer cómo alcanza las decisiones adoptadas. CORTINA ORTS, A., "Ética de la Inteligencia Artificial", *op. cit.*, pp. 390-391.

[739] Véase la Recomendación núm 27 de la Recomendación sobre inteligencia artificial, adoptada el 23 de noviembre de 2021 por la UNESCO. Obtenido de: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa (ultima consulta el 18 de abril de 2023).

[740] BELLOTO GÓMEZ, J.M., "Explicabilidad e inteligencia artificial responsable. Recomendaciones "aterrizadas" al día a día de las empresas", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial*, *op. cit.*, p. 202.

algoritmo a tomar una concreta decisión. Efectivamente, los algoritmos de "caja negra", preocupan considerablemente, ya que, estos no alumbran el modo en el que los objetivos marcados por los programadores se logran[741]. En definitiva, no ha lugar a recibir una explicación sobre la decisión tomada.

No podemos sino mostrar preocupación ante las circunstancias descritas, por cuanto que, aplicadas específicamente en el ámbito del derecho fundamental a la protección de datos personales, la falta de información sobre la práctica de esta técnica de tratamiento, así como sobre la lógica subyacente en su empleo en el ámbito de las redes sociales, conduce a la imposibilidad por parte de los usuarios de estas plataformas de disponer del control de su información personal ni a impugnar las decisiones que empleen estas técnicas (art. 22.3 RGPD). En orden a recuperar la posibilidad real y efectiva de ejercer un control eficaz sobre los datos personales, se debe exigir que los sistemas de IA que cumplan con el principio de transparencia, pues de lo contrario, estos tratamientos de datos carecen de licitud. Más aún, parece que, la UE opta por imponer a las plataformas digitales la obligación de explicar al usuario el método empleado para la publicidad seleccionada, así como la explicación sobre la elaboración de perfiles en el contexto señalado para la muestra de tales anuncios[742]. Por tanto, se debe abandonar la ocultación de esta práctica definitivamente, para a posteriori, comenzar con la explicación transparente y de un modo comprensible para el usuario sobre su lógica aplicada.

En ese sentido, determinadas voces doctrinales se cuestionan si dicha información sobre la lógica aplicada con el fin de cumplir con el principio de explicabilidad conlleva proporcionar al interesado acceso al algoritmo completo o a su código fuente[743]. A nuestro juicio, la explicación que ha de brindarse a los usuarios a efectos de cumplir el principio de transparencia, no implica desvelar el algoritmo completo[744]. Véase que ello impactaría

[741] Los algoritmos de caja negra se definen como aquellos que dada su opacidad en lo que respecta a la toma concreta de decisiones, resulta verdaderamente complejo trazar las bases y razonamientos internos que han conducido al mismo a la toma de la decisión final. OROZCO GONZÁLEZ, M., "Inteligencia artificial y robótica. Propuestas para la configuración de un estatuto jurídico", *Revista doctrinal Aranzadi*, 2021, núm. 8, p. 6.

[742] Considerando 68 del Reglamento (UE), 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE de servicios digitales.

[743] Véase en ese sentido NÚÑEZ SEOANE, J., "El derecho de información y acceso al funcionamiento de los algoritmos que tratan datos personales", en HUERGO LORA, A., (Coordinador), *La regulación de los algoritmos*, Cizur Menor, Aranzadi, 2020, p. 303 y ss.

[744] Conforme con esta consideración se muestra el Tribunal Supremo alemán en el caso SCHUFA, de 28 de enero de 2014, VIZR 153/13 -mientras continuaba vigente la anterior regulación en la Directiva 95/46/CE- cuando afirma que no resulta obligatorio trasladar la fórmula de evaluación empleada a los interesados

con el art. 12 RGPD que propugna claridad y sencillez al momento de explicar el tratamiento, pues las personas no suelen comprender la complejidad técnica de estos cálculos. Antes bien, creemos que el deber de informar sí acarrea un grado de esfuerzo mayor que el exigido hasta la fecha en este ámbito explicativo, dado que, se deben aunar esfuerzos por alcanzar un entendimiento por parte de la población que interactúa con estos sistemas[745]. Por ello, nos sorprende que COTINO HUESO afirme que la información que debe facilitarse a la población, no debe poseer un carácter básico o elemental dirigidos al conocimiento medio de la ciudadanía, sino que deberá alcanzar un nivel técnico accesible para el usuario para que estos puedan defender sus derechos[746]. Véase que ello no garantiza la comprensión por parte del usuario de este tipo de tratamiento de datos personales; en consecuencia, tampoco podrá defender sus derechos ante estos sistemas de IA.

En definitiva, a nuestro juicio, en este campo se debe trabajar y exigir un nuevo concepto de transparencia, más exigente a la par de garantista con el derecho a la protección de datos personales de las personas que interactúan con IA, aplicable especialmente a la finalidad del tratamiento y sus consecuencias[747]. Dado que el objetivo reside en que el usuario comprenda la lógica subyacente de este tipo de tratamientos, se

---

a efectos de determinar su solvencia cuando pretenden acceder a un préstamo bancario. Véase en MEDINA GUERRERO, M., "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales", *Teoría y Realidad Constitucional*, 2022, núm. 49, pp. 158-159.

[745] De conformidad con lo expuesto, el Grupo de Trabajo del Artículo 29 señala que el responsable del tratamiento debe hallar formas sencillas de informar al interesado acerca de la lógica subyacente o los criterios empleados en la toma de la decisión. Sin embargo, no se debe aportar una explicación compleja de los algoritmos utilizados o la revelación del completo algoritmo. Ahora bien, la información facilitada debe resultar suficientemente exhaustiva para que el interesado comprenda los motivos de la decisión. Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 28.

[746] Efectivamente, a pesar de que COTINO HUESO señala que deben diferenciarse dos tipos de transparencia. Por una parte, la transparencia interna, aquella que debe encontrarse presente dentro de la organización o dirigida a auditores internos o externos, los supervisores, los jueves y los interesados (esto es, personas identificadas o identificables); por otra parte, la transparencia externa, que se refiere a la transparencia hacia el exterior o hacia el público en general. Sin embargo, considera que ambas deben alcanzar determinado rigor técnico. COTINO HUESO, L., "Transparencia y explicabilidad de la inteligencia artificial y compañía (comunicación, interpretabilidad, iteligibilidad, auditabilidad, testabilidad, comprobabilidad y simulabilidad…). Para qué, para quién y cuánta", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2022, p. 45-50.

[747] Así, el Supervisor Europeo de Protección de Datos ya reclamaba adaptar el principio de transparencia al nuevo contexto digital en su Opinión 7/2015 sobre "Hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios la protección de datos desde el diseño y la rendición de cuentas", de 19 de noviembre de 2015. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (última consulta el 13 de febrero de 2023), p.10 y ss.

deberá garantizar en todo momento que los interesados entienden y comprenden el modo en el que los algoritmos adoptan concretas decisiones[748]. En consecuencia, en este ámbito, debe garantizarse, sobre todo, la explicabilidad de estos algoritmos a la ciudadanía; sin perjuicio de que, como veremos, frente a otros destinatarios la información deba revestir mayor rigor técnico, como, por ejemplo, frente a autoridades de control.

Consciente de la necesidad regulatoria en el campo específico de la IA, la UE aprueba la Propuesta de Reglamento del Parlamento Europeo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, de 21 de abril de 2021(en adelante, Propuesta de Reglamento sobre IA)[749]. La mencionada propuesta, acoge en un texto jurídicamente vinculante y homogéneo para la totalidad del espacio europeo el haz de ideas y principios que la Comisión Europea venía sentado paulatinamente a través de sus trabajos recientemente expuestos en relación a la IA. Así, el objetivo de la Propuesta de Reglamento sobre IA se halla en mejorar el funcionamiento del mercado interno mediante el establecimiento de un marco jurídico uniforme, en lo que se refiere al desarrollo, la comercialización y la utilización de la IA de conformidad con los valores de la Unión. En efecto, el Considerando 5 de la Propuesta de Reglamento sobre IA dispone que la UE precisa de un marco jurídico que defina una serie de normas armonizadas en materia de IA orientadas a impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, a su vez, ofrezcan un elevado nivel de protección de los intereses públicos, como la salud, la seguridad y los derechos fundamentales reconocidos y protegidos por el Derecho de la UE.

Apreciamos que la Propuesta de Reglamento sobre IA se alinea con el propósito de la UE de erigirse como pionera en el desarrollo de una IA ética[750]. En ese sentido,

[748] Así, COTINO HUESO entiende que se debe diferenciar la transparencia de la explicabilidad, afirmando que, si bien se constituyen como conceptos estrechamente relacionados, la explicabilidad debe garantizar la comprensión por parte de la ciudadanía del razonamiento del algoritmo. Ya que, puede ocurrir que una explicación transparente, no acompañada de determinado grado de explicabilidad, no garantice la comprensión por parte de los interesados. COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial*, *op. cit.*, p. 56.

[749] Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la unión, COM (2021) 206 final.

[750] De conformidad con BENEDITO CAÑIZARES, la UE no desea desarrollar un mercado único digital competitivo a cualquier precio. BENEDITO CAÑIZARES, M.T., "Estadio intermedio de reflexión para una futura regulación de la ética en el espacio digital europeo: los principios de transparencia y acountability", *Revista de Derecho y Nuevas Tecnologías,* 2021, núm. 55, p. 4.

establece, por una parte, un haz de sistemas de IA que deberán prohibirse dada su manifiesta oposición a los valores, principios y derechos de la UE; por otra parte, califica una suerte de sistemas de IA como de alto riesgo, para los cuales, las obligaciones y requisitos a cumplir resultarán mayores. Así las cosas, en virtud de lo dispuesto en el Considerando 15 la Propuesta de Reglamento sobre IA (materializado en el art. 5), esta técnica puede considerarse una herramienta para desarrollar prácticas de manipulación, explotación y control social. Como no podía ser de otro modo, dichas prácticas resultan sumamente intrusivas para las personas y lesivas para sus derechos, motivo por el que habrán de prohibirse; ello se debe principalmente a que, se muestran contrarias a la dignidad humana, libertad, igualdad, democracia y Estado de Derecho y a los derechos fundamentales que reconoce la UE como, el derecho a la no discriminación, la protección de datos y la privacidad, así como los derechos del niño.

De su lectura, puede apreciarse implícitamente el deseo de la UE de no permitir sistemas de IA, que además de vulnerar los derechos fundamentales, no persigan una finalidad ética. En efecto, solamente habrán de permitirse aquellos sistemas de IA que sirvan al beneficio de la sociedad, por tanto, ¿resultan respetuosos con los principios éticos aquellos sistemas de IA cuyo fin reside en controlar y manipular a las personas con fines de publicidad y mercadotecnia directa o se emplean para personalizar la experiencia del usuario en redes sociales? Aparentemente, dichos sistemas contravienen los derechos fundamentales más elementales por cuanto que, limitan la autonomía individual de las personas y afectan a su dignidad, entre otras. Es más, la finalidad de dicha práctica, además de no respetar los derechos fundamentales, no sirve al interés general, sino a intereses particulares y principalmente económicos.

En este orden de cosas, resultan de especial interés las aportaciones del Grupo Especial de Expertos de la ONU encargado de elaborar el proyecto de recomendación sobre la ética de la inteligencia artificial, de 7 de mayo de 2020[751]. En particular, el apartado 26 establece que el método de IA ha de resultar conveniente y proporcional al fin de lograr un objetivo determinado además de no poseer una excesiva repercusión negativa en los valores fundamentales; asimismo, habrá de resultar adecuado al contexto[752]. Por ello, con mayor intensidad reiteramos la pregunta formulada hace escasas

[751] Primera versión del proyecto de Recomendación sobre la ética de la Inteligencia Artificial del Grupo Especial de Expertos de la ONU, elaborado en París el 7 de mayo de 2020.
[752] Primera versión del proyecto de Recomendación sobre la ética de la Inteligencia Artificial del Grupo Especial de Expertos de la ONU, elaborado en París el 7 de mayo de 2020, p. 9. Posteriormente, en 2021

líneas sobre si los sistemas de IA diseñados con fines de marketing y publicidad en redes sociales respetan dichas consideraciones, a la que deseamos añadir, igualmente, otra cuestión en relación a los menores de edad: ¿resultan éticamente correctos el control y manipulación de menores con fines de publicidad y mercadotecnia directa?; asimismo, ¿puede considerarse ético el control y manipulación de menores con el fin de personalizar la experiencia del usuario en redes sociales?

Los sistemas de IA pueden contribuir a generar una sociedad mejor y más respetuosa con los derechos fundamentales; ahora bien, los sistemas que no alcancen un estándar ético, además de no cumplir la normativa implicada, no deben resultar aptos para interactuar con las personas. De este modo, comprendemos que la IA puede resultar beneficiosa en sectores como la medicina, ya que, tal y como afirma HERRÁN ORTÍZ, estas técnicas de tratamiento masivo de datos han beneficiado a la planificación sanitaria, a la atención y diagnóstico de pacientes e incluso a la investigación en este campo[753]. También puede resultar valiosa en el cuidado del medio ambiente donde puede incidir de manera decisiva en el aprovechamiento de los recursos naturales, etc.; sin embargo, estimamos que debe prohibirse su aplicación en sectores donde su empleo busca direccionar el comportamiento del usuario como en redes sociales, con fines principalmente económicos o en el peor de los casos, carentes de ética como controlar manipular a la población. En efecto, esta técnica no debe implementarse para determinadas finalidades de tratamiento.

Más aún, en sintonía con la presente investigación, no debemos obviar que los menores interactúan con esta suerte de sistemas de IA que no siempre se diseñan con fines éticos. Así las cosas, de conformidad con el Grupo Especial de Expertos de la ONU, se ha de proteger a los menores de los daños razonablemente previsibles que se deriven de los sistemas de IA (véase apartado 2.3 del presente Capítulo). En efecto, los diseñadores de estos sistemas de IA, deben prever que personas vulnerables, incluidos

la UNESCO continúa reclamando idéntica proporcionalidad y adecuación al contexto de los sistemas de IA en su Recomendación sobre Inteligencia Artificial, adoptada el 23 de noviembre de 2021 por la UNESCO. Obtenido de: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa (ultima consulta el 18 de abril de 2023), p. 18.

[753] HERRÁN ORTIZ, A.I., "Datos personales de salud, investigación científica, y tecnología big data. De la necesidad de un marco normativo propio en la UE", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma*, *op. cit.*, p. 181.

entre otros, los menores, interactúan con los mismos[754]. Por ello, han de adaptar los sistemas de IA a dichas particularidades para que la IA redunde en beneficio de toda la humanidad. Sin embargo, los sistemas de IA empleados por redes sociales no prevén particularidades en relación a la edad de los usuarios. Por tanto, los menores se exponen a los riesgos que la IA supone para su desarrollo sin medidas específicas para su protección como sujetos especialmente vulnerables.

Por otra parte, la Propuesta de Reglamento sobre IA se centra en establecer una serie de requisitos y obligaciones con carácter reforzado para los sistemas calificados de alto riesgo por el Anexo III de la propuesta[755]. Considera la UE, dichos sistemas de IA albergan riesgos considerables para los derechos fundamentales de las personas, motivo por el que deberán cumplir una suerte de deberes a efectos de garantizar la seguridad de las personas usuarias, entre las que destaca la explicabilidad reforzada[756]. Ahora bien, el mentado Anexo no consideraba los sistemas de IA empleados por los proveedores de redes sociales de alto riesgo, cuestión que estimábamos criticable habida cuenta que, si bien dichos sistemas aparentemente no suponen un riesgo tan evidente como los restantes sistemas que se incluían en el Anexo, la realidad ha demostrado como un incorrecto empleo de los mismos ha llegado a incidir tanto en la estabilidad de democracias como en las bases de un Estado de Derecho; en efecto, los escándalos de Cambridge Analytica o Brexit, se consideran ejemplos en los que los sistemas de IA en redes sociales, al servicio de objetivos carentes de ética se convierten en un verdadero arma para los pilares

[754] Primera versión del proyecto de recomendación sobre la ética de la Inteligencia Artificial del Grupo Especial de Expertos de la ONU, elaborado en París el 7 de mayo de 2020, p. 8. En especial, véase el apartado 24.

[755] En ese sentido, los sistemas de IA calificados como de alto riesgo deberán cumplir requisitos adicionales entre los que destacan: la implantación de un sistema de gestión de riesgos; los datos y gobernanza de los mismos conllevará que los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de adecuada gobernanza y gestión de datos; estos sistemas de IA habrán de proveerse de documentación técnica previa a su introducción en el mercado; asimismo, se procederá al registro automático de eventos mientras funcionan; se diseñarán de tal modo que garanticen un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida; habrán de vigilarse por personas, esto es, deberán controlarse por personas físicas durante el período de uso; por último, deberán alcanzar un nivel elevado de precisión, solidez y ciberseguridad. Por otra parte, para mayor información sobre las obligaciones concretas, véanse el art. 16 de la propuesta de Reglamento sobre IA.

[756] Se entiende por sistema de IA de alto riesgo, aquel que conlleve un riesgo significativo derivado del desarrollo, la implementación y el uso de la inteligencia artificial, la robótica, las tecnologías conexas, de causar lesiones o daños a las personas o a la sociedad, vulnerando los derechos fundamentales y las normas de seguridad establecidas en el Derecho de la Unión, teniendo en cuenta su uso o finalidad específicos, el sector en el que se desarrollan, implementan o usan y la gravedad de las lesiones o daños que cabe esperar que se produzcan. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012 (INL), p. 56.

más fundamentales de nuestros Estados. Sin embargo, destacamos positivamente que la versión final de la norma pendiente de aprobación, de mayo de 2023, haya incluido en mentado Anexo los sistemas de recomendación empleados por las plataformas de medios sociales[757].

Así las cosas, consideramos que todos los sistemas de IA deberían cumplir determinado grado de transparencia y explicabilidad, independientemente de su consideración de alto o bajo riesgo, dado que, cualquier sistema de IA puede llegar a ocasionar perjuicios graves para los derechos fundamentales, aunque aparentemente no revista peligro[758]. La diferenciación entre sistemas de alto y bajo riesgo, así como la previsión de cumplimiento de requisitos y obligaciones únicamente para los primeros, predispone a no cumplir con ninguna obligación en aquellos sistemas que no posean tal consideración[759]. Eventualmente, puede ocurrir, que los sistemas de bajo riesgo continúen desarrollándose de manera oscura, lo que, a pesar de cumplir con la Propuesta de Reglamento sobre IA, impacta con la protección de datos personales, pues al amparo del principio de transparencia, cualquier tratamiento ha de explicarse al interesado (art. 12 RGPD)[760].

---

[757] Enmiendas de los comités parlamentarios del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial) y modifica determinados actos legislativos de la Unión, de 9 de mayo de 2023. Obtenido de: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf (última consulta el 17 de mayo de 2023).

[758] En ese sentido, la UE ha tomado conciencia, tras el revuelo generado por la aplicación ChatGPT, de que varios sistemas de IA pueden vulnerar derechos fundamentales y por ello, prevé normas de transparencia para los mismos. FERNÁNDEZ, C., "El Parlamento Europeo, estudia someter a los sistemas como ChatGPT a las mismas obligacones que los sistemas de IA de alto riesgo", *Diario La Ley (Ciberderecho).* Obtenido de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAEWQTW-DMAyGf01znAL00B1yKXBoRVk_2LSdJgMWRMsSFCds_Pt5VNoOfiXbrx_ZDtCS2mYCuhDBFK5T6ZroGRtofzvO9-j3i5IiuADmiqSSbJsIGt1XDbMeIGhn9-BV4yMK3Z-qyw2NOqGNZ69tpycwSfqeSO71qi6llGnymO12UszoiYfVix7QBhSjHsaKI9xZQKSpgACqeMqbt3O5SbdFs8na8pXl-MxSl4IQfDeeYUBVaQrAG0YToHfUHPIHoOlbGPvBp91W4x3dGU4YjTkYtP3f9lRBtN14ieiXe8n8Fw69qi4MFTBNZrk6w79YPZMj5sdPPuJgc_AuEn9A_gBDWLotXQEAAA==WKE (última consulta el 4 de mayo de 2023).

[759] En efecto, tal y como señala GIL MEMBRADO, la autorregulación se reserva a los sistemas cuyo nivel se encuentre por debajo del nivel alto. GIL MEMBRADO, C., "Una nueva era: hacia el robot sanitario autónomo y su encaje en el derecho", en GIL MEMBRADO, C., (Directora y Coordinadora) *Bioderecho y retos: M-Health, genética, IA, robótica y criogenización,* Madrid, Dykinson, 2022, p. 382.

[760] Conformes con HERRÁN ORTÍZ, deben eliminarse las barreras que impiden dar a conocer el funcionamiento de los algoritmos y tomar en consideración que, cuanto mayor sea el riesgo para los derechos de las decisiones adoptadas por el algoritmo, mayor deberá ser también la explicabilidad del mismo. HERRÁN ORTIZ, A.I., "Inteligencia artificial, salud y derechos humanos: ¿hacia un gobierno de los algoritmos?", en GIL MEMBRADO, C., (Directora y Coordinadora) *Bioderecho y retos: M-Health, genética, IA, robótica y criogenización,* Madrid, Dykinson, 2022, p. 318.

Ahora bien, dicha transparencia, no debe limitarse únicamente a la información facilitada a las personas usuarias de dichos sistemas, sino que, ha de caber la posibilidad de auditar y controlar el diseño e implementación de estos sistemas de IA por sujetos diferentes a sus diseñadores. La rendición de cuentas resulta fundamental en este ámbito, en el sentido que, eventualmente debe caber la opción de que expertos en algoritmos puedan revisar la lógica subyacente del mismo, para lo que se deberán poner a su disposición los parámetros de diseño del algoritmo, así como los conjuntos de datos de los que este se nutre[761]. Solamente en ese caso se podrá comprobar el respeto de estos sistemas con los derechos y valores más elementales de la UE[762]. En este caso, naturalmente, la información debe resultar detallada además de alcanzar un elevado nivel técnico.

Véase que con estas técnicas se accede masivamente a información privada, pero los resultados de los tratamientos, no en pocas ocasiones, se encuentran al amparo de secreto legal e industrial[763]. En efecto, los desarrolladores de algoritmos inteligentes, se muestran reacios a desvelar los detalles de los algoritmos diseñados e implementados por sus compañías. Sin embargo, la propuesta que planteamos salvaría dicha información del conocimiento público, pues mientras que a las personas usuarias solamente se les proporcionaría una explicación que contuviese la lógica subyacente de las decisiones

[761] En ese sentido, la ciudad de Nueva York ha incluido en su Código Administrativo de la ciudad (*Administrative Code of the city of New York*) un nuevo subapartado, concretamente el 25, sobre herramientas automatizadas en la toma de decisiones, que obliga a auditar los sistemas algorítmicos empleados para la contratación laboral. En efecto, la norma se decanta por imponer a los empleadores que se valgan de estas herramientas, el sometimiento a auditoría independiente de los sistemas algorítmicos. A mayor abundamiento, la ley Local Law 2021/144, de 12 de noviembre de 2021, que modifica dicho código obliga a cualquier empleador o agencias de empleo que se valgan de estos sistemas algorítmicos a: en primer lugar, a notificar con diez días de antelación que se emplearán en el proceso de selección algoritmos en orden a evaluar al candidato; en segundo lugar, las cualificaciones y características del puesto de trabajo que empleará la herramienta en la valoración de dicho candidato; en tercer y último lugar, a solicitud de la persona candidata, deberán compartirse con esta los datos empleados en por el algoritmo, así como la fuente de los mismos. Local Law 2021/144, de 12 de noviembre de 2021, sobre las herramientas automatizadas en la toma de decisiones, por la que se modifica el Código Administrativo de la ciudad (*Administrative Code of the city of New York*). Obtenido de: https://www.dfs.ny.gov/system/files/documents/2022/04/NYC_Council_Automated_Employment_Decision_Tools.pdf (última consulta el 20 de enero de 2023).

[762] La Comisión Europea concede verdadera relevancia a la erradicación de la opacidad en este ámbito tecnológico, considerándola la principal responsable de generar dificultad a la hora de comprobar el cumplimiento de la legislación vigente de la UE sobre la protección de los derechos fundamentales. Concretamente, la Comisión europea señala que, la falta de transparencia complica las posibilidades de demostrar los posibles incumplimientos de la legislación, especialmente, aquellas disposiciones cuyo fin reside en la protección de los derechos fundamentales. Libro Blanco sobre inteligencia artificial de la Comisión Europea sobre "Un enfoque europeo orientado a la excelencia y a la confianza", de 19 de febrero de 2020, COM (2020) 65 final, p. 17.

[763] COTINO HUESO, L., "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho", *op. cit.*, p. 14.

adoptadas, el acceso a la información detallada y completa de los algoritmos diseñados solamente se proporcionaría a una autoridad competente. Así, la propiedad intelectual quedaría salvaguardada por cuanto que estas autoridades deberán garantizar la confidencialidad sobre el diseño del algoritmo[764].

En este orden de cosas, el Gobierno español presentó el 21 de abril de 2021 la Estrategia Nacional Española de IA, con el fin de proponer una serie de medidas en este ámbito. Entre ellas destacan, la creación de diversos organismos al servicio de la IA como: la Oficina del Dato, el *Chief Data Officer* cuyo fin reside en la creación de repositorios de datos seguros, o la previsión de programas como, el Programa Nacional de Algoritmos Verdes, el sello nacional de calidad IA y por último, pero no por ello menos importante, la puesta en marcha de un observatorio de evaluación ética y jurídica de los sistemas algorítmicos[765]. En efecto, el Consejo de Ministros ha aprobado el 5 de diciembre de 2022, un acuerdo por el que determina la sede física e la futura Agencia Española de Supervisión de Inteligencia Artificial[766].

Así mismo, también aprobó en julio de ese mismo año la Carta de Derechos Digitales reiteradamente citada en el presente estudio, en la que, al amparo del art. 25, el Gobierno español aboga por el establecimiento de sistemas de IA en condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad y supervisión humana[767]. No

[764] Efectivamente, la solución propuesta se muestra en sintonía con el Considerando 63 RGPD que limita el derecho de acceso cuando pueda afectar a secretos comerciales o propiedad intelectual que protegen programan informáticos. Pueden servir de guía normas aprobadas por otros Estados como el proyecto de Ley sobre responsabilidad algorítmica (*Algorithmic Accountability Act*) que EEUU ha presentado el año 2019. Por ello, la propuesta de COTINO HUESO que aboga por facilitar datos detallados sobre estos algoritmos con carácter general, tal y como se ha señalado anteriormente, colisiona frontalmente con el Considerando 63 RGPD, lo que la conduce a no resultar idónea. COTINO HUESO, L., "Transparencia y explicabilidad de la inteligencia artificial y compañía (comunicación, interpretabilidad, iteligibilidad, auditabilidad, testabilidad, comprobabilidad y simulabilidad…). Para qué, para quién y cuánta", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial, op. cit.,* p. 50.

[765] Estrategia Nacional de Inteligencia Artificial (ENIA) del Gobierno de España, de 21 de abril de 2021. Obtenido de: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf (última consulta el 26 de enero de 2022).

[766] Orden PCM/1203/2022, de 5 de diciembre, por la que se publica el Acuerdo de del Consejo de Ministros, por el que se determina la sede física de la futura Agencia Española de Supervisión de Inteligencia Artificial, Boletín Oficial del Estado, de 6 de diciembre de 2022, núm. 292.

[767] Carta de Derechos Digitales del Gobierno de España. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022). p. 28.

obstante, las labores de vigilancia y control no resultarán posibles sin la instauración de una verdadera cultura de transparencia y auditabilidad de los sistemas de IA.

Así, mientras que los sistemas de IA no podrían funcionar sin un enorme banco de datos, personales o no, la propuesta de la UE salva su regulación afirmando que una IA lícita habrá de cumplir la normativa sobre protección de datos personales a la vez que la Propuesta de Reglamento sobre IA. A pesar de ello, en la presente investigación se ha probado que la normativa de protección de datos personales resulta reiteradamente incumplida en este ámbito. Por tanto, no parece un buen comienzo para regular los sistemas de IA de un modo fiable, remitirse al cumplimiento de una normativa que no se respeta por un sector que emplea sistemas de IA como las redes sociales. Véase que la falta de respeto a los valores y principios en la recogida de datos personales, puede conllevar la falta de licitud de los sistemas de IA, dado que estos se nutrirán de datos recabados de modo ilícito.

Sin perjuicio de que se deba abogar por la educación y concienciación de la sociedad sobre el funcionamiento de la IA, se debe fomentar igualmente, la participación de los desarrolladores de IA en la construcción de un marco normativo y ético que aporte confianza en el empleo de sistemas de IA, además de asegurar un respeto máximo de sus premisas desde un auténtico compromiso. La participación de los actores implicados resulta lógica, ya que el legislador difícilmente puede llegar a conocer las implicaciones técnicas que estos sistemas de IA aparejan, pudiendo generar un efecto negativo en la normativa diseñada que, en consecuencia, conduzca a privar a la sociedad de los avances de la IA[768].

Así las cosas, la UE debe fomentar, con mayor rigor, el cambio de cultura en los desarrolladores de sistemas de IA, debiendo formar a estos en la creación de sistemas de IA respetuosos con los derechos fundamentales a la par de respetuosos con los principios éticos implicados al amparo del principio de responsabilidad proactiva. De acuerdo con PLAZA PENADÉS, se debe poner especial cuidado en que los derechos fundamentales

[768] PEGUERA POCH, M., "En búsqueda de un marco normativo para la Inteligencia Artificial", en CERRILLO I MARTÍNEZ, A., y PEGUERA POCH, M., (Coordinadores), *Retos jurídicos de la Inteligencia Artificial*, Cizur Menor, Aranzadi, 2020. p. 52. En ese sentido, PEGUERA POCH sostiene que una regulación basada en la ignorancia o en el miedo ante la IA podría ocasionar el perjuicio de privar a la sociedad de los potenciales beneficios que la IA sin duda puede aportar.

de la persona prevalecen sobre la tecnología[769]. Véase que abrazar una suerte de principios éticos que guíen la evolución de la IA, conducirá a estos al respeto de las normas sobre protección de datos personales y al abandono del oscurantismo en estas prácticas. Concretamente, los desarrolladores de IA deben emplear su ingenio para desarrollar una IA ética y lícita; y no aquella que se propone sortear la normativa al percibirla como un límite a la evolución de sus sistemas inteligentes. En consecuencia, destacamos positivamente y creemos que debería extenderse a la UE, el acuerdo que EEUU desea formalizar con las grandes tecnológicas en orden a realizar una evaluación pública de los sistemas de IA con el objetivo de garantizar la adecuación de estos sistemas a los derechos y seguridad de las personas[770].

Coincidimos con OLIVER-LALANA y MUÑOZ SORO en que, instaurar tratamientos de datos respetuosos con la privacidad no dificulta el avance de las TIC, sino que, en realidad, ponen coto a un modelo de negocio[771]. Los proveedores de redes sociales se lucran con la información personal de sus usuarios, motivo principal por el que no desean la imposición de trabas que dificulten dicha recogida y análisis de datos.

En la línea de lo expuesto, a nuestro juicio, no consiste únicamente en aprobar nueva normativa específica, sino que, la actualmente vigente, que prevé principios verdaderamente valiosos, se exija y respete por aquellas empresas desarrolladoras de sistemas de IA[772]. En ese sentido, el RGPD desde hace varios años, fomenta un cambio de cultura en los responsables al tratar de abandonar el sistema reactivo por otro que priorice la prevención. En efecto, la responsabilidad proactiva (art. 5.2 RGPD) se convierte así en pieza angular de la evolución de la tecnología. Así las cosas, puede

[769] PLAZA PENADÉS, J., "La moderna configuración de la transparencia en la prestación de servicios y en la contratación en Internet", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial, op. cit.,* p. 228.

[770] FERNÁNDEZ, C., "EEUU acuerda con las grandes tecnológicas realizar una evaluación pública de los sistemas de IA generativa", *Diario La Ley (Ciberderecho).* Obtenido de: https://diariolaley.laleynext.es/Content/Inicio.aspx (última consulta el 11 de mayo de 2023).

[771] OLIVER-LALANA, D., Y MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J., (Coordinador) *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica, op. cit.,* pp. 191-192.

[772] En ese sentido, contemplamos con asombro que determinadas autoras como FERNÁNDEZ-ALLER y SERRANO PÉREZ afirmen que el RGPD no puede ofrecer gran protección frente a la IA, lo que, a su entender conduce a la necesidad de debatir sobre herramientas normativas complementarias al mismo. Sin desmerecer dicha consideración, creemos que, de nada servirá aprobar normativa complementaria si primeramente no se aboga por cumplir la normativa sobre protección de datos personales como presupuesto indispensable para alcanzar una IA fiable. FERNÁNDEZ-ALLER, C., y SERRANO PÉREZ, Mª.M., "¿Es posible una Inteligencia Artificial respetuosa con la protección de datos?", *Cuadernos de Filosofía del Derecho*, 2022, núm. 45, p. 331.

desarrollarse una IA que recabe menos datos, pero de mayor calidad, lo que se alinea con el principio de minimización; se puede trabajar en una mayor transparencia en torno al funcionamiento de los sistemas de IA, lo que no equivale a desvelar el código fuente de los algoritmos diseñados; y por último, también se puede abogar por una programación de algoritmos respetuosa con los derechos y principios implicados.

En definitiva, el legislador europeo y nacionales, así como las autoridades de control deben exigir a estas compañías, por una parte, el abandono de propósitos carentes de ética; y por otra, se debe reclamar la sustitución del tratamiento de datos personales que prioriza los beneficios económicos, por otro en el que se instaure una cultura ética de tratamiento. Solamente un verdadero compromiso de quienes desarrollan e implementan la tecnología descrita conducirá a una IA respetuosa con los derechos fundamentales. Ahora bien, en caso de que continúen sin demostrar un verdadero compromiso, ello justificará que se adopten medidas reactivas para su logro.

Con todo, el equilibrio entre la protección de datos personales y el avance de la IA resulta complejo. Otros países como EEUU, se encuentran avanzados en la implementación de IA en pluralidad de sectores económicos, no obstante, su compromiso con la información personal no goza de la misma prioridad que en el ámbito europeo. En efecto, en EEUU no se prevé la recogida de un consentimiento previo, informado y explícito por parte de los interesados que autorice el tratamiento, sino que, en caso de que un interesado no desee que una corporación trate su información personal, habrá de solicitarlo explícitamente con carácter posterior[773]. Consecuentemente, la fuente de datos de empresas de EEUU en orden a alimentar los sistemas de IA, puede resultar mayor en el contexto descrito. Sentado cuanto antecede, especialmente en el caso de empresas estadounidenses que proveen de plataformas de redes sociales, operan en Europa en condiciones muy similares a las que operan en EEUU, es decir, no adaptan sus modelos de negocio a los valores y principios del lugar en el que prestan sus servicios[774]. Por tanto,

[773] Informe de la AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS sobra Inteligencia Artificial: decisiones automatizadas en Cataluña. Obtenido de: https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf (última consulta el 12 de enero de 2022), p. 14.
[774] Sirva como muestra que, Mark Zuckerber, CEO del Grupo Meta, ha amenazado con retirar los servicios de las plataformas sociales Facebook e Instagram de la Unión Europea ante las obligaciones que el RGPD impone en materia de transferencias internacionales de datos personales. En concreto, la compañía se muestra contraria a no poder transferir el gran volumen de datos de personas recabados en la UE a sus compañías estadounidenses. Para mayor información, véase la noticia de *El Diario Vasco*, de 7 de febrero de 2022, obtenido de https://www.diariovasco.com/economia/empresas/zuckerberg-amenaza-retirar-20220207165631-ntrc.html (última consulta el 8 de febrero de 2022).

a pesar de alabar el deseo de la UE de avanzar en la IA desde un prisma ético, la falta de consenso global en la materia se presenta como un verdadero escollo en su alcance.

CAPÍTULO V:

LA DELIMITACIÓN NORMATIVA DE LOS DERECHOS DEL MENOR EN LA SALVAGUARDA DE SU INFORMACIÓN PERSONAL. ESPECIAL REFERENCIA AL DERECHO AL OLVIDO DIGITAL EN REDES SOCIALES, ¿UTOPÍA O REALIDAD?

La normativa sobre protección de datos personales regula una serie de facultades cuyo fin reside en garantizar al usuario un poder de control sobre su información personal. Concretamente, los derechos de acceso, rectificación, oposición, portabilidad y supresión adquieren se configuran como aquellos derechos que el interesado podrá ejercitar rente al responsable para para asegurar el destino de sus datos personales. Antes bien, cuando el interesado no alcanza la mayoría de edad, garantizar dicha salvaguarda a través de su ejercicio se enfrenta a varios retos.

1. DILEMAS EN EL EJERCICIO DE LOS DERECHOS ARCO-POL QUE ASISTEN AL MENOR DE EDAD PARA LA PROTECCIÓN DE SU INFORMACIÓN PERSONAL EN REDES SOCIALES

El ejercicio de los derechos que la normativa de protección de datos confiere al interesado, se constituye como uno de los pilares básicos en la garantía del control de los datos personales por parte del interesado junto con la prestación del consentimiento al tratamiento. En efecto, los derechos que como contenido esencial conforman y configuran el derecho a la protección de datos personales, han de considerarse valiosísimas herramientas al servicio de las personas para defender su información personal. En ese sentido, recordemos que el menor que pueda prestar consentimiento válido por sí mismo (mayor de 14 años) podrá, igualmente, ejercitar autónomamente los derechos que le asisten para la salvaguarda de su información personal.

Así las cosas, el Dictamen 2/2009 del Grupo de Trabajo del Artículo 29 citado en apartados anteriores de la presente investigación, realizaba la labor, hace más de una década, de adaptar el ejercicio de los derechos Arco (Acceso, rectificación, cancelación y oposición) al particular caso en el que estos debieran ejercitarse por menores de edad o sus representantes. A la luz del dictamen, en ocasiones, el niño podrá ejercer sus derechos por sí mismo[775]. En la actualidad, se suman a los derechos señalados, otros derechos incorporados por el RGPD como el derecho a la portabilidad de los datos, el derecho a oponerse a decisiones individuales automatizadas, el derecho de supresión o también

[775] Dictamen 2/2009 del Grupo Protección de datos del Artículo 29 sobre la protección de datos personales de los niños (Directrices generales y especial referencia a las escuelas), de 11 de febrero de 2009, WP 160, p. 4.

conocido como "derecho al olvido digital" y el derecho a la limitación[776]. Damos por sentado que, si el menor cuenta con la posibilidad de consentir el tratamiento autónomamente, también podrá ejercitar este haz de facultades en defensa de su información personal. Sin embargo, algunos de los derechos mencionados, contienen particularidades cuando su ejercicio acontece en el entorno *online* y especialmente frente a proveedores de redes sociales.

1.1. Sobre la revisión de los tradicionales derechos para la protección de la información personal en la era del *big data* y las redes sociales

En efecto, la irrupción de la era digital, también ha condicionado el ejercicio de los derechos que son el contenido esencial, que hace posible el control de la información. A efectos de continuar considerándose como garantías útiles en la salvaguarda de la información personal, los derechos previstos en la normativa, han sufrido una evolución desde el pasado siglo en el que no resultaba sencillo vislumbrar la fuerza con la que irrumpiría la sociedad de la información por la que se caracteriza el siglo XXI.

Con el fin de profundizar en las vicisitudes de su ejercicio en el ámbito digital, nos proponemos comenzar por el derecho de acceso regulado en el art. 15 RGPD. Este derecho se conforma por tres dimensiones, a saber: el usuario debe conocer si el responsable trata o no información personal sobre su persona; en caso afirmativo, el interesado se encontrará provisto del derecho a obtener la información sometida a tratamiento; y, por último, el responsable deberá informar a este los diversos detalles del tratamiento como los propósitos, los datos sometidos a tratamiento, los destinatarios o categorías receptores[777], la duración del tratamiento y los derechos que asisten al interesado en caso de transferencias de datos. En esencia, puede observarse como el derecho de acceso posee un alcance mayor que el simple acceso a la información personal, pues de su ejercicio, se busca que el usuario pueda comprobar si se trata información personal concerniente a su persona por el responsable con el fin de facilitar

[776] Sobre este último derecho, no centraremos el objeto de estudio del presente epígrafe por no encontrarse en sintonía con la investigación que se presenta.
[777] Sobre el acceso a la identidad concreta de los destinatarios de los datos personales, el TJUE ha señalado recientemente, que el art. 15.1.c) RGPD ha de interpretarse de tal modo que la persona interesada pueda decidir si desea conocer la identidad de los destinatarios de los datos personales o las categorías de los mismos. En consecuencia, en orden a garantizar un verdadero acceso al interesado, el responsable deberá proporcionar la identidad concreta salvo que acredite que la solicitud del interesado resulta infundada o excesiva. Sentencia del Tribunal de Justicia de la Unión Europea, de 12 de enero de 2023, *Österreichische Post*, Asunto C-154/21, aptdo. 51.

el ejercicio de los derechos que le asisten[778], como por ejemplo, el derecho de supresión o rectificación. Efectivamente, el derecho de acceso se posiciona como una herramienta extremadamente útil en orden a verificar qué datos trata el responsable y si trata estos conforme a la normativa sobre protección de datos personales[779].

No obstante, en el ámbito de las redes sociales, el ejercicio de dicho derecho presenta dificultades. En primer lugar, el mismo puede volcar una infinidad de datos ante la múltiple información que se comparte en la red por los usuarios, especialmente si el perfil de estos se encuentra configurado de manera pública. Por ello, convenimos con el CEPD cuando propone a los responsables del tratamiento exponer la información a la que se ha solicitado el acceso por capas. Así, los responsables deberán ubicar en la primera capa aquella información que consideren más relevante para el interesado[780].

En tal sentido, el CEPD continúa señalando que el responsable deberá demostrar que la exposición de la información por capas coadyuvará a comprender la información proporcionada al interesado. A nuestro juicio, el mecanismo señalado puede servir de ayuda a los proveedores de redes sociales en orden a garantizar la comprensión a los usuarios del alud de informaciones que volcará la solicitud del derecho de acceso por parte de estos. Piénsese en el volumen de información que se ha podido llegar a compartir con el proveedor de la red social en caso de que la vigencia de la prestación del servicio dure años, habida cuenta de que los usuarios, especialmente menores, emplean estos servicios de manera constante.

Ha quedado sentado que los responsables del tratamiento deberán facilitar al interesado la información objeto de tratamiento en caso de que el interesado solicite la

[778] Sentencia del TJUE, de 20 de diciembre de 2017, *Pedro Nowak vs. Comisionado de protección de datos*, Asunto C-434/16.

[779] En ese sentido, la AEPD ha reprendido a compañías por atender en el orden equivocado las solicitudes del derecho de acceso y el derecho de cancelación. En efecto, sienta el organismo que, en primer lugar, debe atenderse el derecho de acceso y posteriormente, el derecho de cancelación. Resolución R/02958/2011 de la AEPD sobre el bloqueo y cancelación de datos personales. Obtenido de: https://www.aepd.es/es/documento/td-01259-2011.pdf (última consulta el 29 de enero de 2023).

[780] Así, creemos conveniente destacar el ejemplo empleado por el CEPD en torno al modo en el que debe exponerse la información sobre la que se ha solicitado el acceso, pues afirma que cuando el responsable realice tratamientos basados en parámetros de *big data* con el fin de analizar el comportamiento de los interesados, es posible que dicha información deba ocupar una posición en las capas preferentes al entregar la información al interesado. *Guidelines 01/2022 of European Data Protection Board on data subjet rights-Right of access*, Version 1.0, adopted on january 2022, p. 44 párrafo 143 concretamente.

misma[781]. Antes bien, desacertadamente a nuestro juicio, indica MIRALLES que el derecho de acceso no contempla la posibilidad de acceso a los datos personales generados o calculados a partir de los datos personales obtenidos del interesado[782], cuestión trabajada rigurosamente en capítulos anteriores de la presente investigación. Cierto es que el tenor literal del art. 15 RGPD impone a los responsables informar a los interesados sobre la práctica de estos tratamientos, así como proporcionar una explicación detallada sobre la lógica aplicada de los mismos, pero no se pronuncia sobre la posibilidad de acceder a la información resultante de la aplicación de dichas técnicas.

Sin embargo, dicha exclusión deja al margen del conocimiento del interesado informaciones verdaderamente valiosas, que como ha quedado probado, se han inferido de los datos personales compartidos por el usuario de redes sociales o de la observación constante de su comportamiento. Es más, en muchas ocasiones, el usuario no es consciente de la generación de estos nuevos datos a través de los datos primitivamente aportados, lo que, sin duda, repercute negativamente en su capacidad de control sobre la información personal, ya que, no puede deducir dicho comportamiento de las políticas de privacidad, pero tampoco puede conocer dichos nuevos datos calculados a través del ejercicio del derecho de acceso.

A causa de las consideraciones expuestas, creemos conveniente una reinterpretación del derecho de acceso que prevea la posibilidad de que se facilite al usuario la información inferida que el responsable almacena sobre su persona. En ese sentido se manifiesta el CEPD en las Directrices 01/2022, sobre los derechos del interesado- el derecho de acceso, de 18 de enero de 2022, cuando afirma que los responsables del tratamiento deberán proporcionar (entre otra) la siguiente información

[781] Adviértase que el usuario de la red social posee derecho a conocer y obtener, al amparo del Considerando 63 RGPD: copia de los datos personales que son objeto de tratamiento; los fines del tratamiento; las categorías de datos personales de que se trate; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; de ser posible, el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo; la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; el derecho a presentar una reclamación ante una autoridad de control; cuando los datos personales no se hayan obtenido directamente del usuario, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado; cuando se transfieran datos personales a un tercer país o a una organización internacional, el usuario tiene derecho a recibir información de las garantías adecuadas en relativas a la transferencia realizada.

[782] MIRALLES, R., "El derecho a la portabilidad de los datos personales o prestaciones premium del tradicional derecho de acceso", en VALERO TORRIJOS, J., (Coordinador), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Cizur Menor, Aranzadi, 2013, p. 289.

cuando se ejercite el derecho de acceso por parte del interesado: los datos inferidos de datos proporcionados por el interesado como, por ejemplo, resultados algorítmicos, los resultados de una evaluación médica lograda a través de dicha información, los resultados de una puntuación crediticia, etc[783].

A lo expuesto se debe agregar que la posibilidad de realizar una captura de la imagen o vídeo y compartirla infinidad de veces, dificulta el conocimiento por parte del solicitante de muchas de las informaciones que circulan en la red. Esto es, puede conocer los datos que el proveedor de la red social maneja sobre los usuarios, pero el rastro se pierde más allá del proveedor de los servicios de redes sociales si son los particulares quienes han almacenado dicha información capturada de la red. En verdad, muchos de estos tratamientos recaerán en el ámbito de aplicación de la excepción doméstica, pero se ha podido constatar que no la totalidad podrán beneficiarse de la misma. La UE, consciente de las limitaciones que el derecho de acceso puede suponer en el contexto digital, regula el derecho de portabilidad como una forma avanzada del derecho de acceso como veremos posteriormente[784]; sin embargo, anticiparemos que solamente otorga respuesta a la primera cuestión planteada, esto es, configura cómo debe facilitarse la información disponible *online* al interesado que la solicite, pero guarda silencio sobre las restantes consideraciones realizadas.

Por otra parte, el derecho de rectificación (art. 16 RGPD) se convierte en una garantía fundamental ante las informaciones inexactas o erróneas que puedan circular en la red, no obstante, nos preguntamos si este derecho se encuentra suficientemente garantizado jurídicamente, en el sentido que, los usuarios y especialmente aquellos que asumen obligaciones de un responsable del tratamiento pueden compartir información inexacta o errónea sobre otras personas usuarias. Así las cosas, a futuro deberá reforzarse la posibilidad de que los usuarios que asumen obligaciones de un responsable del tratamiento faciliten canales para ejercitar este derecho ante eventuales informaciones

[783] *Guidelines 01/2022 of European Data Protection Board on data subjet rights-Right of access*, Version 1.0, adopted on january 2022, p. 6 párrafo 96 concretamente.

[784] En ese sentido, MIRALLES califica este nuevo derecho como la versión "Premium" del derecho de acceso. MIRALLES, R., "El derecho a la portabilidad de los datos personales o prestaciones premium del tradicional derecho de acceso", en VALERO TORRIJOS, J., (Coordinador), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica, op. cit.,* p. 278.

incorrectas que publiquen en sus perfiles. De lo contrario, el principio de exactitud (art. 5.1.d) RGPD no será efectivo.

A mayor abundamiento, prevemos que el derecho de rectificación adquirirá especial relevancia en el ámbito de tratamientos de datos basados en parámetros de *big data* e IA, ello se debe a que, tal y como se ha probado anteriormente, los datos inexactos pueden generar inferencias erróneas o defectuosas, lo que justifica en mayor medida que el derecho de rectificación adquiera especial virtualidad en dicho contexto. Nótese que, de continuar disponibles informaciones inexactas susceptibles de captura, loas datos inferidos no serán exactos. Así, el art. 85 LOPDGDD, cuyo fin reside en regular el derecho de rectificación en Internet, se antojaba como el momento idóneo para proporcionar un nuevo alcance a este derecho; sin embargo, el precepto contempla un ejercicio del derecho de rectificación imbricado a la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación[785]. En consecuencia, carece de utilidad ante los nuevos tratamientos de datos masivos.

Por otra parte, el derecho de oposición regulado en el art. 21 RGPD, garantiza al usuario de redes sociales la posibilidad de oponerse al tratamiento de sus datos siga produciéndose. Ahora bien, el devenir de los años, ha alumbrado la necesidad de adaptar el derecho de oposición a nuevos riesgos para la información personal de los interesados. Efectivamente, el RGPD incorpora la posibilidad de oponerse a la elaboración de perfiles, así como el empleo de sus datos para fines de mercadotecnia directa[786]. No obstante, las redes sociales no informan al usuario con claridad sobre si elaboran perfiles (levemente puede intuirse su práctica). Además, tampoco exponen de manera explícita las finalidades de este tratamiento, tal y como ha quedado expuesto en capítulos anteriores, lo que dificulta conocer si comparten información recopilada para que eventualmente las empresas colaboradoras que el usuario desconoce, realicen dichos perfiles (contraviniendo los arts. 12 y 13 RGPD sobre transparencia). En este contexto, el usuario no puede ejercitar un derecho de oposición frente a un tratamiento que desconoce. Más aún, también le resultará complejo conocer ante qué entidad deben ejercitar el derecho de oposición cuando sean las empresas colaboradoras quienes elaboren dichos perfiles.

[785] Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, Boletín Oficial del Estado, de 27 de marzo de 1984, núm. 74.
[786] Véase en ese sentido la guía de la AEPD sobre la "Protección de datos: Guía para el ciudadano". Obtenido de https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf (última consulta 6 de mayo de 2021, p. 20.

Por último, la posibilidad de ejercitar el derecho de oposición en las redes sociales resulta complejo en virtud de los mecanismos que las redes sociales han desarrollado para su ejercicio. Ello puede deberse principalmente a que, en caso de ejercitarlo, el usuario resulta menos valioso para la red social, pues no puede emplear los datos de este con fines de publicidad y mercadotecnia directa. Este tipo de técnicas son útiles a efectos de personalizar servicios y productos para armonizarlos con las necesidades de las personas, actividad que se ofrece por las redes sociales. En efecto, tal y como ha señalado el Grupo de Trabajo del Artículo 29 en las directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, la amplia disponibilidad de datos en Internet, así como la capacidad de hallar correlaciones y crear vínculos, puede permitir determinar, analizar y predecir ciertos aspectos de la personalidad o el comportamiento, los intereses y los hábitos de una persona[787]. Así, las redes sociales blindan en sus políticas de privacidad la personalización de los servicios como una cuestión indispensable para la ejecución del servicio, actividad que consideramos no resulta imprescindible para la puesta a disposición de una plataforma en orden a facilitar la socialización de las personas usuarias[788].

Como último derecho tradicional, brevemente cabe señalar el derecho de cancelación (art. 16 de la antigua LOPD) cuya sustitución ha traído causa de la manifiesta obsolescencia que presentaba frente al avance de la sociedad de la información. Sobre el mismo volveremos con mayor detalle más adelante.

1.2. Nuevas facultades para garantizar al interesado el control sobre sus datos personales en el marco de la inteligencia artificial ante el avance de las redes sociales

Nos hemos referido a los derechos tradicionales garantes de un tratamiento lícito de datos personales, así como la necesaria evolución de algunos de ellos al ámbito de las

[787] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 5.

[788] De acuerdo con dicha afirmación se muestra DEL CASTILLO VÁZQUEZ cuando dispone que el acceso a los servicios de redes sociales no debe condicionarse a la prestación de un consentimiento a efectos de recibir publicidad comportamental, dado que esta condición anularía la libertad requerida para la prestación del consentimiento válido *estudiado en el capítulo III de la presente tesis doctoral*. [la cursiva es nuestra]. DEL CASTILLO VÁZQUEZ, I.C., "Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (comentario al artículo 7 RGPD y al artículo 6 LOPDGDD)", *op. cit.*, p. 952.

TIC. No obstante, el RGPD ha incorporado nuevos derechos íntimamente relacionados con la evolución tecnológica que han sacudido los tratamientos de datos personales, lo que nos conduce a una necesaria mención de los mismos en la presente tesis doctoral. En efecto, con acierto destaca ALVAREZ CARO que el entorno digital predispone nuevos retos para el derecho fundamental a la protección de datos personales, motivo por el que debe continuar garantizándose a los ciudadanos la posibilidad de ejercer un control efectivo sobre su información personal[789].

En ese sentido, cuando estos derechos se ejercitan frente a proveedores de redes sociales, adquieren especial relevancia los derechos de portabilidad y supresión regulados tanto el RGPD como la LOPDGDD. Antes bien, centraremos el presente estudio en el derecho de portabilidad, pues tal y como se ha expuesto, el derecho de supresión se analizará rigurosamente en apartados posteriores.

Así las cosas, el derecho a la portabilidad regulado en los arts. 20 RGPD y arts. 17 y 95 LOPDGDD), constituye un complemento al derecho de acceso. Mediante el ejercicio de este derecho, el responsable, a solicitud de la persona interesada transmite a esta los datos personales concernientes a su persona que se hayan recopilado para que, esta última, o bien los almacene en sus dispositivos personales o los transmita a otra empresa o entidad. Además, también podrá el interesado pretender que los datos se transmitan de responsable a responsable cuando dicha operación resulte técnicamente posible según prevén, el Considerando 68 RGPD y art. 20.2 RGPD. En concreto, el objeto de este nuevo derecho reside en mejorar la capacidad del interesado de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro[790].

Concretamente, el objetivo del legislador europeo al incluir el presente derecho como nueva facultad del interesado, persigue un doble objetivo. Por un lado, fomentar la competencia en el mercado ante los posibles monopolios de datos personales que las grandes empresas como Google, Microsoft, Amazon o Facebook pueden constituir. Para

[789] En ese sentido, se pronuncia con manifiesto acierto la autora en ÁLVAREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en RECIO GAYO, M., Y PIÑAR MAÑAS, J.L., (Directores) *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad, op. cit.*, pp. 229-230.

[790] Así, se constituye como un derecho que puede resultar muy útil para el interesado cuando desea darse de baja de determinado servicio *online*, como por ejemplo el que presta una red social, pero no desea perder gran la información que ha ido compartiendo en su perfil. En relación con la idea expuesta, de forma pionera, la clausurada plataforma Tuenti, tras anunciar su cierre habilitó un enlace para la totalidad de los usuarios que permitía a estos la descarga de todos los contenidos compartidos en la plataforma durante años.

el legislador europeo, la obligación de transmitir datos a otras empresas, puede fomentar la libre competencia en el mercado, favoreciendo especialmente, a pequeñas y medianas empresas que puede resultarles dificultoso competir en el mercado con grandes empresas con acceso a grandes bancos de datos personales. En ese sentido, el mentado derecho posee su origen en la portabilidad numérica regulada en el art. 30 de la Directiva 2002/22/CE, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal)[791], cuyo fin se halla en obligar a los operadores telefónicos a traspasar a otro proveedor elegido por el cliente el número de teléfono de este en un plazo inferior a 24 horas[792].

De conformidad con GONZÁLEZ PACANOWSKA, la medida puede revestir interés con el fin de detraer valor a los datos, puesto que el interesado puede decidir reutilizarlos para sus fines o cederlos a otros responsables[793]. No obstante, a nuestro juicio, este derecho se constituye como un arma de doble filo para la protección de datos personales a pesar de que, para el legislador europeo, este derecho se afiance como una facultad más a efectos de garantizar a los usuarios un mayor control sobre su información personal al poder decidir transmitir datos personales a un responsable de su elección. Las razones que nos llevan a recelar de señalada facultad, se expondrán como sigue.

Cabe anticipar que si bien la reciente incorporación de esta facultad, deja por determinar la aplicabilidad y ejercicio de este derecho con mayor rigor, el Grupo de Trabajo del Artículo 29 se ha pronunciado en sus Directrices sobre el derecho a la portabilidad de los datos, adoptadas el 5 de abril de 2017 con el fin de determinar algunas

[791] Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), citada previamente.

[792] Véase MARTÍNEZ LÓPEZ-SÁEZ, M., "El nuevo derecho a la portabilidad de datos personales a la luz del RGPD y la LOPDGDD: ¿objetivo ambicioso o misión imposible?", en GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (Editoras), *Protección de Datos. Un enfoque nacional y comparado*, Valencia, Tirant lo Blanch, 2019, p. 268.

[793] GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales", en GONZÁLEZ PACANOWSKA, I., (Coordinadora) *Protección de datos personales,* Valencia, Tirant lo Blanch, 2020, p. 677.

condiciones sobre la aplicabilidad del mismo[794]. Con las mismas como guía, interpretaremos el art. 20 RGPD[795].

En ese sentido, al amparo del art. 20 RGPD, podrá solicitarse la portabilidad de los datos personales por parte del interesado cuando se cumplan los requisitos que se señalan como sigue, a saber: por una parte, el tratamiento se practique en virtud de las bases legales del consentimiento (art. 6.1.a) RGPD) o ejecución de un contrato (art. 6.1. b) RGPD); por otra parte, el tratamiento se efectúe a través de medios automatizados. En consecuencia, la portabilidad no podrá solicitarse cuando la base legal del tratamiento resulte diferente a las señaladas, ni ante tratamientos de datos personales no automatizados[796]. Por consiguiente, el ámbito de aplicación del derecho a la portabilidad se ve considerablemente reducido cuando el responsable del tratamiento practica tratamientos fundados en diferentes bases legales.

Así las cosas, continúa el art. 20 estableciendo que el interesado podrá recibir los datos en un formato estructurado, de uso común y de lectura mecánica. Sobre este aspecto, es patente que el RGPD ha tratado de adaptarse a la nueva era digital en la que, la información almacenada de una persona puede alcanzar cifras muy elevadas, y de diversos formatos para lo que, obliga a los responsables del tratamiento a emplear mecanismos que faciliten al usuario la recepción de dicha información. Además, puede el interesado puede desear la transmisión directa de datos personales a otro responsable del tratamiento, sobre este aspecto volveremos más adelante.

Ahora bien, la interpretación del art. 20.1 en torno a los datos objeto de portabilidad no se encuentra carente de polémica. El apartado 1 del mentado precepto, sienta que los datos personales objeto de portabilidad serán aquellos facilitados por el interesado a un responsable del tratamiento. Así las cosas, la interpretación del término "facilitar" no resulta tan sencilla como pudiera parecer. Efectivamente, el Grupo de Trabajo 29 opta por incluir en la noción de "facilitados" tanto los datos compartidos

[794] Directrices del Grupo de Trabajo del Artículo 29 sobre el derecho a la portabilidad de los datos, de 5 de abril de 2017, WP 242, p.3.
[795] Sin perjuicio de ello, algunos autores han analizado el precepto, entre los que destacamos FERNÁNDEZ-SAMANIEGO Y FERNÁNDEZ-LONGORIA, "El derecho a la portabilidad", en PIÑAR MAÑAS, J.L., ÁLVAREZ CARO, M., y RECIO GAYO, M., *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad*, Madrid, Reus, 2016, pp. 262-269.
[796] Muchas redes sociales justifican los tratamientos de datos que practican en la base legal de interés legítimo (art. 5.1.f RGPD) de manera errónea. Consecuentemente, dichas informaciones personales no son susceptibles de portabilidad.

activamente por el interesado, como aquellos que se logran a través de la observación del comportamiento este (datos pasivos).

Sin embargo, tal y como apunta PAZOS CASTRO, el tenor literal del RGPD conduce a pensar que los datos simplemente observados no han de considerarse facilitados por el usuario, pues el término facilitar posee una connotación activa que la observancia del comportamiento no cumple[797]. Efectivamente, el usuario no suele ser consciente de esta recopilación. Por el contrario, GONZÁLEZ PACANOWSKA señala que considerar los datos pasivos no susceptibles de portabilidad, conduce a la normativa europea a una temprana obsolescencia, pues la portabilidad se posiciona en esta circunstancia como un mecanismo idóneo con el fin de que el interesado aproveche las ventajas de un entorno cada vez más interconectado[798]. De modo similar se posiciona la AEPD, cuando afirma que la portabilidad ha de extenderse a los datos facilitados por el propio usuario y a aquellos que resulten del propio uso o desarrollo del servicio contratado[799].

A nuestro juicio, la no inclusión de los datos pasivos en el ámbito del derecho de portabilidad, aportaría mayor seguridad a la información personal del usuario de redes sociales, dado que los datos pasivos (unidos a los activos) pueden servir de gran utilidad en orden a determinar las pautas de consumo, personalidad, comportamiento del interesado, etc. y en consecuencia, contribuir a desvelar en mayor medida la privacidad del interesado. No obstante, la afirmación traída a colación ha de matizarse, pues en caso de que la portabilidad solicitada por el interesado pretenda la transmisión de los datos al propio solicitante, la información a transmitir a este debería abarcar tanto la información activa como pasiva tratada por el responsable. De esta manera, el usuario puede tomar conciencia sobre la totalidad de datos tratados sobre su persona y decidir obrar en

---

[797] PAZOS CASTRO, R., "El nuevo derecho a la portabilidad de los datos personales en el Reglamento (UE) 2016/679, de 27 de abril de 2016", *Revista Crítica de Derecho Inmobiliario,* 2020, núm. 779, pp. 1544-1545.

[798] GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales", en GONZÁLEZ PACANOWSKA, I., (Coordinadora) *Protección de datos personales, op. cit.,* p. 688-689. También se posiciona así MARTÍNEZ LÓPEZ-SÁEZ, M, "El nuevo derecho a la portabilidad de datos personales a la luz del RGPD y la LOPDGDD: ¿objetivo ambicioso o misión imposible?", GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (Editoras), *Reglamento General de Protección de Datos. Un enfoque nacional y comparado, op. cit.,* p. 271-272.

[799] Véase la Resolución de la AEPD /00552/2019 (TD/00195/2019). Obtenido de: https://www.aepd.es/es/documento/td-00195-2019.pdf (última consulta el 15 de septiembre de 2022).

consecuencia con los mismos (emplearlos para uso doméstico o compartirlos con otros responsables de tratamiento).

Por el contrario, si la solicitud de portabilidad pretende una transmisión directa entre responsables del tratamiento (art. 20.2 RGPD), consideramos que la portabilidad deberá interpretarse restrictivamente y alcanzar únicamente los datos activos del solicitante con el fin de salvaguardar su privacidad. Creemos que se protege en mayor medida la información personal del usuario de este modo, porque mediante la transmisión directa de datos entre responsables, el usuario puede no conocer que los datos pasivos pueden llegar a tratarse (junto con la restante información personal) por un nuevo responsable para obtener un valioso rendimiento sobre los mismos. Por ello, puede resultar más conveniente interpretar restrictivamente el término "facilitar" en el contexto señalado. Sin perjuicio de lo expresado, corresponde al TJUE clarificar la interpretación sobre el término "facilitar" empleado por la normativa, puesto que la falta de unanimidad en la interpretación sobre el alcance de los datos susceptibles de portabilidad, genera incertidumbre e inseguridad jurídica.

Por otra parte, el Grupo de Trabajo 29 se decanta por prohibir la transmisión de datos deducidos, esto es, aquellas informaciones generadas por el proveedor de servicios tras la aplicación de algoritmos o elaboración de perfiles[800]. Igualmente respaldan dicha interpretación GONZÁLEZ PACANOWSKA y la AEPD en sus trabajos recientemente citados, así como SANTAMARÍA RAMOS cuando afirma que los datos deducidos quedan fuera del alcance del derecho de portabilidad al no considerarse que los mismos se hayan facilitado por el interesado; ya que, a su entender, estos datos se crean por el responsable[801]. Sin embargo, consideramos que nuevamente, se precisa de una matización al respecto. En efecto, la transmisión de datos inferidos debe prohibirse cuando la misma opera entre responsables. Por el contrario, si los datos se transmitirán al usuario, consideramos que este también debe recibir la información calculada o inferida sobre su persona para decidir o bien almacenarla o transmitirla nuevamente a otro responsable.

[800] Directrices del Grupo de Trabajo del Artículo 29 sobre el derecho a la portabilidad de los datos, de 5 de abril de 2017, WP 242, p.10 y las Directrices del CEPD *Guidelines 01/2022 of European Data Protection Board on data subjet rights-Right of access*, Version 1.0, adopted on january 2022, p. 32.

[801] SANTAMARÍA RAMOS, J.F., "Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (Comentario al artículo 95 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.,* p. 4308.

Solamente de este modo puede el usuario conocer dichos resultados algorítmicos y perfiles realizados sobre su información personal.

Antes bien, en el caso de que la red social comparta información sometida a tratamiento (activa y pasiva), tan sensible, el responsable receptor podría aplicar con carácter posterior dichas herramientas a la información recibida, esto es, que elabore perfiles a posteriori tras la recepción de los datos personales. Por tanto, en última instancia, los datos de las personas usuarias pueden someterse a tratamiento de un modo no consentido.

Tal y como destaca el Grupo de Trabajo 29, el responsable receptor solamente debe aceptar y conservar los datos que sean necesarios y pertinentes para el servicio que preste este nuevo responsable. Es este mandato el que más preocupación nos suscita, en el sentido que, la información que los proveedores de redes sociales almacenan y tratan sobre las personas usuarias, posee un alcance desconocido para estas, de modo que su transmisión a otro responsable puede conllevar a compartir información que el usuario no creía que se sometía a tratamiento. Sobre este extremo puede considerarse una buena práctica remitir al usuario-interesado la información que eventualmente resulte objeto de transmisión. Más aún, el usuario-interesado debe confiar que el responsable receptor no someterá a tratamiento informaciones que no se consideren necesarias para las finalidades de tratamiento declaradas por este, entre las que destaca información tan valiosa como los datos facilitados de forma activa y consciente por el interesado (esto es, todas sus interacciones en la plataforma) pero también, los datos observados del interesado en virtud del análisis del uso del servicio o dispositivo, que como hemos tenido oportunidad de ver, en el caso de redes sociales generan una información muy detallada[802].

Por último, constituye una práctica habitual en redes sociales compartir información de terceras personas. Lo que puede conducir a que cuando el interesado solicita la portabilidad de sus datos, se llegue a transmitir también información personal de terceras personas que ha compartido en su perfil. Recordemos que los usuarios de redes sociales comparten información propia pero también de terceras personas cuando comentan, editan o comparten fotografías de estas. Así, el Considerando 68 RGPD afirma

[802] Así las cosas, se deberá confiar en que dicha información no se emplee para elaborar perfiles de los interesados o cualquier otro tratamiento que no precise tales datos personales portados.

que, cuando un conjunto de datos personales determinado concierne a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento (así accedía al cuerpo del RGPD en el art. 20.4).

En consecuencia, entendemos que la portabilidad de datos personales de terceros usuarios de redes sociales, puede llegar a menoscabar el derecho fundamental a la protección de datos personales de estos, ya que, tal y como señala GONZÁLEZ PACANOWSKA, en redes sociales puede resultar complicado no someter a portabilidad datos de terceros implicados al aparecer estos en fotografías, vídeos, comentarios, etc. del interesado[803]. Sin perjuicio de ello, la autora considera que no concurrirán efectos negativos si con el nuevo responsable la situación de tratamiento es la misma (mismas finalidades).

Nada conformes con dicha afirmación, debe considerarse que el ejercicio del derecho de portabilidad en el que se incluyen datos de terceros puede generar un conflicto entre los intereses de ambas partes a pesar de que la finalidad del tratamiento del nuevo responsable constituya la idéntica que la del responsable transmitente. Sirva como ejemplo, tal y como dispone MARTÍNEZ LÓPEZ-SÁEZ, que puede ocurrir que mientras que el interesado desea ejercitar la portabilidad de determinados datos personales en redes sociales, el tercero cuyos datos también se verían transmitidos, (piénsese en una fotografía o un vídeo en redes sociales en el que además del interesado aparezca el tercero) quizás desee ejercitar el derecho de supresión[804]. Queda en evidencia que, se precisan mayores aclaraciones que conduzcan a facilitar la ponderación de derechos e intereses en juego en el contexto señalado.

En otro orden de consideraciones, en el ámbito nacional, mientras que el art. 17 LOPDGDD remite el ejercicio del derecho de portabilidad al RGPD, el art. 95 LOPDGDD defiende la portabilidad de "cualquier contenido" y no solo de datos facilitados por el usuario en el contexto de redes sociales. Antes bien, consideramos que dicho planteamiento colisiona con varias de las consideraciones realizadas hace escasas

[803] GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales", en GONZÁLEZ PACANOWSKA, I., (Coordinadora) *Protección de datos personales, op. cit.*, p. 715.
[804] MARTÍNEZ LÓPEZ-SÁEZ, M, "El nuevo derecho a la portabilidad de datos personales a la luz del RGPD y la LOPDGDD: ¿objetivo ambicioso o misión imposible?", GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (Editoras), *Reglamento General de Protección de Datos. Un enfoque nacional y comparado, op. cit.*, p. 284.

líneas sobre el alcance de los datos susceptibles de portabilidad. En ese sentido, cabe interpretar que el legislador nacional aboga por la portabilidad de información inferida incluso en contra de lo que la AEPD y organismos europeos sientan en sus recomendaciones y resoluciones citadas.

Con todo, a futuro, el ejercicio de este derecho deberá someterse a importantes revisiones al fin de garantizar el poder de control de los interesados sobre su información personal, así como no mermar el de terceras personas al ejercitarlo, especialmente si el solicitante de dicha portabilidad es menor de edad. En la actualidad, la falta de unanimidad en la interpretación sobre el alcance de este derecho, coloca al interesado en una posición de posible indefensión en orden a ejercitar el control sobre sus datos personales con totales garantías. A mayor abundamiento, consideramos que, la portabilidad se erigiría como un derecho de gran utilidad se informara correctamente a los interesados de los tratamientos a practicar sobre su información personal, pero en el contexto actual de desinformación, la portabilidad puede conllevar a una mayor pérdida de control de los datos personales. Efectivamente, para considerar el derecho de portabilidad como un derecho que contribuye a reforzar el control sobre la información personal, se deberá buscar un equilibrio entre la libre circulación de datos (art. 1.3 RGPD) y el derecho fundamental a la protección de datos personales.

Por último, sin ánimo de extendernos, pues se dedican apartados posteriores a su estudio, el derecho a la supresión o tal y como se ha conocido hasta épocas recientes, el derecho "al olvido digital" (art. 17 RGPD y arts. 93 y 94 LOPDGDD), en origen, se posiciona como pilar fundamental para combatir el rastro indefinido que la información genera en la red.

En suma, los derechos que asisten al interesado para la salvaguarda de sus datos personales, se configuran como herramientas que no garantizan en suficiente medida su cometido en el entorno digital, y concretamente, en redes sociales. Desde que el usuario se da de alta en el servicio *online*, su información personal se muestra susceptible a tratamientos ilícitos por parte del proveedor de la red social sin que cuente con herramientas garantes para combatirlos. Inciden decisivamente en la mentada circunstancia, tanto el diseño, funcionamiento, como el comportamiento del propio usuario titular de datos personales; a lo que se deben añadir, las dificultades que alumbra

el ejercicio garantista de los derechos de los que el interesado puede valerse a efectos de proteger sus datos.

Sin perjuicio de lo anterior, el ejercicio de los derechos señalados por parte de los menores de edad se enfrenta a un obstáculo considerable de necesaria mención en relación a la capacidad que estos poseen de ejercitar de manera autónoma los derechos señalados. Los menores de edad deben alcanzar la edad de 14 años a efectos de poder ejercitar por sí mismos los derechos destinados a proteger sus datos personales, de lo contrario se tratará de sus representantes legales quienes, deberán proceder. Ahora bien, la ausencia de un sistema eficaz en la verificación de la edad de los menores como usuarios de las redes sociales, imposibilita de igual modo acreditar la edad del titular ejerciente de los derechos señalados. En definitiva, la práctica puede conducir al ejercicio de derechos a personas que carecen de la edad establecida por la LOPDGDD para ello. No solo eso sino, también aumenta el riesgo de que, personas que carecen de la madurez suficiente para tomar conciencia de lo valiosa que resulta su información personal, no ejerciten dichos derechos y que, al mismo tiempo, sus progenitores desconocedores de la actividad *online* de sus hijos, no ejerciten un control efectivo de los datos personales de sus hijos[805].

2. DEL "RIGHT TO PRIVACY" DE WARREN Y BRANDEIS AL DERECHO AL OLVIDO DIGITAL

El universo de datos creado en los últimos años por nuestros hábitos *online*, ha llevado a la disponibilidad de infinidad de informaciones de manera ilimitada. Mientras que varias compañías destacan positivamente la capacidad de extraer un rendimiento económico a dicha información, otras cuestiones son las que preocupan desde el punto de vista jurídico, a saber: el rastro permanente que la información genera en Internet. En efecto, cada dato -activo o pasivo- generado por las personas usuarias, resulta susceptible de captura y almacenamiento para su posterior tratamiento. Ello se debe a que toda la información compartida por los usuarios en Internet, queda registrada y grabada por defecto. En este contexto, el derecho al olvido digital o derecho de supresión, se erige como aquella facultad que pretende proporcionar a sus titulares la posibilidad de eliminar dicha huella disponible en la red. Sin embargo, ¿existe una posibilidad real de eliminar los datos compartidos con los proveedores de redes sociales?

[805] Todo ello a pesar de que el art. 12.6 LOPDGDD reconozca que los representantes legales del menor, efectivamente, podrán ejercitar los derechos que asisten a este en aras de proteger sus datos personales.

Los antecedentes del derecho al olvido se remontan a la última década del siglo XIX, coincidiendo con el impacto que la prensa y otros medios de comunicación de la época comienzan a causar en la privacidad de las personas. Concretamente, el concepto actual sobre privacidad hunde sus raíces en Estados Unidos, donde el juez estadounidense Thomas Cooley dispuso en 1888 que la privacidad podía definirse como *the right to be let alone*, esto es, como el derecho a ser dejado en paz. Poco tiempo después, en 1889, el concepto se desarrolló de la mano de WARREN y BRANDEIS en su conocido artículo *The Right to Privacy,* en el que ambos analizaban el derecho de las personas a no sufrir intromisiones en sus vidas privadas por parte de los medios de comunicación de la época (principalmente radio y prensa)[806].

El artículo de WARREN Y BRANDEIS trae causa de la injerencia protagonizada por los medios de comunicación en la vida privada del primero[807]. Así, el artículo buscaba recabar amparo legal, tanto de las intromisiones no deseadas de la prensa en cuestiones privadas de las personas, como de la publicación generalizada de aspectos íntimos de la vida privada de estas. En aquel momento, los medios de comunicación comenzaban a irrumpir, publicaban columnas en sus periódicos con el fin de satisfacer la curiosidad de los lectores a costa de interferir en el ámbito privado de las personas. Por ello, los autores del artículo, se mostraban preocupados por los avances tecnológicos como la toma de fotografías o empleo del teléfono y radio, herramientas que se empleaban en orden a divulgar información de carácter privado. Y a este respecto, concluyen los autores que todo ciudadano se encuentra provisto del derecho a que la autoridad, prensa o terceros se mantengan al margen de la esfera que solo pertenece al individuo.

Tres años más tarde de la publicación del artículo, el Tribunal Supremo de Nueva York emplea la expresión acuñada por Warren y Brandeis en el caso *Marks v. Jaffa*, resolución en la que estima que el demandante posee el derecho a que su imagen no se

[806] WARREN, S.D., y BRANDEIS, L.D., "The Right to Privacy", *Harvard Law Review,* de 15 de diciembre de 1980, núm.5, Vol.4, pp. 193-220.

[807] Dicha injerencia tuvo lugar, principalmente, como consecuencia de las fiestas que la familia Warren acostumbraba a ofrecer en su domicilio de Boston. En dichos encuentros, acostumbraban a reunirse personas de la alta sociedad, lo que captaba el interés de la prensa local, en especial del periódico *Saturday Night Gazette*, que divulgaba lo sucedido en las mismas a gran detalle, compartiendo informaciones personales, sensibles e incluso escabrosas con el fin de causar en los lectores la idea de despilfarro, derroche y amoralidad de la elevada clase social. ÁLVAREZ CARO, M., *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital,* Madrid, Reus, 2015, p. 49.

publique en un periódico sin su consentimiento[808]. Varios años después, en 1931, la Corte de Apelaciones de California resuelve uno de los primeros casos de derecho al olvido, denominado *Melvin v. Reid,* afirmando que los hechos que se demandaban vulneraban la privacidad de la señora Darley y debía reconocerse a las personas el derecho a olvidar y ser perdonadas[809].

En este orden de cosas, en el año 1960, PROSSER revisa y sistematiza el artículo de Warren y Brandeis[810]; sin embargo, conviene recalcar que en dicha obra el autor trata la problemática que suscita recuperar hechos referentes a figuras públicas acontecidos en el pasado. De este modo, afirma que las mentadas personas habrán de soportar hasta el final de sus días el recuerdo que el público posea de dichos acontecimientos, poseyendo la prensa el derecho a informar de los mismos. En esa línea se pronunciarán los tribunales estadounidenses, pues en el caso *Time Inc. v. Hill* en 1967, la Corte Suprema entendió que no cabía considerar que la privacidad de la familia Hill resultaba violada al verse envuelta reiteradamente en hechos noticiosos. Corroboran esta tendencia casos como *Briscoe v. Reader's Digest Assoc.,* de 1971 en el que los tribunales establecen que un personaje público no se vuelve a convertir en persona privada por el mero transcurso del tiempo[811].

Así, a pesar de que Estados Unidos puede considerarse uno de los primeros países en dictar pronunciamientos favorables al derecho a las segundas oportunidades, la jurisprudencia termina por asentar dos criterios que impiden en la actualidad la configuración de un derecho al olvido digital. Por una parte, que una noticia de interés público, siempre revestirá dicho interés. Por otra parte, que una persona que se convierte

[808]CORRAL TALCIANI, H., "El derecho al olvido en internet: antecedentes y bases para su configuración jurídica", *Revista jurídica digital UANDES,* 2017, núm. 1, p. 45.

[809] Así las cosas, la señora Darley (prostituta de profesión) había entregado al deportista de élite Leonard Tropp, con el que mantenía una relación sentimental, una suma de dinero con el fin de que este comprara un anillo de compromiso, que para sorpresa de la señora Darley, finalmente entregó a una mujer diferente para pedirle matrimonio. Años más tarde, la película *The Red Kimono* desvelaba los hechos, empleando el nombre real de la señora Darley. ORZA LINARES, R., "La regulación del derecho al olvido en la Unión Europea. Aspectos críticos", en DURÁN RUIZ, F.J., (Director), *Desafíos de la protección de menores en la sociedad digital: Internet, redes sociales y comunicación,* Valencia, Tirant lo Blanch, 2018, p. 126. Para más información sobre la jurisprudencia norteamericana en relación al derecho al olvido, véase RIGAUX, F., "L´elaboration d´un right of privacy par la jurisprudence americaine", *Revue Internationale de Droit Comparé,* XXXIII, 1980, p. 701-730.

[810] PROSSER, W., "Privacy", *California Law Review,* 1960, núm. 3, vol. 48, pp. 383-423.

[811] Véase al respecto MORENO BOBADILLA, A., "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: un antes y un después para el derecho al olvido digital", *Estudios constitucionales,* 2020, núm. 2, pp. 125-127.

en personaje público, no podrá volver a ser privada[812]. En consecuencia, si bien la jurisprudencia llegó a otorgar preeminencia al derecho a la intimidad de los ciudadanos, sirviendo incluso de ejemplo a los tribunales europeos, finalmente la Corte Suprema de Estados Unidos otorga un valor prácticamente absoluto al derecho a la información[813].

No obstante, en el ámbito europeo, cabe destacar la participación activa del Estado francés en la construcción de un derecho al olvido. En efecto, el país galo puede considerarse precursor de las segundas oportunidades desde los años 60 a 80. Destacamos así, la sentencia del Tribunal de Gran Instancia del Sena, de 4 de octubre de 1965, pionera en reconocer el derecho de los ciudadanos a tener una segunda oportunidad. En ella, el órgano jurisdiccional comienza a sentar los orígenes del derecho al olvido, previo a la era digital mediante el *droit a l'oublie*[814]. Más aún, de forma prematura, la Ley de protección de informaciones personales de 1978 francesa, ya disponía de un derecho al olvido digital[815].

Sentado cuanto antecede, tras el transcurso de ciento treinta y dos años desde el primero de los artículos de Warren y Brandeis, los avances tecnológicos actuales generan un riesgo para la vida privada de las personas con un alcance sin precedentes[816]. Así las cosas, resultan oportunas las palabras de SIMÓN CASTELLANO cuando afirma que el debate sobre la regulación del derecho al olvido se reabre con intensidad ante las características de Internet, dado que este medio permite la difusión y almacenamiento de grandes volúmenes de información de forma perenne[817]. De tal modo, las preocupaciones actuales no residen en la puesta en conocimiento y difusión de noticias sobre hechos

[812] ABRIL, P., y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana. Una visión comparativa del derecho al olvido", *Indret,* 2014, núm. 1, p. 21.
[813] FRANZ, W., "The Right to Inform v. the Right to be Forgotten: a Transatlantic Clash", *Georgetown University. Center for Transnational Legal Studies Colloquium,* 2009, núm. 2, p. 286.
[814] MORENO BOBADILLA, A., "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: un antes y un después para el derecho al olvido digital", *Estudios constitucionales, op. cit.,* p, 125-127.
[815] Loi núm. 78-17 de janvier 1978 relative à l' informatique, aux fichiers et aux libertés, *Journal Officiel de la Republique Française,* num. 227.
[816] Sin embargo, el paso del tiempo ha conducido a Estados Unidos y a Europa a adoptar soluciones legales completamente antagónicas en cuanto al derecho al olvido. Efectivamente, en el primero, el interés público no desaparece a pesar del transcurso del tiempo. Por el contrario, en el continente europeo, la información no debe mostrarse siempre accesible, pues el interés público ha de desaparecer con según pasa el tiempo.
[817] En ese sentido, el autor afirma que una de las principales características del ciberespacio reside en la preservación del pasado y la perennidad de la información, que se produce por defecto por la propia naturaleza y arquitectura red. SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014,* Boch, Barcelona, 2015, p. 61.

acontecidos en el pasado, sino en el mantenimiento de informaciones incorporadas hace años a la red, pero que gracias a las TIC, permanecen accesibles para los usuarios, inicialmente, con carácter perpetuo.

Más aún, debemos contemplar que las propias personas usuarias de Internet y redes sociales comparten las informaciones, que a posteriori, se mantendrán visibles en la red. La evidencia del cambio nos conduce a advertir, que mientras en siglos pasados el acceso a la esfera íntima de las personas tenga lugar mediante la injerencia en la misma de terceros, en la actualidad, estas mismas personas desvelan información privada susceptible de captura. En el contexto descrito, la posibilidad de que terceros accedan a informaciones personales que se creían olvidadas nunca se encontró tan sencillo[818]. Sin embargo, el verdadero riesgo de esta disponibilidad de información, se halla en que la información que contiene la web puede suponer un recuerdo constante de hechos que pueden causar daños en los derechos de la personalidad.

En efecto, en el comienzo del siglo XXI se visibiliza la potencial peligrosidad que el rastro de las interacciones supone para un hipotético olvido de la información personal; la proliferación de servicios *online*, la creación de plataformas sociales, el masivo éxodo de nuestros comportamientos a la red etc., constituyen circunstancias que influirán decisivamente en la paulatina construcción de nuevos derechos, fruto de la evolución de los tradicionalmente reconocidos en la normativa sobre protección de datos personales. Efectivamente, la obsolescencia de los derechos de cancelación y oposición para el logro de una eficaz supresión de los datos personales objeto de tratamiento en línea, condujo al reconocimiento de un derecho al olvido digital que continuase garantizando a los titulares de datos personales un control eficaz sobre su información personal.

No obstante, consideramos que en pleno avance del siglo XXI y a la luz de la rápida metamorfosis de las TIC, cabe cuestionarse si los derechos de supresión u olvido digital se tornan en aspiraciones complejas ante los tratamientos de datos sometidos a técnicas de *big data* e IA, dado que estos posibilitan que determinados datos se empleen, sin importar su antigüedad o exactitud, con el fin de inferir nuevas informaciones sobre las personas. Efectivamente, las herramientas electrónicas cada vez presentan una mayor capacidad de almacenamiento y una extraordinaria eficacia en la selección y recuperación

[818] Efectivamente, resultan esclarecedoras las palabras de TERWAGNE cuando apunta que, en Internet, al contrario de lo que acontece con las personas, la memoria es la regla; mientras que el olvido, la excepción. TERWAGNE, C., "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Revista de Internet, Derecho y Política,* 2012, núm. 13, p. 54.

de información (no solo aportada por usuario); a lo que debemos añadir, la creación de nuevos datos a partir de los datos primitivos. Así, mientras que la simple aparición de Internet ya se constituía como un fenómeno capaz de conducir al fin del olvido, debemos contemplar, que quizás, la vertiginosa evolución de esta herramienta confirme dicho pesar.

Con todo, a nuestro juicio, la preocupación aumenta cuando en un futuro cercano los jóvenes que hoy en día navegan en la red con manifiesta despreocupación, dejando su vida grabada en la red, se encuentren con posibles perjuicios causados por el recuerdo no siempre positivo de informaciones disponibles en la red. En efecto, informaciones pasadas pueden acechar su presente y condicionar su futuro. Sirva como ejemplo de lo expuesto el siguiente acontecimiento: Estados Unidos denegó la entrada al Estado a un psicoterapeuta canadiense de 66 años a causa de un artículo publicado en Internet 30 años atrás, en el que relataba las conclusiones alcanzadas en los experimentos realizados con la sustancia LSD[819]. En definitiva, podemos constatar que la información que de modo perpetuo se encuentra disponible en la red, puede volver a visibilizarse a pesar del transcurso del tiempo, pues Internet no conoce de las barreras de espacio y tiempo. En definitiva, tal y como señala HERRÁN ORTÍZ, el recuerdo digital contribuye a debilitar el importante papel que desempeña el olvido en el mundo analógico[820].

3. ANTECEDENTES NORMATIVOS DEL DERECHO AL OLVIDO DIGITAL

El derecho al olvido digital o derecho de supresión, posee una serie de precedentes en la normativa sobre protección de datos personales que, si bien no reconocen un derecho al olvido como tal, sirven de antecedente en su, finalmente, positivización en el RGPD. En efecto, la Directiva 95/46/CE disponía una suerte principios que pueden considerarse los antecesores del derecho al olvido tan presente en el ámbito digital. Concretamente, el art. 6.1.d), que establecía que habrán de suprimirse los datos inexactos o incompletos en relación a los fines para los que se recogieron y el art. 12.b), que sienta la rectificación, supresión o el bloqueo de datos cuyo tratamiento no se ajuste a la Directiva citada. Así,

[819] ROSEN, J., "The web means the end of forgetting", *The New York Times*, de 21 de julio de 2010. Obtenido de: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (última consulta el 13 de abril de 2022).

[820] HERRÁN ORTÍZ, A. I., "¿Nuevos tiempos, nuevos derechos?:A propósito del difícil olvido en Internet", en EMALDI CIRIÓN, A., y LA SPINA, E., (Editoras), *Retos del Derecho ante un mundo global*, Valencia, Tirant lo Blanch, 2020, pp. 39-40.

los referidos artículos constituyen el origen y fundamento normativo del actual derecho al olvido digital en el ámbito del tratamiento de datos personales[821].

En el contexto nacional, por su parte, el derecho de cancelación regulado en el derogado art. 16 de la LOPD, se considera el precedente de mentado derecho. Ciertamente, el precepto impone al responsable del tratamiento la obligación de cancelar los datos personales que no se ajusten a la ley o resulten inexactos o incompletos. Ahora bien, la cancelación conllevará el bloqueo de dichos datos, conservándose los mismos únicamente a disposición de las Administraciones públicas, Jueces y Tribunales para atender a posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de estas. Una vez prescrito el plazo, se podrá proceder a la supresión de los mismos. De igual modo, en caso de que los datos se hubieran comunicado a terceros, el responsable del tratamiento deberá informar a estos para su cancelación.

Véase que la solicitud de cancelación de los datos personales, no significaba la supresión de los mismos de modo inmediato, sino que el responsable del tratamiento debía abstenerse de su tratamiento activo, reservándolos a disposición únicamente de autoridades competentes durante el plazo de prescripción señalado por la norma en cada caso concreto[822]. Solamente el transcurso de dicho lapso de tiempo legitimaba al responsable a la supresión definitiva de los mismos.

A pesar de lo expuesto, tanto la Directiva 95/46/CE como la LOPD, no se encontraban preparadas para atender a la eliminación de datos personales en plena era digital[823]. Efectivamente, en aquel entonces no se auguraba el impacto que la informática alcanzaría sobre los datos personales de los interesados. Así las cosas, el derecho de cancelación podía garantizar el control personal de la información en un contexto

[821] Así lo consideran, por una parte, DÍAZ DÍAZ, E., "El derecho de supresión. El derecho al olvido (comentario al artículo 17 RGPD y artículo 15 LOPDGDD", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, p. 1574. Por otra parte, ALVAREZ CARO, M., *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital, op. cit.*, pp. 75-76.

[822] Resolución de la AEPD R/02958/2011. Obtenido de https://www.aepd.es/es/documento/td-01259-2011.pdf (última consulta el 28 de enero de 2023).

[823] En ese sentido, convergen diversas voces doctrinales entre las que destacan MINERO ALEJANDRE, G., "A vueltas con el derecho al olvido. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid,* 2012, núm. 30, p.132; ÁLVAREZ CARO, M., *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital, op. cit*., p. 78*;* Así como ARENAS RAMIRO, M., "Hacia un futuro derecho al olvido de ámbito europeo", en VALERO TORRIJOS, J., *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica,* Cizur Menor, Aranzadi, 2013, p. 334.

principalmente analógico, pero pronto se atisbaría la insuficiencia de mentada facultad en el ámbito *online*. Ello se debe a que Internet y las redes sociales plantean una suerte de dificultades para el logro de una eficaz supresión de la información, a saber: en primer lugar, resulta complejo controlar con quién se comparte o divulga la información; en segundo lugar, puede ocurrir que la información compartida en determinado momento de la vida, no necesariamente se corresponda con el deseo de que dicha información permanezca permanentemente disponible en la web. En este sentido, jurídicamente puede que los usuarios hayan revocado el consentimiento al tratamiento y este se siga practicando o también cabe señalar que el principio de minimización exige que los datos no se traten de manera perpetua; por último, el avance de la tecnología ha desembocado en la posibilidad de que las compañías no almacenen y traten datos que se limitan a los aportados por las personas, sino también aquellos metadatos sobre su comportamiento en Internet y redes sociales.

3.1. Las autoridades nacionales de control de datos personales en la construcción de un derecho al olvido: especial referencia a la intervención de la AEPD en el reconocimiento del derecho al olvido digital

En pleno contexto digital, cada vez con mayor asiduidad, la AEPD comienza a recibir solicitudes de cancelación y oposición al tratamiento de datos personales en Internet por parte de internautas. Concretamente, la Memoria de la AEPD del año 2009 señala que las solicitudes de los ciudadanos en relación al olvido digital aumentaron un 200% en el señalado año, habida cuenta que en el año 2008 se recibieron 18 solicitudes, frente a las 57 recibidas en 2009[824].

Cabe afirmar, que el interés de los ciudadanos en poder evitar que sus datos aparezcan en resultados de buscadores de Internet a partir de los datos identificativos de su persona aumentó exponencialmente si se parte sobre la base de que en el año 2007, la agencia solamente recibió tres solicitudes en relación al olvido de datos personales en Internet[825]. Ya en el año 2010, se consolida dicho incremento de las consultas ciudadanas

[824] Memoria de la AEPD del año 2009. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2009.pdf , p. 11. (última consulta el 3 de abril de 2022).
[825] Memoria de la AEPD del año 2009. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2009.pdf , p. 11. (última consulta el 3 de abril de 2022).

en relación al ejercicio de los derechos de cancelación y oposición frente a la perpetuidad de los datos que contiene la web. En concreto, las solicitudes recibidas por la AEPD en relación al olvido en Internet ascienden a 98, afectando el 87% de las mismas al motor de búsqueda Google[826]. En la actualidad, la AEPD continúa recibiendo reclamaciones sobre el derecho al olvido digital, en concreto, señala el organismo que el 30% de las reclamaciones versan sobre alguno de los derechos previstos en la normativa de protección de datos personales, acaparando el derecho de supresión o al olvido digital el 7% de las mismas[827].

Así las cosas, la AEPD se pronuncia por primera vez de modo favorable al reconocimiento del derecho a que los interesados se opongan o cancelen los datos en Internet en el año 2007[828]. Antes bien, durante ese mismo año, también se adoptan resoluciones en las que estima que la publicación de informaciones veraces quedaba al amparo del ejercicio de las libertades informativas, debiendo los conflictos entre el señalado derecho y el derecho a la protección de datos personales solventarse en la jurisdicción ordinaria. De igual modo, consideraba que la labor de los motores de búsqueda no merecía la consideración de responsable del tratamiento, por cuanto que en su labor se limitaban a localizar información en Internet.

Sin embargo, a partir del año 2008 y con especial intensidad desde el año 2009, se puede constatar cómo la AEPD modifica su criterio y comienza a dictar resoluciones que estiman responsables del tratamiento a los buscadores sobre los datos que tratan. Concretamente, la AEPD afirma que la normativa europea resulta de aplicación a los motores de búsqueda e igualmente, los considera responsables del tratamiento de datos en su habitual tarea de indexar datos, algunos de ellos personales, procedentes de otras páginas web. En efecto, la labor del buscador en línea, no se limita a poner a disposición de las personas internautas información publicada en otras fuentes, sino que, en ese cometido, también analizan, clasifican y estructuran la información personal a mostrar. Por último, también reconoce la posibilidad de los interesados de desear la eliminación de dicha información personal[829]. Por otra parte, la AEPD sostiene que el olvido debe

[826] Memoria de la AEPD del año 2010, Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2010.pdf , p. 8. (última consulta el 3 de abril de 2022).
[827] Memoria de la AEPD del año 2021. Obtenido en: https://www.aepd.es/es/documento/memoria-aepd-2021.pdf, p. 88. (última consulta el 13 de abril de 2022).
[828] Resolución de la AEPD R/00598/2007 (TD/00266/2007).
[829] Véase en ese sentido la Resolución TD/01164/2008 disponible en la Menoría del año 2008 de la AEPD. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2008.pdf (última consulta el 13 de abril de 2022).

canalizarse mediante el ejercicio de los derechos de cancelación y oposición en orden a forzar a los buscadores a no indexar información en sus páginas web[830]. En los años que siguen, la AEPD continuó resolviendo reclamaciones relacionadas con el derecho a la supresión u olvido digital, lo que contribuyó sin duda al posterior reconocimiento de este derecho en el seno de la UE como se verá más adelante[831].

Lo cierto es que la actividad de la AEPD puede calificarse como intensa en relación a la construcción del derecho al olvido digital. Podemos afirmar, de conformidad con SIMÓN CASTELLANO, que el papel de la AEPD fue pionero en el reconocimiento del derecho al olvido digital, al considerarse la primera autoridad que reconoció la tutela de derechos de oposición y cancelación frente a los motores de búsqueda[832].

De todos modos, si bien la AEPD adquiere un papel protagonista en el reconocimiento del derecho al olvido digital, no puede considerarse como la única autoridad que ha participado en su reconocimiento. En ese sentido, el *Garante per la Protezione del Dati Personali* Italiano (en adelante, Garante Italiano), resolvía en el año 2004 una solicitud afirmando la existencia del derecho al olvido digital en el marco del principio de finalidad en materia de protección de datos personales[833]. Por otra parte, la CNIL francesa, desde hace más de una década ha habilitado en su web un espacio cuya finalidad reside en proporcionar a los usuarios un apartado para que soliciten la eliminación de la información de los motores de búsqueda[834].

---

[830] Véase la Resolución de la AEPD R/00898/2010 (TD/01887/2009). Obtenido de: https://www.aepd.es/es/documento/td-01887-2009.pdf (última consulta el 15 de septiembre de 2022).

[831] La AEPD continúa manifestándose sobre el derecho al olvido digital en años posteriores a 2009, sirvan como ejemplo la Resolución R/02283/2010 (TD/00754/2010). Obtenido de: https://www.aepd.es/es/documento/td-00754-2010.pdf , la Resolución R/02806/2012 (TD/01178/2012). Obtenido de: https://www.aepd.es/es/documento/td-01178-2012.pdf o la Resolución R/02806/2012 (TD/1065/2013). Obtenido de: https://www.aepd.es/es/documento/td-01065-2013.pdf (última consulta de todas las resoluciones el 15 de abril de 2022).

[832] SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014, op. cit.*, p. 220.

[833] Decisión del Garante per la Protezione del Dati Personali, de 10 de noviembre de 2004 sobre el recurso *Reti Telematiche e Internet- Motori di ricerca e provvedimenti di Autoritá indipendenti: le misure necessarie a garantire il c.d. "diritto all´oblio.,* Obtenido de: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1116068 . (última consulta el 13 de abril de 2022).

[834] Consúltese la versión actualizada a la página en el siguiente enlace: https://www.cnil.fr/fr/cnil-direct/question/comment-faire-supprimer-des-informations-me-concernant-diffusees-sur-internet (última consulta el 15 de septiembre de 2022).

Concretamente, podemos considerar a la CNIL como la verdadera precursora en la consagración del derecho al olvido en su cuarto Informe de actividad referente a los años 1982-1983[835]. Reconocimiento que, extendió al ámbito de Internet varios años después[836]. Incluso cabe señalar que, en el año 2009 este mismo organismo reconoce el carácter fundamental del derecho al olvido en el tercer Informe de actividad del año 2009 cuando afirma que, resulta peligroso e inaceptable que la información publicada *online* sobre una persona permanezca fija e intangible, mientras que la naturaleza humana implica que los individuos cambien, se contradigan o, en definitiva, evolucionen de forma natural. Continúa la CNIL disponiendo que a causa de lo expuesto, la Comisión acoge con satisfacción del debate que se abre en Francia sobre este tema, recordando con fuerza el carácter fundamental del derecho al olvido[837].

Antes bien, otras autoridades como la *Information Commissioner´s Office* inglesa, han mostrado verdadero escepticismo ante el reconocimiento de un derecho al olvido digital, dado que, a su entender, garantizar la efectividad del mismo resulta muy complejo[838]. No debe extrañar dicho posicionamiento del organismo británico, pues Reino Unido se considera un país en el que a causa de su tradición jurídica de *common law*, el derecho al olvido no posee un encaje análogo a los países de tradición civilista como España o Francia. Ciertamente, en países como Reino Unido resultan habituales conductas como publicar íntegramente las sentencias o garantizar un acceso libre a los antecedentes penales, comportamientos ambos impensables en países como el nuestro. Por ello no debe extrañar que los autores que se guían por la tradición del *common law*, se muestren más escépticos ante el reconocimiento de este nuevo derecho. Entre ellos, cabe destacar la preocupación de ROSEN cuando afirmaba que, el reconocimiento del derecho al olvido digital puede generar una confrontación dramática entre la concepción de privacidad y libertad de expresión que existe en Europa y Estados Unidos, lo que, a su vez, puede conducir a una Internet mucho menos abierta[839].

---

[835] *Quatrième rapport d´activité de la CNIL*, 1982-1983, París, La Documentation Française, p. 222.
[836] *20ème rapport d´activité de la CNIL*, 1999, París, La Documentation Française, p. 6.
[837] *30éme rapport d´activité de la CNIL*, 2009, París, La Documentation Française, p. 29.
[838] Contribución de la Information Commissioner´s Office del Reino Unido a la consulta de la comisión europea, Obtenido de: http://bit.ly/pBfWna, (última consulta el 24 de abril de 2023), p. 6.
[839] ROSEN, J., "The right to Be Forgotten", *Stanford Law Review Online*, 2012, núm. 88, vol. 64. Obtenido de: https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/#:~:text=According%20to%20the%20regulation%2C%20when,states%20in%20their%20local%20laws. (última consulta el 13 de abril de 2022).

3.2. La configuración jurisprudencial del derecho al olvido digital en el ámbito europeo y nacional

Entre las reclamaciones recibidas por la AEPD en relación al ejercicio de los derechos de cancelación y oposición frente a datos personales vertidos en búsquedas de Internet, destaca la reclamación de D. Mario Costeja, pues esta servirá de precedente en el reconocimiento del derecho al olvido digital por parte del TJUE. De esta suerte, el 5 de marzo de 2010, Don Mario Costeja presenta una reclamación ante la AEPD contra La Vanguardia Ediciones, S.L., empresa que publica un periódico de gran difusión en Cataluña y contra Google Spain y Google Inc. La pretensión de la reclamación reside en ejercitar el derecho de cancelación de los datos publicados en relación a un anuncio de subasta de un inmueble a causa de las deudas a la Seguridad Social que este había acumulado en 1998. El señor Costeja alega que, para los casos en los que se introduce una búsqueda de su nombre y apellidos en el buscador de Google, el mismo visibiliza dos vínculos hacia páginas que informan sobre dicha deuda pasada y saldada años atrás[840].

De este modo, la AEPD resuelve el 30 de junio de 2010, que La Vanguardia Ediciones, S.L., no ha de retirar dicha información, puesto que la propia Seguridad Social ordenó la publicación de la mencionada información a efectos de dotar de mayor difusión la subasta pública prevista a causa de las deudas contraídas por este. Sin embargo, la resolución no contempla el mismo desenlace para Google, en el sentido que, el buscador sí debe cancelar o borrar los datos de su buscador[841]. La empresa estadounidense, manifiestamente descontenta por el sentido de la resolución de la AEPD, recurre ante la Audiencia Nacional la misma, organismo judicial que ante las dudas que el caso presenta, plantea la cuestión prejudicial al TJUE.

Concretamente, la Audiencia Nacional eleva tres cuestiones al TJUE para su resolución, a saber: la aplicabilidad, por aquel entonces vigente, de la Directiva 95/46/CE

[840] Cabe señalar que El Sr. Consteja, contactó en el año 2009 con la editorial La Vanguardia con el fin de que esta retirara los enlaces referentes a la subasta acontecida años atrás al entender que se trataba de información carente de relevancia debido al tiempo transcurrido. Sin embargo, la editorial rechaza la solicitud, aduciendo que la información se publicó por orden del Ministerio de Trabajo y Asuntos Sociales para dotar de mayor difusión a la subasta. El Sr. Costeja, en febrero de 2010, solicita a Google Spain que adoptara medios a efectos de que la introducción de su nombre y apellidos en el buscador no aportara como resultado el enlace a mentada deuda. La empresa rechaza dicha petición.

[841] Véase la resolución de la AEPD R/01680/2010 (TD/00650/2010). Obtenido de: https://www.aepd.es/es/documento/td-00650-2010.pdf (última consulta el 14 de abril de 2022).

al buscador Google como empresa estadounidense; la consideración de Google como entidad que trata datos, así como su condición de responsable de tratamiento en relación a las labores de buscador; por último, la posibilidad de reconocer un derecho al olvido digital cuando la información se indexa en buscadores para su difusión[842]. Así, las dos primeras cuestiones, se han abordado detalladamente en capítulos previos del presente trabajo. Por tanto, cabe ahora detenerse a analizar la tercera de las cuestiones planteadas por la Audiencia Nacional en relación al reconocimiento del derecho al olvido digital en búsquedas de Internet.

La cuestión prejudicial planteada pronto generó gran expectación, puesto que de su resolución dependía, en parte, el reconocimiento de un derecho al olvido digital. Incluso cabe tener presente, que la Propuesta de Reglamento General de Protección de Datos de 2012 citada previamente, reconocía prematuramente tal derecho bajo la rúbrica del "derecho al olvido y a la supresión" en su art. 17. Antes bien, las conclusiones del Abogado General JÄÄSKINEN no alumbraron un futuro esperanzador para el reconocimiento del derecho al olvido[843], lo que incluso condujo a la UE a eliminar la expresión "derecho al olvido" tras la primera lectura de la Propuesta realizada por el parlamento el 12 de marzo de 2014[844]. Efectivamente, el Abogado General afirmaba la aplicabilidad de la normativa de protección de datos europea a Google; sin embargo, a pesar de considerar la indexación de información en motores de búsqueda como un tratamiento de datos personales, no estimaba a Google responsable del mismo. Finalmente, en dichas conclusiones el Abogado General rechaza la posibilidad de reconocer un derecho al olvido en la circunstancia descrita.

Concretamente, para JÄÄSKINEN, la actividad del buscador consistente en recopilar, grabar, organizar y almacenar datos contenidos en la página web fuente para su posterior difusión, puede considerarse un tratamiento de datos personales. Antes bien, ello no puede aparejar la consideración del proveedor de servicios de motor de búsqueda como responsable de del tratamiento de datos personales. A su entender, el buscador se

[842] Consúltese la Petición de decisión prejudicial presentada por la Audiencia Nacional (España), de 9 de marzo de 2012- *Google Spain, S.L., Google, Inc. / Agencia de Protección de Datos (AEPD)* (Asunto C-131/12).
[843] Conclusiones del Abogado General Niilo Jääskinen, del 25 de julio de 2013. Obtenido de: http://ep00.epimg.net/descargables/2013/06/25/56e4461f3e4296befe3a8f4a56465de4.pdf (última consulta el 14 de abril de 2022).
[844] HEREDERO CAMPO, Mª T., "Evolución tecnológica y derecho al olvido digital, desde sus inicios a la actualidad", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información, op. cit.*, p. 93

limita a proporcionar una herramienta de localización de información, pero no ejerce control alguno sobre los datos personales incluidos en las páginas web de terceros que el buscador indexa. Por otra parte, el Abogado General también señala que la Directiva 95/46/CE no reconoce tal derecho, fundamentando su negativa al reconocimiento de un derecho a eliminar los datos personales de un resultado de búsqueda, en que no se debe permitir que una preferencia subjetiva del interesado se considere como una razón legítima para permitir el borrado de los datos personales. A su juicio, otorgar preferencia al deseo subjetivo del interesado de eliminar datos personales concernientes a su persona, puede debilitar tanto el derecho de libertad de expresión del editor de la página web, como el derecho de libertad de información de los usuarios de este espacio[845].

A pesar de que las conclusiones alcanzadas por el Abogado General no pronosticaban el reconocimiento de un derecho al olvido digital por parte del TJUE, el tribunal europeo, contra todo pronóstico, se desvincula de las conclusiones generales del Abogado General[846]. Sorprendentemente, además de considerar la normativa europea aplicable a Google, también estima que la tarea consistente en indexar información en motores de búsqueda constituye un tratamiento de datos personales del que Google ha de considerarse responsable a todos los efectos[847]. En este mismo sentido, dada la relevancia que adquirirá con posterioridad en la presente investigación doctoral, recordemos que, los proveedores de redes sociales gozan de idéntica consideración[848].

Por otra parte, a nuestro juicio, el pronunciamiento más sorprendente de la sentencia reside en el reconocimiento en contra de lo esperado de un nuevo derecho al olvido en el ámbito digital. En ese sentido, el TJUE afirma que razones inicialmente legítimas del tratamiento pueden caducar con el tiempo, lo que, a nuestro entender, puede ocasionar que el interesado tenga derecho a la eliminación de dicha información de un

[845] Apartados 131-132 de las Conclusiones del Abogado General Niilo Jääskinen, del 25 de julio de 2013. Obtenido de: http://ep00.epimg.net/descargables/2013/06/25/56e4461f3e4296befe3a8f4a56465de4.pdf (última consulta el 14 de abril de 2022).

[846] En efecto, las conclusiones de Niilo Jääskinen supusieron un paso atrás en el reconocimiento del derecho al olvido digital, tal y como afirma SIMÓN CASTELLANO con manifiesto acierto. SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, *op. cit.*, p. 241.

[847] El presente pronunciamiento se ha reiterado, con carácter posterior, en diversas ocasiones por el TJUE, en sentencias como, por ejemplo, en la Sentencia del Tribunal de Justicia de la Unión Europea, de 24 de septiembre de 2019, *Commission nationale de l'informatique et des libertés (CNIL) vs. Google, LLC*, Asunto C-136/17.

[848] Véase Capítulo III de la presente tesis doctoral.

portal abierto al mundo. En efecto, el transcurso del tiempo puede conducir a la obsolescencia y desfase de la información; sin embargo, buscadores como Google continúan otorgando a esta publicidad un posicionamiento protagonista en la web.

Ahora bien, el reconocimiento de un olvido digital se acompaña de una serie de cautelas o límites por parte del TJUE, en el sentido que, habrán de ponderarse caso por caso los derechos en juego con el fin de determinar si priman el derecho a la vida privada y a la protección de datos personales del interesado, debiendo este acreditar las razones legítimas de su situación particular que justifiquen el ejercicio de este derecho; o por el contrario, los intereses legítimos de los internautas potencialmente interesados en acceder a la información en cuestión[849].

Además, si bien los derechos a la vida privada y protección de datos personales, prevalecen con carácter general sobre el resto de intereses, ello no es óbice para que, en ocasiones, esta regla se rompa debido a la naturaleza de la información que se trate y del carácter sensible para la vida privada de la persona afectada, así como del interés del público en obtener dicha información, que puede variar en caso de que la información corresponda a un personaje público[850]. En efecto, en estos casos, tal y como ha afirmado recientemente el TEDH en la sentencia de 6 de octubre de 2022, cuando el interesado desempeña un papel en la vida pública deberá presentar un grado de tolerancia mayor, puesto que se encuentra expuesto al escrutinio público de modo inevitable[851].

Así las cosas, los jueces y tribunales nacionales podrán ordenar al buscador la eliminación de datos personales de la lista de resultados obtenidos tras la introducción del nombre del interesado, aunque concierna a información publicada por terceros. Dicha eliminación deberá proceder a pesar de que no se solicite la misma a la página web fuente, y aunque la publicación de la información se considere lícita. Además, los interesados pueden solicitar la eliminación de información personal cuando resulte perjudicial para

[849] Es más, véase que el conflicto señalado enfrenta, a su vez, los derechos a la información y libertad de expresión (art. 20 CE) y el derecho a la protección de datos personales (art. 18.4 CE), ambos fundamentales.
[850] Véase a tal efecto el párrafo 97 Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González,* Asunto C-131/12. Así, tal y como dispone MUÑOZ, la ponderación en orden a hallar el equilibrio expuesto deberá basarse en cuatro factores: en primer lugar, la naturaleza de la información susceptible de supresión; en segundo lugar, el carácter sensible de la inforamción para la vida privada del interesado; en tercer lugar, el interés público en la disposición de dicha información; por último, el papel que dicha persona pueda desempeñar en la vida pública. MUÑOZ, J., "El llamado derecho al olvido y la responsabilidad de los buscadores. Comentario a la sentencia del TJUE de 13 de mayo de 2014", *Diario La Ley*, 2014, núm. 8339, p. 3.
[851] Véase así el apartado 41 de la Sentencia del Tribunal Europeo de Derechos Humanos, de 6 de octubre de 2022, *Khural y Zeynalov vs. Azerbaiyán*, rec. 55069/11.

su persona o incluso cuando su deseo resida en su eliminación dado el lapso de tiempo transcurrido desde su publicación[852]. En definitiva, el TJUE abre la puerta al reconocimiento de un nuevo derecho al olvido digital; antes bien, el mismo no se configura con carácter absoluto, habrá de analizarse caso por caso su aplicabilidad[853]. No podría ser de otro modo, habida cuenta que el TC ya sentaba en su pronunciamiento 11/1981, de 8 de abril, que no existen derechos absolutos, por lo que, cuando se produzca una colisión entre derechos subjetivos, deberán ponderarse los derechos en liza en orden a determinar cuál de ellos debe prevalecer[854].

Volviendo a la célebre sentencia del caso del Sr. Costeja, tras el pronunciamiento del TJUE, la Audiencia Nacional dicta sentencia el 29 de diciembre de 2014[855], aplicando en su resolución las consideraciones del tribunal europeo al respecto. De este modo, estima que, habida cuenta del carácter sensible de la información difundida en los anuncios publicados por el periódico - una subasta pública por deudas contraídas con la Seguridad Social- para la vida privada del Sr. Costeja, y tomando en consideración que la publicación inicial se remonta a 16 años atrás, en el presente caso no prevalece el derecho del público a acceder a mentada información a partir de la introducción del nombre del interesado, lo que habilita al Sr. Costeja a exigir la eliminación de estos vínculos de la lista de resultados de Google.

El 30 de mayo de 2014, Google habilitó un enlace a efectos de que los interesados pudieran ejercitar el derecho al olvido digital de los contenidos indexados por el buscador. En las primeras veinticuatro horas de disponibilidad a la población del enlace, Google recibió 12.000 solicitudes de cancelación u oposición de los datos personales de usuarios.

---

[852] Recordemos sobre este particular, que un tratamiento inicialmente lícito, puede con el tiempo devenir incompatible con la normativa sobre protección de datos personales al no considerarse los mismos necesarios en relación con los fines para los que se recogieron o trataron como acertadamente señala PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? A propósito de la STJUE de 13 de mayo de 2014 (Google Spain, S.L. y Google Inc./ Agencia Española de Protección de datos [AEPD] Y Mario Costeja González, C-131/12", *op. cit.*, p. 42

[853] Sobre el reconocimiento del derecho al olvido digital, véanse los apartados 94, 96, 97 y 99 de la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc. vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*, Asunto C-131/12.

[854] Sentencia del Tribunal Constitucional 11/1981, de 8 de abril, Boletín Oficial del Estado, de 25 de abril de 1981, núm. 99, pp. 28 a 34.

[855] Sentencia de la Audiencia Nacional 4899/2010, de 29 de diciembre de 2014, (rec. 725/2010).

El 9 de julio de ese mismo año, las reclamaciones ascendieron a 1000 solicitudes diarias[856]. Así las cosas, desde su reconocimiento en 2014, Google Search ha recibido hasta el 26 de mayo de 2020 (en España) más de 87.000 solicitudes de retirada de contenidos que involucran prácticamente 300.000 URL. A nivel europeo, la cifra asciende a más de 1 millón de solicitudes.

Como cabía esperar, el pronunciamiento del TJUE no se ha encontrado libre de críticas. En efecto, ORZA LINARES advierte que la solución propuesta no resulta la idónea debido a que la información cuya supresión se solicita, persiste en la fuente original[857]. En efecto, en el ámbito expuesto, el olvido se ejercita desindexando la información del buscador, pero la información continua disponible en la página que originalmente procedió a su publicación. Sin embargo, no compartimos la primera crítica que expone ORZA LINARES, pues efectivamente, la información debe permanecer en la fuente original, ya que la misma se publica de manera lícita.

En contra de lo que acontece con las publicaciones ilícitas, esto es, aquellas en las que la información debe eliminarse de la fuente original por dañar el honor, intimidad personal o familiar o propia imagen del titular[858], en el caso que se presenta, la publicación se realiza de manera justificada en un momento del pasado; sin embargo, el problema reside en que a pesar de que la misma pierde actualidad, la disponibilidad inmediata de la misma al indexarse por el buscador resulta excesivamente gravosa para su titular. Por ello, estimamos suficiente que, mediante la supresión en el buscador no se atribuya a la misma una difusión permanente; antes bien, sin ánimo de profundizar, pues no constituye objeto de análisis en el presente epígrafe, esta permanencia de la información en la fuente original puede debilitar la privacidad de los interesados en un contexto de tratamientos basados en *big data* e IA.

Por otra parte, afirma el autor que cabe la posibilidad de acceder a la información a través de otros buscadores *online*. Esto es, la solicitud de supresión tiende a dirigirse a un buscador en concreto, pero los restantes podrán continuar desempeñando su actividad

[856] Así se manifiesta con acierto SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014, op. cit.*, p. 268.
[857] ORZA LINARES, R., "La regulación del derecho al olvido en la Unión Europea. Aspectos críticos", en DURÁN RUIZ, F.J., (Director), *Desafíos de la protección de menores en la sociedad digital: Internet, redes sociales y comunicación, op, cit,* p. 130.
[858] Véase así, MARTÍNEZ OTERO, J.M., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google. V. AEPD y Mario Costeja", *Revista de Derecho Político,* 2015, núm. 93, p. 111 y ss.

consistente en indexar la información recopilada. Si bien la solución puede residir en solicitar la supresión de la información a cada buscador en línea, puede resultar complejo ejercitar el derecho de supresión frente a múltiples buscadores en relación a unos mismos datos personales[859]. Por ello, nos parece interesante la reflexión de ÁLVAREZ CARO que aboga por, además de exigir el desindexado al motor de búsqueda, se obligue a las páginas originales a emplear medios que eviten la indexación, ya que así, los restantes buscadores tampoco podrán indexar tales informaciones personales[860]. En definitiva, alabamos los esfuerzos en el reconocimiento de un derecho de supresión en un contexto digital, pero ciertamente, los avances técnicos que se suscitan constantemente por parte de estos proveedores en lo que al tratamiento de datos se refiere, dificultan la búsqueda de un medio de supresión completamente satisfactorio.

En tercer lugar, se deja en manos privadas (buscadores de Internet) la ponderación de derechos fundamentales a la hora de decidir sobre la procedencia de la supresión de la información indexada. Compartimos así el descontento de ÁLVAREZ CARO cuando sienta que el pronunciamiento del TJUE coloca a Google en una posición delicada al verse obligado a decidir sobre cuestiones particularmente sensibles sobre derechos fundamentales, debiendo aplicar unos criterios generales y poco precisos en orden a resolver los conflictos que se presenten entre derechos fundamentales[861]. Pero a nuestro juicio, debemos añadir a tal preocupación, que dejar en manos de un operador privado la ponderación de derechos fundamentales genera inseguridad jurídica, puesto que los intereses del buscador tienden a que este se declare con una manifiesta falta de imparcialidad a la hora de resolver las solicitudes de supresión.

---

[859] Así, nos mostramos conformes con las palabras de ALVAREZ CARO cuando sienta que, devendría en un procedimiento muy costoso para el ciudadano solicitar la supresión de determinadas informaciones ante múltiples buscadores. ALVAREZ CARO, M., "Reflexiones sobre la Sentencia del TJUE en el asunto Mario Costeja (C131/12) sobre el derecho al olvido", *Revista Española de Derecho Europeo,* 2014, núm. 51, p. 182.

[860] *Ibid*, p. 179. En efecto, puede revestir mayor efectividad impedir el indexado a cualqluier motor de búsqueda, en vez de exigir solamente a uno de ellos el desindexado de concretas informaciones que podrán continuar indexándose por los restantes motores de búsqueda frente a los que no se ha solicitado la supresión de la información. Así, tal y como ilustra MARTÍNEZ OTERO, pueden emplearse herramientas de no indexación, como las etiquetas ".txt" cuyo fin reside en evitar la indexación de las páginas originales en los motores de búsqueda. MARTÍNEZ OTERO, J.M., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google. V. AEPD y Mario Costeja", *op. cit.*, p. 136.

[861] ALVAREZ CARO, M., "Reflexiones sobre la Sentencia del TJUE en el asunto Mario Costeja (C131/12) sobre el derecho al olvido", *op. cit.*, p. 182.

En cuarto y último lugar, parte de la doctrina española se ha mostrado abiertamente contraria al reconocimiento de un derecho al olvido al igual que el Abogado General JÄÄSKINEN. Entre estos, destaca PAZOS CASTRO cuando afirma que no resulta necesario proclamar una prevalencia de los derechos de la persona identificada por sus datos personales en el contexto señalado, ya que, a su entender, la propia sociedad olvidará la información con su desinterés por acceder a ella[862]. Antes bien, no podemos sino mostrarnos contrarios a la opinión aducida por el autor. A nuestro juicio, la protección que se procura otorgar al interesado mediante el ejercicio de este derecho reside en mitigar la facilidad con la se puede volver a acceder a la información al indexarse por un motor de búsqueda. En efecto, tal y como señala MORENO BOBADILLA, cualquier dato del pasado puede volver al presente a causa de la inmediatez y ausencia fronteras temporales que Internet predispone[863]. Por tanto, los motores de búsqueda dificultan considerablemente que las personas puedan olvidar o perder el interés en acceder a una información a la que el buscador puede otorgar una posición protagonista en la lista de resultados.

Así, dado que habrá de analizarse caso por caso la procedencia del derecho de supresión, cabe destacar que el TJUE ha continuado, de manera más reciente, resolviendo cuestiones prejudiciales relacionadas con esta facultad en relación a la labor de los motores de búsqueda. Concretamente, la sentencia de 8 de diciembre de 2022, el TJUE sienta que el responsable del tratamiento deberá suprimir la información inexacta que se indexe en el motor de búsqueda, siempre que la persona interesada pruebe la inexactitud de la misma; asimismo, con carácter novedoso, señala que la previsualización de imágenes que aparecen en miniatura en el buscador tras la introducción de una búsqueda de nombre y apellidos y que remiten a la fuente original de información en cuestión, deberá eliminarse igualmente si se solicita su supresión por parte del interesado. Ya que, entiende con acierto que la aparición de la imagen en la indexación, acarrea una injerencia, todavía mayor, en la privacidad de la persona interesada[864]. Sin embargo, lamentamos que, hasta la fecha, el TJUE no se haya pronunciado sobre el ejercicio del

[862] PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? A propósito de la STJUE de 13 de mayo de 2014 (Google Spain, S.L. y Google Inc./ Agencia Española de Protección de datos [AEPD] Y Mario Costeja González, C-131/12", *op. cit.*, p. 46.
[863] MORENO BOBADILLA, A., "El olvido previo a Internet: los orígenes del actual derecho al olvido digital", *Revista Mexicana de Derecho Constitucional*, 2020, núm. 43, p. 200.
[864] Véanse al respecto los apartados 72 y 94 de la Sentencia del Tribunal de Justicia de la Unión Europea, de 8 de diciembre de 2022, *TU Y RE vs. Google, LLc.*, Asunto C-460/20.

derecho de supresión de datos personales frente a proveedores de redes sociales. En efecto, la totalidad de las sentencias, resuelven cuestiones relativas al ejercicio del derecho de supresión frente a motores de búsqueda o hemerotecas digitales. Sobre esta cuestión, volveremos más adelante.

Por otra parte, en el ámbito nacional, la jurisprudencia española se posiciona como la más activa en cuanto a resoluciones sobre el derecho al olvido digital, ya que, hasta el año 2020 se ha pronunciado en 250 ocasiones sobre esta facultad[865].

En efecto, los tribunales nacionales se han pronunciado en reiteradas ocasiones sobre el derecho al olvido digital. Si bien, al igual que lo que acontece en el ámbito de la UE, los tribunales nacionales tampoco se han pronunciado sobre las vicisitudes del ejercicio del derecho de supresión frente a proveedores de redes sociales, a pesar incluso de que el art. 94 LOPDGDD prevea la supresión específica frente a estos prestadores de servicios. Los esfuerzos del TS y del TC se han centrado en perfilar el ejercicio de esta facultad frente a motores de búsqueda y hemerotecas digitales, principalmente. En consecuencia, sin intención de extendernos, procedemos ahora a poner de relieve las consideraciones respecto al principio de finalidad en el tratamiento (art. 5 RGPD) que en estas sentencias se trabajan y su relación con el transcurso del tiempo, debido a que cobrarán especial interés posteriormente en la presente investigación doctoral.

Así, en la sentencia del TS 545/2015, de 15 de octubre[866], el Alto tribunal afirma que lo que se debate en relación al olvido digital, reside en determinar si los fines para los que se trató la información personal continúan vigentes en la actualidad, configurándose el tiempo como factor fundamental, dado que un tratamiento inicialmente adecuado a la finalidad, puede devenir con el transcurso del tiempo inadecuado[867]. De

[865] GARROTE FERNÁNDEZ, I., "La regulación del derecho al olvido en los arts. 17 y 21 del RGPD y en el art. 93 de la LOPDGDD", en GONZÁLEZ PACANOWSKA, I., (Coordinadora), *Protección de datos personales*, Valencia, Tirant lo Blanch, 2020, p. 374.

[866] Sentencia del Tribunal Supremo 545/2015, Sala 1ª de lo Civil, de 15 de octubre de 2015 (rec. 2772/2013). En la reseñada resolución, el diario El País publicó en los años ochenta, información sobre la detención de unas personas, identificando sus nombres y apellidos por presunto delito de tráfico de drogas, así como la adicción de estas a dichas sustancias. Una de las personas, era familiar de un político conocido en aquel entonces. A partir del año 2007, el periódico vuelca dicha información a la hemeroteca digital, no impidiendo que los buscadores pudieran indexar la reseñada información.

[867] Efectivamente, el TS reitera dicho razonamiento, afirmando que debido al paso del tiempo el interés público en la divulgación de la información puede ser menor en relación al perjuicio que su accesibilidad ocasiona al afectado. Sentencia del Tribunal Supremo 210/2016, Sala 1ª de lo Civil, de 5 de abril de 2016, (rec. 3269/2014). En este caso, el TS se pronuncia sobre la publicación de un indulto en el Boletín Oficial

este modo, el factor tiempo ha conducido al TS a estimar la supresión de la información, bastando como muestra alguno de sus recientes pronunciamientos en la sentencia del TS 12/2019, de 11 de enero de 2019[868]; pero este criterio temporal también ha conducido al Alto Tribunal a no reconocer la procedencia de la supresión de determinadas informaciones[869]. Asimismo, cabe señalar que este factor temporal, también se configura como una cuestión que ha generado controversia en otros países del entorno europeo[870].

Sentado cuanto antecede, si bien el tiempo se posiciona como pieza angular en la procedencia de la supresión de los datos personales que con el transcurso del tiempo han perdido relevancia pública y, en consecuencia, los fines para los que se recabaron y trataron pierden virtualidad en la actualidad, la AEPD ha incorporado una suerte de consideraciones en orden a valorar la procedencia de la supresión, que siguen la estela marcada por el TJUE. A su entender, el derecho al olvido digital predispone que las personas deseen ampararse en el mentado derecho para reescribir su historia personal cuando la información volcada en la red se vuelve molesta[871]. Por tanto, además de valorar el factor temporal, también deberá contemplarse que la información no corresponda a un personaje público o que la información no revista relevancia actual en el debate público por constituir hechos que generen impacto social.

Sobre esta última cuestión, el TC ha perfilado estos criterios en su sentencia 89/2022, de 29 de junio de 2022[872], sentando que, a pesar de que desde el punto estricto de la temporalidad, pueden considerarse actuales las publicaciones cuya supresión solicita

---

del Estado sobre unos hechos delictivos ocurridos en 1999. No obstante, el demandante acciona contra los buscadores, debido a que la información continúa apareciendo en las primeras búsquedas del motor de búsqueda.

[868] Sentencia del Tribunal Supremo 12/2019, Sala 3ª de lo Contencioso-Administrativo, de 11 de enero de 2019 (rec. 5579/2017).

[869] Sentencia del Tribunal Supremo 426/2017, Sala 1ª de lo Civil, de 6 de julio de 2017, (rec. 3440/2015). En el presente caso, el TS rechaza el recurso de casación alegando que no procede la supresión de la fotografía de un acusado por un crimen en la vista oral, dado que, si bien es cierto que el crimen ocurrió en 1997, la vista no se celebró hasta 2012, lo que conduce al tribunal a estimar que la proximidad en el tiempo no ha afectado al principio de finalidad.

[870] En el caso de Alemania, dos hermanos que cometieron un asesinato en 1991, deseaban la supresión de su nombre y apellidos en el año 2007 de la estación de radio que había proporcionado difusión nuevamente en Internet sobre el caso. Así el TEDH señaló que existía un interés público permanente en estos hechos que ocurrieron en el pasado, de modo que, no cabía priorizar el derecho a la privacidad de los demandantes en el contexto señalado. Así, Sentencia del Tribunal Europeo de Derechos Humanos, de 28 de junio de 2018, *ML* y *WW vs. Alemania*, Caso 607/98/10 y 65599/10.

[871] Véase, la Resolución de la AEPD R/00512/2018, (TD/02270/2017). Obtenido de: https://www.aepd.es/es/documento/td-02270-2017.pdf (última consulta el 15 de septiembre de 2022) donde la AEPD desestima la reclamación de eliminar determinadas URL de una alta funcionaria por considerar que su relevancia pública conduce a que el interés público predomine ante el borrado de los enlaces.

[872] Sentencia del Tribunal Constitucional 89/2022, de 29 de junio de 2022, Boletín Oficial del Estado, de 29 de julio de 2022, núm. 181, pp. 110173 a 110217.

el interesado (quejas publicadas en un portal web por una particular), dicha actualidad no se traslada a las opiniones vertidas sobre el interesado en este portal de quejas, pues nada tienen que ver con el procedimiento penal en curso contra el interesado que, sí que puede generar un interés superior del público. Así el TC accede a suprimir tales informaciones[873].

En definitiva, queda en evidencia que, tal y como dispone el TJUE, debe analizarse caso por caso la supresión de la información, ya que, efectivamente, la variada casuística de cada caso concreto, puede conducir a resoluciones dispares a la hora de interpretar los criterios expuestos. En ese sentido, acertadamente puntualizaba MARTÍNEZ OTERO en el año 2015 que en los años venideros debería prestarse atención a la jurisprudencia, tanto europea como nacional, pues la misma, de seguro, introduciría paulatinamente matices a la interpretación del derecho al olvido en orden a perfilar sus contornos de modo más preciso[874]. Ahora bien, sin ánimo de resultar reiterativos, advertimos que han sido necesarios múltiples pronunciamientos al fin de encontrar un equilibrio a la hora de ejercitar este derecho frente a motores de búsqueda. En consecuencia, es de intuir que también se requieran aclaraciones que perfilen los contornos en el ejercicio del derecho de supresión cuando el responsable del tratamiento es un proveedor de una red social.

4. LA CONSAGRACIÓN JURÍDICA DEL DERECHO AL OLVIDO DIGITAL EN LA NORMATIVA EUROPEA Y ESPAÑOLA

La inquietud, más que ostensible que genera la perpetuidad de la información en Internet, tanto en la población, como en las instituciones, también arribó a las instituciones europeas, y por ende a los Estados miembros de la UE. Sin embargo, la inclusión del derecho al olvido digital en la normativa sobre protección de datos personales no resultó pacífica. Ello se debe, principalmente, a la incertidumbre que suscitaban las conclusiones generales de JÄÄSKINEN en relación a la cuestión

[873] Es cierto que el TC se pronuncia con carácter posterior sobre criterio de la temporalidad en la Sentencia del Tribunal Constitucional, 105/2022, de 13 de septiembre de 2022, Boletín Oficial del Estado, de 21 de octubre de 2022, núm. 253, pp. 144496-144524, pero fundamenta la argumentación de su fallo, con carácter experso, en la sentencia del Tribunal Constitucional 89/2022, de 29 de junio de 2022, recientemente citada. Por ello, nos remitimos a las consideraciones expuestas anteriormente.

[874] MARTÍNEZ OTERO, J.M., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google. V. AEPD y Mario Costeja", *op. cit.*, p. 135.

prejudicial planteada por la Audiencia Nacional española al TJUE recientemente citada, pues de su resolución dependía, en gran medida, la positivización con éxito del derecho al olvido en la normativa europea.

4.1. La UE como fiel partidaria del reconocimiento del derecho al olvido digital. En especial, de las personas menores en tránsito hacia su madurez

En pleno debate público sobre la reforma del derecho europeo de protección de datos personales ante el imparable avance de la sociedad de la información, nada parecía prever la inclusión en la agenda europea de dicho capítulo reflexivo en torno al derecho al olvido digital. En ese sentido, el Grupo de Trabajo del Artículo 29, tampoco introducía menciones al mismo en su Dictamen 1/2009, sobre el futuro de la privacidad, de 1 de diciembre de 2009[875]. Sin embargo, no tardaron en sucederse ligeras visibilizaciones del derecho al olvido digital por diversas instituciones de la UE ante el imparable avance de Internet. En efecto, el 30 de noviembre de 2010, Viviane Reding, vicepresidenta de la Comisión Europea mostraba su preocupación ante la pérdida de control de los datos personales que los usuarios sufrían, especialmente, cuando manejaban Internet y redes sociales[876].

Finalmente, ante la manifiesta preocupación que azotaba a la UE en relación a la imposibilidad de clausurar cuentas en redes sociales, la falta de destrucción de los datos por parte de estas plataformas, así como a las dificultades en la mudanza de dichos datos de unas redes sociales a otras, la Comisión Europea se inclina por el refuerzo del control sobre la información personal de los usuarios proporcionándoles dos nuevas herramientas, a saber: el derecho al olvido digital y el derecho a la portabilidad de los datos. Por consiguiente, la primera referencia explícita al derecho al olvido puede hallarse en la ya mencionada Comunicación de la Comisión al Parlamento Europeo, sobre "Un enfoque global de la protección de datos personales en la Unión Europea", de 4 de noviembre de 2010. La presente comunicación de la Comisión al Parlamento, se centra en el nacimiento de un derecho al olvido digital, fuertemente vinculado al mundo *online*,

[875] Dictamen 1/2009 del Grupo de Trabajo del Artículo 29, sobre el futuro de la privacidad, de 1 de diciembre de 2009, WP 168.
[876] REDING, V., *Privacy matters- Why the EU needs new personal data protection rules*. Obtenido de: file:///C:/Users/estelabrion/Downloads/Viviane_Reding_Vice-President_of_the_European_Commission__responsible_for_Justice__Fundamental_Rights_and_Citizenship_Privacy_matters___Why_the_EU_needs_new_personal_data_protection_rules_The_European_Data_Pr.pdf (última consulta el 27 de abril de 2023).

y especialmente, a las redes sociales que se encontraban en plena irrupción y apogeo en aquel entonces.

Antes bien, la positivización del derecho al olvido digital en el RGPD, se encuentra fuertemente marcada por la tramitación de la cuestión prejudicial del Sr. Consteja contra Google recientemente citada, que como puede apreciarse, transcurrió prácticamente en paralelo. Ello se debe a que, si bien todo apuntaba, de conformidad con RALLO LOMBARTE, a que el reconocimiento del derecho al olvido digital contaría con un escaso éxito[877], lo finalmente acontecido distó considerablemente de lo pronosticado. A pesar de la incertidumbre generada por la cuestión prejudicial ante el TJUE, el Proyecto de RGPD, de 25 de enero de 2012, reconocía tímidamente un derecho al olvido digital, a pesar de subsumirlo en el derecho de cancelación. Aunque cierto es que el Parlamento Europeo suprimiría la rúbrica de derecho al olvido digital el 12 de marzo de 2014[878], ante el conocimiento de las conclusiones alcanzadas por el Abogado General Jääskinen, fiel opositor al reconocimiento de un derecho al olvido digital, tal y como se ha puesto de manifiesto.

Así las cosas, íntimamente relacionado con el objeto de estudio de la presente tesis doctoral, el Proyecto de RGPD presentado en 2012, ya mostraba su preocupación por la relevancia que el olvido adquiere cuando los datos personales conciernen a menores de edad, concretamente en el considerando 53 y art. 17.1 RGPD[879]. La razón reside en que la información personal de estos puede quedar obsoleta con una manifiesta facilidad dada su particular situación de tránsito hacia su madurez, de modo que, el olvido se presenta

[877] RALLO LOMBARTE, A., "El debate europeo sobre el derecho al olvido en Internet" en RALLO LOMBARTE, A., y GARCÍA MAHAMUT, R., (Editores), *Hacia un nuevo derecho europeo de protección de datos*, Valencia, Tirant lo Blanch, 2015, p. 705.

[878] Véase la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Obtenido de: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_ES.html#title2 (última consulta el 14 de abril de 2022).

[879] Sin embargo lamentamos que, mientras la Propuesta del art. 17.1 RGPD regulaba el derecho al olvido, con especial consideración, cuando el titular de los datos es menor de edad, dado que literalmente disponía que "El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente lo que respecta a los datos personales proporcionados por el interesado siendo niño", veremos que la versión actualmente vigente del RGPD obvia dicha mención a la minoría de edad. Antes bien, el Considerando 65 continúa advirtiendo de la relevancia de este derecho en el caso de menores de edad.

como una facultad verdaderamente valiosa para los jóvenes, especialmente cuando ya no poseen tal condición.

Con todo, la sentencia del TJUE por la que se reconoce, sin lugar a dudas, un derecho al olvido digital, terminó por despejar las incertidumbres que dificultaban la UE la inclusión del mentado derecho en el RGPD. Tras un largo caminar, que transcurre desde aproximadamente el año 2010, hasta la aprobación del RGPD en el año 2016, la normativa actualmente vigente reconoce el derecho de supresión (al olvido digital) en su art. 17.

En ese sentido, los responsables del tratamiento deberán garantizar la supresión de los datos personales cuando los interesados soliciten la misma, siempre que se cumplan los supuestos de aplicación que el mentado artículo establece, a saber: a) los datos ya no son necesarios para los fines para los que se recogieron o se han tratado de otro modo; b) el interesado retira el consentimiento y el tratamiento no se basa en otra base jurídica que legitime el tratamiento; c) el interesado se opone al tratamiento de datos personales (art. 21 RGPD); d) los datos se han tratado ilícitamente por el responsable del tratamiento; e) los datos deben suprimirse en cumplimiento de una obligación legal establecida en la UE o Estado miembro; y los datos se han obtenido en relación con la oferta de servicios de la sociedad de la información a menores (art. 8.1 RGPD).

En concreto, los apartados a) y f) expuestos recientemente. El primero de ellos, sin lugar a dudas, acoge la principal premisa establecida por el TJUE en relación a la finalidad del tratamiento, en el sentido que, puede ocurrir que con el transcurso del tiempo el tratamiento de datos personales devenga inadecuado para los fines para los que se recabó. A nuestro juicio, este aspecto cobra especial virtualidad con el presupuesto f) pues, es posible que los datos de menores de edad, ante su gran susceptibilidad de cambio, puedan incurrir en esta situación con facilidad.

No obstante, el apartado f) prevé la posibilidad recogida en el Considerando 65 en relación a la supresión de datos de menores, esto es, el olvido digital adquiere especial relevancia cuando se refiere a suprimir datos cuyo tratamiento se consintió durante la minoría de edad, y el paso del tiempo, ha conducido al interesado (ahora ya mayor de edad) a pretender la supresión de dicha información. Cabe señalar, que la presente tesis doctoral, se centrará en el estudio específico del ejercicio derecho al olvido en el contexto digital. Principalmente, porque consideramos que prevé una herramienta de control de la

información personal que los más jóvenes hasta el momento no sienten la necesidad de emplear. En cambio, a nuestro juicio, en un breve lapso de tiempo, la generación que ha crecido inmersa en Internet y redes sociales, perciba la necesidad de eliminar el alud de información compartida en estos espacios al llegar a una edad más adulta, para lo que el derecho deberá articular garantías eficaces que aseguren dicha desaparición de la información.

Así las cosas, los proveedores de redes sociales, como responsables del tratamiento, deberán ofrecer sin dilación indebida la supresión de los datos personales que le conciernan al interesado. Conforme con esta afirmación se muestra BERROCAL LANZAROT cuando dispone que, los responsables de tratamiento pueden ser, webmaster, motores de búsqueda, proveedores de redes sociales, hemerotecas digitales, etc[880]. Antes bien, en ocasiones se percibe que el ejercicio del derecho de supresión se relaciona exclusivamente en la actividad de los motores de búsqueda. Ciertamente, tanto el TJUE como las instituciones europeas[881], han desarrollado en mayor medida el ejercicio de este derecho en el mencionado escenario, sin embargo, el derecho de supresión también puede ejercerse frente a otra clase de responsables del tratamiento, como proveedores de redes sociales.

Por otra parte, el derecho de supresión no presenta carácter absoluto. El propio art. 17.3 RGPD enumera una serie de limitaciones a su ejercicio que habrán de someterse a valoración. En concreto, no podrá prevalecer la supresión ante: a) el ejercicio del derecho de información y expresión[882]; b) el cumplimiento de una obligación legal o misión en interés público, así como ejercicio de poderes públicos conferidos al responsable; c) razones de interés público en el ámbito de la salud pública; d) fines de archivo en interés público, fines de investigación científica, histórica o fines estadísticos; y por último el apartado e) la formulación, ejercicio o defensa de reclamaciones.

---

[880] BERROCAL LANZAROT, A.I., *Derecho de supresión de datos o derecho al olvido,* Madrid, Reus, 2017, p. 219.

[881] En efecto, el CEPD cuando se pronuncia sobre el derecho de supresión o al olvido digital realiza una serie de recomendaciones de ejercicio de este derecho exclusivamente en el ámbito de motores de búsqueda. Véanse las Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD, de 7 de julio de 2020.

[882] Para más detalle sobre la ponderación entre el derecho a la supresión y los derechos de expresión e información en conflicto cuando el olvido digital se ejercita ante buscadores de Internet, véase BERROCAL LANZAROT, A.I., *Derecho de supresión de datos o derecho al olvido, op. cit.,* pp. 242-260.

En definitiva, la normativa sobre protección de datos personales prevé la posibilidad de ejercitar la supresión de datos personales frente a proveedores de redes sociales. Además, los menores de edad, como titulares del derecho fundamental a la protección de datos personales, se encuentran habilitados para solicitar la supresión de información frente a proveedores de redes sociales, y especialmente, cuando se encuentren en la circunstancia que contempla el art. 17.1.f) RGPD.

En ese sentido, el legislador europeo supo anticipar el gran dilema ante el que se encontrarán millones de jóvenes, que durante su minoría de edad consintieron el tratamiento de datos de un elevado volumen de informaciones concernientes a su persona, en un entorno que tiende al recuerdo perpetuo como la red. Como garantía adicional a favor de los menores, el art. 17.1.f) RGPD concede la posibilidad de ejercitar el derecho de supresión sin necesidad de probar ninguno de los supuestos enumerados en las letras a) a la d) de ese mismo precepto[883]. En consecuencia, lograr la supresión de la información concerniente a menores de edad resulta formalmente más sencillo, lo que debe valorarse positivamente.

Por último, sin ánimo de detallar, pues no constituye objeto de análisis del presente epígrafe, el art. 17.2 RGPD dispone que, cuando el responsable del tratamiento realizare públicos datos personales cuya supresión se solicita, deberá informar a los responsables que traten dichos datos, que eliminen cualquier enlace a dicha información o cualquier copia o réplica que de los mismos conserven. Así, como consecuencia del considerando 66, el olvido debe alcanzar, igualmente, a la información que terceros traten y cuya supresión se solicite por parte del interesado. El presente precepto, cobra especial relevancia en el ámbito de las redes sociales por dos motivos. Por una parte, la información que en ellas se publica o recopila (activa y pasiva) se comparte con terceras empresas (generalmente anunciantes), que en lo sucesivo tratarán dichos datos. Por otra

[883] Así las cosas, la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, prevé el ejercicio del derecho a la supresión u olvido digital basándose en que el tratamiento de datos personales del Sr. Costeja podía responder a fines lícitos en un inicio (dotar de publicidad la subasta derivada del embargo de bienes), pero que el paso de tantos años (prácticamente 20), ocasionaba que los fines para los que se trató dicha información no devinieran necesarios en la actualidad. Puede verse como en la actualidad, la esencia de dicha aseveración se encuentra presente en el art. 17.1.a) del RGPD. Por otra parte, ello no obsta que, habrá de analizarse caso por caso si los fines continúan resultando legítimos en la actualidad, lo que conducirá a pronunciamientos diversos dependiendo de los hechos. Sin embargo, para el caso de menores de edad que deseen suprimir dicha información, el logro de la supresión se prevé más sencillo, pues basta con demostrar que el consentimiento se prestó durante la minoría de edad, junto con el deseo de retirar la información disponible.

parte, muchos perfiles activos en estos espacios se configuran de modo público. Sobre este aspecto volveremos más adelante.

4.2. El diferente camino normativo seguido por el legislador español en la regulación del derecho al olvido digital en la LOPDGDD

El legislador español decide regular el derecho al olvido digital siguiendo un camino diferente al planteado por el legislador europeo[884]. En efecto, mientras que en el ámbito europeo el RGPD no realiza distinciones entre los responsables ante los que se puede ejercitar el derecho de supresión, ofreciendo una regulación unitaria al respecto, en el ámbito nacional se regula, por una parte, el olvido digital ante buscadores de Internet (art. 93 LOPDGDD); por otra parte, frente a redes sociales y servicios equivalentes (art. 94 LOPDGDD).

En ese sentido, parte de la doctrina critica fuertemente dicha decisión, destacando entre ellas la de GARROTE FERNÁNDEZ-DÍEZ cuando afirma que llevar a cabo una regulación fragmentada del derecho al olvido digital se opone frontalmente al espíritu del RGPD que se identifica con agrupar todos los supuestos de ejercicio del derecho de supresión[885]. Por contra, RALLO LOMBARTE defiende el planteamiento del legislador nacional, considerando que este ha procurado adaptar la normativa a la sentencia del TJUE, de 13 de mayo de 2014, en el art. 93 LOPDGDD por una parte; y por otra, ha extendido la doctrina aplicable a buscadores a los restantes responsables del tratamiento *online* (art. 94 LOPDGDD)[886]. A nuestro juicio, compartimos en parte la decisión adoptada por el legislador nacional, en el sentido que, resulta previsible que las particulares características de los servicios prestados por cada uno de los responsables del tratamiento *online*, generen necesidades que propicien garantías específicas para el eficaz

[884] Al amparo del Considerando 10 del RGPD, los Estados miembros se encuentran habilitados para introducir especificaciones sobre el tratamiento de datos personales en sus respectivas normativas nacionales.

[885] GARROTE FERNÁNDEZ, I., "La regulación del derecho al olvido en los arts. 17 y 21 del RGPD y en el art. 93 de la LOPDGDD", en GONZÁLEZ PACANOWSKA, I., (Coordinadora), *Protección de datos personales*, *op. cit.*, p. 395.

[886] RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales*, *op. cit.*, pp. 38-39.

ejercicio del derecho de supresión[887]. En efecto, el art. 94 LOPDGDD adapta el ejercicio del olvido digital en el ámbito de las redes sociales, lo que resulta loable, habida cuenta que se constituye como un ámbito en el que se tratan datos de manera constante. Estas afirmaciones, conduce a que el principio de calidad de los datos pueda vulnerarse con gran facilidad, dado que el transcurso del tiempo puede influir en la exactitud, pertinencia y actualización de la información personal[888].

Tras el análisis del art. 94 LOPDGDD, observamos que el legislador ha regulado el ejercicio del derecho al olvido frente a los proveedores de redes sociales; en ese sentido, el precepto prevé determinadas particularidades cuando este se ejercita frente a los prestadores de los señalados servicios. Véase que el apartado primero del art. 94 dispone que el interesado podrá solicitar la supresión de los datos que hubiera publicado en redes sociales y el responsable deberá proceder a su "simple solicitud". Adviértase, que no habrán de concurrir ninguno de los presupuestos del art. 17 RGPD letras a) a f); la simple solicitud del interesado constituirá elemento suficiente para que deba garantizarse la supresión de la información. Así, se prescinde del juicio de ponderación que el grueso de jurisprudencia y doctrina analiza cuando la supresión se solicita a buscadores o hemerotecas digitales.

Por otra parte, se ha destacado en varias ocasiones, que terceras personas no titulares de la información que comparten, pueden propiciar el tratamiento de datos personales en redes sociales cuando publican información sobre amistades, familiares, etc. Consciente de dicha circunstancia, se incluye en la LOPDGDD el apartado segundo del art. 94, que sienta las bases para la supresión de la información proporcionada por terceros a la red social y que, su titular desea eliminar. Así las cosas, podrán solicitar la supresión cuando los datos resulten inadecuados, inexactos, no pertinentes, 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, y siempre que no concurra la excepción doméstica en el tratamiento del tercero. Cabe señalar que, en efecto, las

[887] Tal y como afirma ADSUARA, el art. 94 LOPDGDD regula el derecho al olvido aplicado a un tratamiento concreto. ADSUARA, B., "Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento)", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales*, Valencia, Tirant lo Blanch, 2019, p. 323.

[888] RALLO LOMBARTE, A., "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales, op. cit.*, p. 40.

consideraciones sobre la inexactitud de los datos, el transcurso del tiempo, así como la naturaleza e interés público de la información analizados previamente, despliegan plena eficacia en este art. 94.2 LOPDGDD, en orden a valorar la procedencia de la supresión de la información compartida por terceros usuarios en redes sociales[889].

No obstante, en cuanto a la eficacia sobre la excepción doméstica, debemos recordar aquellas situaciones establecidas en el Dictamen 5/2009 en las que los usuarios de redes sociales pueden no quedar amparados por la misma. Puesto que, si bien es cierto que la excepción doméstica opera como un límite al ejercicio del derecho de supresión, cabe prever que ejercitar el derecho de supresión devendrá imposible al quedar muchos tratamientos amparados por la excepción. Sin embargo, otro gran número de tratamientos practicados por usuarios, no recaerá en el ámbito de aplicación de la misma y deberá garantizarse la supresión efectiva de la información personal. Consideramos que, deberían precisarse con mayor rigor aquellos tratamientos de datos que en redes sociales no quedan amparados por la excepción doméstica, ya que, de lo contrario, devendrá complejo garantizar la supresión de la información aportada en el descrito contexto. Es de intuir que, por defecto, se considere que el tratamiento de información de un tercero publicada en redes sociales, recae en la excepción doméstica y por ende, no se garantice su supresión. Lamentamos así, que el legislador haga depender esta facultad de una materia sobre la que quedan cuestiones por aclarar.

Por último, el apartado tercero del art. 94 LOPDGDD, refuerza, al igual que el RGPD, el olvido digital cuando el titular de los datos no alcanzaba la mayoría de edad al momento de compartirlos con el proveedor de la red social. En ese sentido, tal y como se ha expuesto en apartado precedentes, cuando los datos se facilitasen al proveedor de la red social durante la minoría de edad, este deberá proceder a su supresión (se compartieran estos por el titular o terceros) por la simple solicitud, no debiendo concurrir las circunstancias del apartado segundo recientemente expuestas[890]. Sin lugar a dudas, el

[889] Recuérdense sobre esta cuestión las sentencias del TS: Sentencia del Tribunal Supremo 545/2015, de 15 de obtubre, Sentencia del Tribunal Supremo 12/2019, de 11 de enero de 2019 o Sentencia del Tribunal Constitucional 89/2022, de 29 de junio, citadas todas previamente.

[890] Sin embargo, el Estado de California ya contemplaba en una ley la posibilidad de que todos los menores de dieciocho años pudieran solicitar la supresión de forma permanente de toda la información compartida por estos en redes sociales. California Senate Bill 568, Privacy, Internet, minors, Approved by Governor September 23. Obtenido de: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (última consulta el 21 de febrero de 2023).

espíritu del legislador se alinea con el deseo del Considerando 65 RGPD cuando busca garantizar el olvido de la información digital de menores. Efectivamente, el ejercicio del derecho al olvido digital por parte de menores de edad con mayores facilidades, se propone evitar los perjuicios que pudiera causarles en el futuro el excelso volumen de información difundido en redes sociales[891].

En suma, nos mostramos favorables a la previsión del ejercicio del derecho de supresión al ámbito de las redes sociales. Sin embargo, llama la atención que el art. 15 LOPDGDD, cuyo objeto constituye la regulación del derecho de supresión, remita al art. 17 RGPD en su integridad, de modo que, resulta incoherente la posterior distinción que del mismo se efectúa en el Título X relativo a los derechos digitales[892]. Entendemos que la incorporación al Título X de este derecho manifiesta una falta de sistemática por parte del legislador. Convendría que la misma se hubiera realizado en el art. 15 LOPDGDD que regula este derecho en orden a evitar confusiones, puesto que el RGPD goza de aplicación directa en los Estados miembros[893].

Por otra parte, si bien es cierto que el legislador ha sabido prever la necesidad de adaptar la supresión de la información a este ámbito tan presente en el día a día, especialmente de menores, conviene ahora preguntarnos sobre la posibilidad real y efectiva de eliminar los datos compartidos en redes sociales *online*. El reto resulta mayúsculo, por cuanto que, al contrario de lo que acontece en los buscadores de Internet, donde el desindexado de la información del buscador ha de entenderse por olvido a pesar de que la información permanezca accesible en la fuente de origen, la información

[891] ADSUARA, B., "Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento)", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales, op. cit.*, p.35.

[892] También cabe mencionar la sorpresa que generó la inclusión repentina del Título X de la LOPDGDD tras la enmienda planteada por el Grupo Socialista, tal y como se ha mencionado anteriormente. En ese sentido, también muestra su asombro HERRÁN ORTÍZ tildando la incorporación del derecho al olvido digital, por encontrarse inmerso en el señalado título de "apresurada". HERRÁN ORTÍZ, A.I., "¿Nuevos tiempos, nuevos derechos?:A propósito del difícil olvido en Internet", en EMALDI CIRIÓN, A., y LA SPINA, E., (Editoras), *Retos del Derecho ante un mundo global, op. cit.*, p. 41.

[893] Somos conscientes de que, quizás, el legislador ha querido otorgar a esta facultad la condición de derecho fundamental autónomo incluyéndolo en un Título concerniente a nuevos derechos digitales de los interesados. Sin embargo, TC no termina de confirmar tales aspiraciones, pues la ambigüedad con la que el TC se manifiesta en su sentencia 58/2018, de 4 de julio de 2018, no termina de permitir el reconocimiento de tal proclamación. En efecto, puede parecer en su Fundamento jurídico sexto, que el Tribunal se decanta por proclamar el derecho al olvido como un derecho fundamental autónomo; pero a su vez, el Fundamento jurídico quinto dispone que el llamado derecho al olvido constituye una facultad o dimensión del derecho a la protección de datos personales. Véase así la Sentencia del Tribunal Constitucional 58/2018, de 4 de julio de 2018, Boletín Oficial del Estado, de 7 de julio de 2018, núm. 164, pp. 68409 a 68433.

personal cuya supresión se solicita al proveedor de la red social, no puede suprimirse por medio de dicha técnica como quedará de manifiesto.

5. DIFICULTADES EN LA SUPRESIÓN U OLVIDO DIGITAL DE DATOS PERSONALES DE MENORES EN REDES SOCIALES

A pesar de que la LOPDGDD contemple expresamente un precepto cuyo fin constituye garantizar una supresión de los datos personales compartidos en redes sociales, concurren varios motivos que conducen a estimar dificultoso el logro de una eliminación eficaz de la información personal compartida en dichos espacios.

5.1. ¿El olvido digital se identifica con el desindexado en el contexto de redes sociales?

Como ha quedado expuesto, el desarrollo del derecho al olvido digital se ha orientado, principalmente, a su ejercicio en el ámbito de los buscadores de Internet o motores de búsqueda *online*. En verdad, el grueso de la doctrina, jurisprudencia, así como organismos públicos de datos personales, se han centrado en aclarar los diversos aspectos que engloban el ejercicio del mentado derecho en el ámbito de los motores de búsqueda[894]. Incluso determinados autores como GUICHOT, identifican el derecho al olvido como un equivalente al "derecho al desindexado"[895]. El TJUE, por su parte, también ha empleado dicha denominación, que no compartimos por los motivos que se expondrán a continuación[896].

Asentado que el derecho de supresión puede solicitarse frente a diversos responsables del tratamiento[897] (el art. 17 RGPD se refiere al responsable del tratamiento

[894] El propio CEPD señala en el párrafo sexto de las Directrices 5/2019, sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD, de 7 de julio de 2020, que el presente documento se centra únicamente en el tratamiento de los proveedores de motores de búsqueda.

[895] GUICHOT, E., "El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español", *Revista de Administración Pública,* 2019, núm. 209, p. 88.

[896] Incluso TJUE lo ha denominado de ese modo en su sentencia, de 24 de septiembre de 2019, *Google LLC contra Commission nationale de l'informatique et des libertés (CNIL),* Asunto C- 136/17.

[897]Conforme con esta afirmación se muestra ÁLVAREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en RECIO GAYO, M., Y PIÑAR MAÑAS, J.L., (Directores) *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad, op. cit.,* p. 247, cuando afirma que el derecho al olvido digital se puede ejercer ante todo responsable del tratamiento, más allá de los motores de búsqueda; y continúa sentando que, en ese caso, se podrá ejercer frente a blogs, redes sociales, etc.

en general y la LOPDGDD contempla, además de la remisión al mentado precepto, el ejercicio del olvido ante buscadores y redes sociales), no encontramos criterios que delimiten las circunstancias a valorar para su ejercicio en ámbitos diferentes a los motores de búsqueda *online*, ni siquiera en la jurisprudencia más reciente[898]. Efectivamente, la LOPDGDD prevé explícitamente la posibilidad de ejercitar la supresión de la información frente a proveedores de redes sociales, pero mientras que el art. 93.1 LOPDGDD, detalla en mayor medida cómo articular la supresión, pues incluso establece en el tercer párrafo del precepto que la información podrá conservarse en la fuente original, el art. 94.2 LOPDGDD, parcamente dispone que toda persona podrá solicitar la supresión de "los datos personales que hubiese facilitado para su publicación por servicios de redes sociales". Además, la doctrina y los organismos oficiales tampoco se han pronunciado al respecto[899].

En ese sentido, pese a que los motivos previstos en el art. 17 RGPD que pueden conducir a la solicitud exitosa de la supresión, gozan de plena aplicabilidad frente a los proveedores de redes sociales (con especial énfasis el art. 17.1 a) RGPD, pues el tiempo y la exactitud de los datos se constituyen como factores determinantes para dilucidar la permanencia de la información en la plataforma o no), las dificultades se presentan al determinar cómo proceder a la eliminación eficaz de la información susceptible de supresión. La jurisprudencia citada en la presente investigación, aboga por el desindexado de la información como solución a efectos de garantizar un olvido digital, aseverando que la información deberá continuar disponible en la fuente original. En efecto, la información no se oculta, suprime o bloquea, sino que se limita o dificulta el acceso general a la misma[900]. Incluso dicha premisa ha inspirado el art. 93.2 LOPDGDD en relación al desindexado de búsquedas en motores de Internet. Antes bien, en el ámbito de las redes sociales, no puede emplearse dicha técnica como medio de solución. Principalmente, porque la información permanece disponible en un perfil, lo que en nada se asemeja con

[898] Resulta cuestionable esta dejadez, ya que, por ejemplo, la jurisprudencia europea y nacional se vieron forzadas a matizar que ejercitar el derecho al olvido frente a motores de búsqueda no alcanzaba a eliminar la información de la fuente original DÍAZ DÍAZ, E., "Derecho al olvido en línea (Comentario a los artículos 93 y 94 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales*, Madrid, Civitas, 2021, p. 4287.

[899] Efectivamente, no hemos encontrado directrices que arrojen claridad sobre el ejercicio del derecho de supresión en el ámbito de las redes sociales.

[900] HERRÁN ORTÍZ, A.I., "¿Nuevos tiempos, nuevos derechos?:A propósito del difícil olvido en Internet", en EMALDI CIRIÓN, A., y LA SPINA, E., (Editoras), *Retos del Derecho ante un mundo global, op. cit.*, p. 61.

la introducción de nombre y apellidos en un buscador que, como resultado, proporciona la información de la página original en la que la misma se publicó.

Esta particularidad trae causa de las diferencias entre el funcionamiento de los motores de búsqueda y las redes sociales. Mientras que, en el primer servicio, el motor de búsqueda busca archivos y los almacena en sus servidores, operando como intermediario de información previamente publicada en la red, el servicio de redes sociales propicia la creación de contenidos por parte de los usuarios a través de sus interacciones o empleo del servicio.

Consecuentemente, consideramos que el ejercicio del derecho al olvido digital de datos personales frente a proveedores de redes sociales no equivale al desindexado de los mismos en los motores de búsqueda tras la introducción de nombre y apellidos como parámetro de búsqueda, sino a la eliminación de la información por parte del proveedor de servicios en caso de solicitud por parte del interesado[901]. Efectivamente, de conformidad con ANGULO GARZANO, el derecho de supresión se ejercita de manera diferente en función de si la información se muestra accesible a través de motores de búsqueda o si la misma se expone en redes sociales o servicios equivalentes[902]. Por tanto, sorprende que el propio TJUE constriña el derecho de supresión al "derecho a retirar enlaces", cuando de la vis expansiva en el concepto del responsable en la redacción del art. 17 RGPD cabe interpretar que el olvido puede ejercitarse frente a todo tipo de responsables del tratamiento, en los que se debe incluir, a los proveedores de redes sociales. En el caso nacional, estas afirmaciones cobran mayor rotundidad, pues el propio legislador español ya diferencia el ejercicio del derecho frente a cada uno de los prestadores de servicios en su normativa. En cambio, lo que sobre la normativa parece un gran avance, no se ha trasladado a las vicisitudes prácticas que puedan posibilitar dicha supresión con una mayor eficacia en el ámbito de las redes sociales.

[901] De acuerdo con esta consideración se muestra SANTOS MORÓN cuando establece que el ejercicio del derecho al olvido frente a los servicios de redes sociales, a diferencia de los motores de búsqueda, sí implica la eliminación de los datos personales cuya supresión se solicita. SANTOS MORÓN, Mª. J., "Los contornos del derecho al olvido en España. La aplicación por los Tribunales españoles de la jurisprudencia europea", *Revista de Derecho civil*, abril-junio 2022, núm. IX, p. 99.

[902] ANGULO GARZANO, A., "El derecho al olvido en los motores de búsqueda y en las redes sociales a la luz de la nueva normativa de protección de datos", *Actualidad Administrativa La Ley*, 2019, núm. 4, p. 5.

Como puede apreciarse, el contexto que se plantea propone una supresión total y efectiva de la información, como mínimo, del perfil de la persona solicitante[903]. Sin embargo, aparecen varias dificultades en su logro. Conforme con la consideración expuesta se muestra el Grupo de Trabajo del art. 29 en su Dictamen 5/2009 sobre redes sociales en línea cuando afirma que, la información eliminada por el usuario cuando actualice su cuenta no debería conservarse por parte del proveedor de la red social, antes bien, este continúa tratando dichos datos, principalmente con fines de mercadotecnia directa. A mayor abundamiento, señala el organismo que los datos personales comunicados por el usuario al proveedor de la red social deberían suprimirse cuando el usuario decide darse de baja y cancelar su cuenta y no esperar que este, deba ejercitar el derecho de supresión en orden a evitar que la red social continúe tratando la información. Por último, también señala que cuando el usuario no emplee el perfil durante un tiempo determinado, este debería desactivarse y dejar de mostrarse visible para el resto de usuarios y pasado otro período de tiempo, los datos de la cuenta abandonada deberían resultar objeto de supresión[904].

Así las cosas, sin embargo, los proveedores de redes sociales se comportan de manera contraria a las consideraciones expuestas. En efecto, tal y como dispone la CNIL, en contra de lo que la mayoría de personas jóvenes creen, la eliminación de la cuenta o la aplicación, no supone la supresión de la información personal[905]. Esto es, en la primera situación (eliminación de la cuenta), los datos dejan de mostrarse visibles al público, pero el proveedor de la red social continúa tratando los mismos salvo que se solicite la supresión por parte del interesado; en la segunda circunstancia (eliminación de la aplicación), en cambio, el usuario deja de emplear el servicio, pero los datos continúan visibles, además de susceptibles de tratamiento por parte del proveedor de la red social. Por otra parte, el desuso del perfil del que se dispone en la red social, no supone la desactivación de la cuenta, ni la supresión de la información tras un período de tiempo,

[903] Quizás este planteamiento responda a lo que, en el contexto de ejercitar la supresión frente a proveedores de redes sociales, DÍAZ DÍAZ califica de una obligación de resultado que habrá de alcanzarse efectivamente. DÍAZ DÍAZ, E., "Derecho al olvido en línea (Comentario a los artículos 93 y 94 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales, op. cit.,* p. 4290.
[904] Dictamen 5/2009 del Grupo de Protección de datos del Artículo 29 sobre las redes sociales en línea, de 12 de junio de 2009, WP 163, p. 11.
[905]Informe de la Comisión francesa de protección de datos (CNIL) sobre las prácticas digitales de los jóvenes entre 11 a 18 años. Obtenido de: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf , p. 8. (última consulta el 29 de agosto de 2022)

lo que facilita la disponibilidad perpetua de la información. Contribuye a ello, igualmente, que el usuario no se detiene a valorar que sus datos no se eliminan, cuestión de la que tampoco se le informa con claridad por parte del responsable. Como puede apreciarse, los proveedores de redes sociales han diseñado un sistema que tiende a perpetuar la disponibilidad de la información personal, lo que contraviene la normativa sobre protección de datos personales, concretamente, el principio de limitación del plazo de conservación (art. 5.1. e) RGPD).

Por todo lo expuesto, consideramos que, la eliminación de la cuenta (la solicitud de baja de los servicios ofertados por la red social) debería conllevar la supresión automática de la información personal del usuario. Por el contrario, los proveedores de redes sociales continúan empleando dicha información personal a efectos de construir perfiles de los interesados con fines de mercadotecnia directa, entre otros. De igual modo, en caso de que se solicite la supresión de informaciones personales concretas y determinadas mientras la cuenta permanece en activo, el proveedor de la red social debe abandonar todo tipo de tratamiento practicado sobre dichos datos, incluidos aquellos que realiza con fines de mercadotecnia directa (sobre este aspecto volveremos en apartados posteriores). Efectivamente, la supresión de la información no puede corresponderse únicamente con retirar los datos personales de la visibilidad del público de la red, sino que el responsable del tratamiento (proveedor de la red social) ha de abandonar cualquier tratamiento practicado sobre dicha información.

Además, la supresión total de la información en redes sociales, resulta menos dificultosa desde el punto de vista de otros derechos fundamentales implicados, por cuanto que, cuando se trata de ejercitar el derecho de supresión frente a buscadores por información publicada en prensa *online* o en hemerotecas digitales, el derecho de información puede vencer el derecho de protección de datos personales al amparo del art. 17.3 RGPD. Pero la ponderación no resulta la misma en caso de que la supresión se solicite frente a proveedores de redes sociales que no quedan resguardados por el paraguas del derecho constitucional de información[906]. Los proveedores de redes sociales constituyen entidades privadas con intereses meramente privados y estos intereses en

[906] Recordemos a tal efecto, la Sentencia del Tribunal Supremo 545/2015, de 15 de octubre de 2015 citada anteriormente.

ningún caso prevalecen sobre la privacidad de los usuarios de redes sociales, ni sobre el derecho a acceder a dicha información por parte del resto de usuarios[907].

A pesar de lo expuesto, el paradigma del olvido digital colisiona con dificultades que prácticamente imposibilitan una supresión completa y efectiva de la información personal compartida en redes sociales.

5.2. Los hábitos del usuario en redes sociales: un impedimento para la eficaz supresión de datos personales

El funcionamiento de las redes sociales presenta importantes obstáculos cuando se trata de garantizar la eficaz supresión de los datos compartidos en la plataforma *online*. Sobre este particular, recordemos que, el usuario adopta en redes sociales un papel activo, comentando y compartiendo informaciones propias y de terceras personas. Así, el legislador español, desligándose de la propuesta del RGPD, toma conciencia a través del art. 94.2 LOPDGDD de la posibilidad de que el usuario suprima la información que no se ha publicado por este en primera persona, sino por terceros. A tal efecto, habilita la supresión cuando estos datos resulten inadecuados, inexactos, no pertinentes, 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. Véase que el proveedor de la red social no deberá proceder a la supresión por la simple solicitud del usuario cuando la información se ha publicado por este en primera persona (art. 94.1 LOPDGDD).

Ahora bien, advertimos diversos obstáculos que dificultan, en la práctica, la eficacia del precepto en cuestión y que se expondrán como sigue.

En efecto, el precepto concede la posibilidad de solicitar la supresión que terceros publiquen sobre la persona interesada. Ahora bien, el lapso de tiempo en el que los datos han permanecido disponibles en la red propicia que la información pueda descargarse y

[907] Consideramos oportuno extender la argumentación del apartado 81 de la sentencia del TJUE, de 13 de mayo de 2014 sobre el caso Mario Costeja a la solicitud de supresión de la información frente a proveedores de redes sociales, cuando el tribunal europeo señala que: «*Ya que el interesado puede, habida cuenta de sus derechos con arreglo a los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, es necesario considerar, como se desprende, en particular, del apartado 81 de la presente sentencia, que estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona*».

almacenarse por terceros usuarios de la plataforma en sus dispositivos personales. Así, los *smartphone*, tabletas u ordenadores, permiten la generación de capturas de pantalla y vídeo que contribuyen a que las imágenes, comentarios, vídeos, etc., de un usuario puedan almacenarse en dispositivos de uso personal de terceros. Como es de intuir, las consecuencias en orden a garantizar la supresión resultan devastadoras en el presente contexto. Ello se debe a la evidente pérdida de control que el usuario sufre una vez los datos se descargan y almacenan por terceros, puesto que, no existe un modo de conocer los usuarios que proceden a su recopilación en dispositivos personales, por ende, tampoco cabe garantizar una supresión total de dichos datos[908].

Nos preguntamos si cabría establecer un sistema en redes sociales que obligara a los mentados proveedores a informar y notificar a los usuarios que descarguen datos, de que se ha solicitado la supresión de los mismos en la plataforma. Sin embargo, ello podría colisionar con la excepción doméstica (art. 2.2.c) RGPD), ya que, es de intuir que los usuarios almacenen dichos datos para su uso o almacenamiento personal. Ahora bien, no en todo caso, ya que constituye un comportamiento habitual compartir masivamente publicaciones con otros usuarios en vez de proceder a su almacenamiento personal y privado. Efectivamente, muchos usuarios reciben dicha información y vuelven a compartirla con otros usuarios que, a su vez, procederán del mismo modo. En consecuencia, esta funcionalidad disponible en las redes sociales imposibilita que los usuarios ejerzan un control efectivo sobre sus datos personales, lo que contraviene el contenido esencial del derecho a la protección de datos personales. Por tanto, dado que de nada sirve solicitar el olvido ante la red social si después los usuarios pueden volver a compartir la información que objeto de supresión, este sistema de notificación parece el idóneo para que los usuarios conozcan que no deberían volver a divulgar tales datos personales.

Concretamente, el art. 94.3 LOPDGDD que aboga por garantizar en mayor medida la supresión de datos concernientes a menores de edad, no logra su pretensión dadas las características de diseño de las plataformas sociales. Los menores de edad, que además comparten muchos datos, perderán el control de la información compartida al

[908] SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital,* Valencia, Tirant lo Blanch, 2012, pp. 159-160.

encontrarse susceptible de descarga por parte de la red. Así las cosas, consideramos que, dado el espíritu que la normativa actualmente vigente en relación al olvido digital plantea para la protección del menor, debería considerarse que los perfiles cuya titularidad recae en un menor de edad no pudieran almacenar información personal en sus dispositivos personales para así evitar su posterior difusión. Sin duda, se articula como una medida que podría mitigar el riesgo a no lograr una supresión eficaz de la información.

En otro orden de cosas, el comportamiento activo de los usuarios de redes sociales, conduce a que un determinado número de ellos, bajo determinadas circunstancias, puedan considerarse responsables del tratamiento (art. 4.7 RGPD). Ello ocurrirá, en virtud del Dictamen 5/2009, sobre redes sociales en línea, cuando posean un elevado número de seguidores o un perfil configurado de modo público en el que la totalidad de la red posee acceso (entre otros). En consecuencia, estos usuarios asumirán a su vez, el papel de responsables del tratamiento, lo que les compele a cumplir con las obligaciones de un verdadero responsable del tratamiento de datos personales. Entre estas obligaciones, destaca por encontrarse en sintonía con el presente epígrafe, la necesidad de garantizar la supresión (olvido digital) de los contenidos que sobre terceras personas publiquen.

A causa de la circunstancia descrita, apuntamos las siguientes consideraciones. En primer lugar, tal y como se ha expuesto en apartados precedentes, se han de clarificar con rigor aquellas situaciones en las que el usuario de redes sociales no queda amparado por la excepción doméstica (art. 2.2.c) RGPD) y, en consecuencia, su comportamiento en redes sociales puede conducirle a observar las obligaciones de un responsable del tratamiento[909]. En segundo lugar, se debe advertir que esta circunstancia genera una situación anómala en la que, el usuario responsable de tratamiento, no posee la técnica para garantizar la supresión definitiva de la información disponible en la red. Esto es, el usuario puede eliminar de su perfil los datos cuya supresión se solicita, pero ello no constituye sinónimo de supresión para los proveedores de redes sociales, que pueden continuar sometiendo a tratamiento dichos datos en caso de que no se eliminen de sus

[909] Coincidimos con COTINO HUESO en que, se podría haber aclarado en la Carta de Derechos Digitales el alcance del derecho de supresión de información compartida por terceros usuarios responsables del tratamiento. Sin perjuicio de que, a nuestro juicio, se deban conceder por los órganos judiciales y autoridades de control aclaraciones al respecto, ya que, la carta no resulta jurídicamente vinculante. Así, COTINO HUESO, L., "Expresión, información, creación y acceso a la cultura. Libertades y responsabilidades de usuarios y plataformas en entornos digitales (XIV, XV, XXIV)", en COTINO HUESO, L., (Coordinador) *La Carta de Derechos Digitales,* Valencia, Tirant lo Blanch, 2022, p. 219.

servidores[910]. Por ello, a nuestro juicio, sería conveniente que el derecho de supresión se ejercitara siempre frente al proveedor de la red social (al poseer este la técnica requerida), sin perjuicio de que, este deba informar al usuario responsable sobre la aceptación de la supresión de determinados datos que, este deberá eliminar a su vez (las copias o réplicas que posea) en virtud del art. 17.2 RGPD[911].

Por otra parte, el art. 17.2 RGPD establece que el responsable del tratamiento, cuando realice públicos determinados datos personales, deberá informar a los responsables del tratamiento que se encuentren tratando estos datos, que supriman todo enlace, copia o réplica a los mismos. En este sentido, los proveedores de redes sociales, tal y como ha quedado probado en apartados precedentes, además de hacer públicos datos de perfiles configurados de ese modo, también comparten un sinfín de datos personales de los usuarios con terceros "colaboradores" o anunciantes, entre otros. En consecuencia, a la obligación de suprimir la información personal objeto de olvido digital, ¿deberá exigirse el deber de informar a terceros que tratan la misma a que procedan a su supresión? Lamentablemente, la doctrina, los organismos oficiales y la jurisprudencia, todavía no se han pronunciado sobre la interpretación que debe concederse a la expresión "hacer públicos" que prevé el art. 17.2 del RGPD. Incluso el propio CEPD señala en sus Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD, que entre los objetivos del documento no se encuentra abordar el análisis e interpretación del art. 17.2 RGPD.

A nuestro juicio, entendemos que los proveedores de redes sociales deben cumplir con mentada notificación, especialmente cuando los perfiles se configuran de modo público. Cierto que, garantizar dicha notificación deviene verdaderamente complejo. Nótese que los proveedores de redes sociales poseen millones de colaboradores, que no

[910] Sobre este particular, recordemos que el art. 94.2 LOPDGDD propugna la supresión de los datos compartidos por terceros siempre que sean inadecuados, inexactos, no pertinentes, 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, y no, en cualquier caso.

[911] Se espera que con el tiempo deban proporcionarse respuestas a este tipo de situaciones, ya que, al igual que ocurrió con el ejercicio del derecho de supresión frente a los buscadores de Internet, se deberá clarificar ante qué responsable del tratamiento habrá de ejercitarse el mentado derecho. Recordemos que, en el ámbito de buscadores *online*, se debe ejercitar el olvido frente al buscador, pudiendo permanecer la información en la fuente original.

identifican en sus políticas de privacidad[912], además de tratar información pública que recopilan de la red. De modo que, contemplamos con escepticismo que el art. 17.2 RGPD resulte objeto de cumplimiento por estas plataformas. Consecuentemente, la información puede continuar disponible en la red o empleándose por terceros, sin que la solicitud de supresión de la misma constituya garantía suficiente de su supresión.

En otro orden de cosas, el papel activo que el usuario asume en las redes sociales e incitado por el funcionamiento de estas, lo conduce a compartir informaciones de otros usuarios en su perfil[913]. A causa de ello, puede ocurrir que el titular de determinados datos ejercite el derecho de supresión de los mismos al proveedor de la red social para que esta los elimine de su perfil, pero esta solicitud no alcanza la eliminación de esa idéntica información que se ha compartido en otros perfiles[914]. En ese sentido, cabe plantearse si la supresión debería extenderse a la eliminación de la idéntica información compartida en otros perfiles y cuya supresión se ha solicitado del perfil de su titular.

En tal sentido, el Abogado General de la Unión Europea MACIEJ SZPUNAR, defiende la posibilidad de obligar a los proveedores de redes sociales a eliminar los contenidos idénticos emitidos por otros usuarios, cuya supresión se ha solicitado por el titular en sus conclusiones de 4 de junio de 2019, Asunto C-18/18[915]. A su juicio, la tecnología fácilmente puede detectar los contenidos idénticos y proceder a su supresión. Así las cosas, convenimos con MACIEJ SZPUNAR, pues aceptar el planteamiento contrario, supondría mostrarse favorables a una formulación que no garantiza la eliminación de la información de la red que el titular desea. Ello se debe a que la supresión se practica sobre la información del perfil del titular, pero esas informaciones que lesionan la protección de datos del usuario, continuarán disponibles y visibles en los perfiles de otros usuarios, además de sometidas a tratamiento por el proveedor de la red social[916].

---

[912] Véase el epígrafe 4.1.1. del Capítulo III.

[913] Sirva como ejemplo que, en la red social Twitter, habitualmente los usuarios tienden a "retwittear" contenidos. Esto es, que los usuarios vuelvan a compartir en sus perfiles informaciones publicadas por otros. También pueden servir de ejemplo las fotografías en las que se etiquetan personas en Facebook

[914] Así, los usuarios de redes sociales tienden a volver a compartir informaciones recabadas de otros perfiles en los suyos propios. En el caso de la red social Twitter, cabe volver a señalar que, la conducta consistente en "retwittear", esto es, volver a compartir información publicada por un usuario, se constituye como la base de la interacción entre usuarios.

[915] Conclusiones del Abogado General de la UE, Maciej Szpunar, de 6 de junio de 2019, Asunto C-18/18. Obtenido de: https://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2122873 (última consulta el 2 de junio de 2022).

[916] Recordemos que, los proveedores de redes sociales recopilan y someten a tratamiento información que terceros comparten sobre los usuarios.

Por último, se ha podido constatar, que la solicitud de supresión de la cuenta no conlleva la eliminación de las fotografías, comentarios, etc. que se hayan compartido en los perfiles de otros usuarios (no nos referimos ahora a idénticos contenidos, sino a contenidos que el usuario comparte en perfiles de terceros usuarios). En efecto, los comentarios realizados a amistades, los "me gustas" proporcionados a sus fotografías, continúan disponibles en los perfiles de estos terceros usuarios[917]. Así las cosas, de conformidad con ENISA, los proveedores de redes sociales deben diseñar herramientas que garanticen la completa eliminación de las cuentas de los usuarios, lo que, a nuestro juicio, incluye la supresión de toda la información vinculable al usuario que solicita la eliminación y no solamente la que permanece en su perfil. De igual modo, el organismo europeo propone permitir a los propios usuarios, eliminar por sí mismos los comentarios y publicaciones realizados en perfiles de terceros[918], medida que consideramos positiva para los casos en los que se desea continuar empleando el perfil. No obstante, los propios proveedores también deberían proceder a la eliminación de la señalada información, esto es, al abandono total de su tratamiento.

5.3. El derecho de supresión (olvido digital) en tiempos de *big data* e inteligencia artificial

La presente investigación, nos ha llevado a visibilizar que los proveedores de redes sociales han dado con la tecnología capaz de recopilar y tratar un gran volumen de datos proveniente de diversas fuentes con el fin de inferir nuevas informaciones. Así las cosas, los proveedores de redes sociales emplean tecnologías de IA para la elaboración de perfiles de los usuarios, con el fin de compartirlos con empresas anunciantes a las que denominan "colaboradores".

En efecto, la variada información que estos proveedores recopilan como la información que el usuario comparte en su plataforma, se emplea para elaborar un detallado perfil del usuario con fines de mercadotecnia directa.

[917] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, "Security Issues and Recommendations for Online Social Networks", *Position paper,* núm. 1, octubre 2007, p. 11.
[918] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, "Security Issues and Recommendations for Online Social Networks", *Position paper,* núm. 1, octubre 2007, p. 20.

Recordemos a tal efecto que, los potentes algoritmos basados en parámetros de IA, se nutren de un gran volumen de datos personales que se conocen como datos personales de entrada (recopilados de las fuentes expuestas en el párrafo anterior); posteriormente, las técnicas de tratamiento generarán los datos de salida, esto es, el perfil elaborado -con datos inferidos- sobre la persona a la que atañen los datos recopilados. En esencia, se generarán datos personales inferidos de la información primitiva recopilada que guiará a los anunciantes y colaboradores en sus campañas de publicidad.

No obstante, procede destacar ahora las consecuencias que el ejercicio del derecho de supresión de determinada información puede generar en el contexto de tratamientos de datos basados en *big data* e IA. Cabe subrayar, que la solicitud de supresión de informaciones detalladas en el párrafo anterior (datos personales de entrada), suscita la duda sobre si el sistema de IA empleado para inferir informaciones sobre el usuario a través de la elaboración de perfiles, continuará empleando la información cuya supresión se ha solicitado. En ese sentido, la información puede continuar disponible en los servidores del proveedor de la red social, por lo que no parece descabellado plantear, que el olvido digital no alcance a suprimir los datos del sistema que entrena al algoritmo.

En el caso del desindexado de información de motores de búsqueda, la afirmación expuesta adquiere gran visibilidad, puesto que existe un mantenimiento de la información en la fuente original, de modo que, los datos personales continúan disponibles para su recopilación y tratamiento basado en parámetros de IA por parte del proveedor de la red social a pesar de proceder a su desindexación. Efectivamente, los proveedores de redes sociales recopilan datos de libre acceso en la web, por tanto, a pesar de que la información se desindexe del motor de búsqueda, es susceptible de captura en la fuente original y podrá emplearse para la elaboración de un perfil[919].

En efecto, dicho modo de proceder, puede generar fricciones en el contexto de tratamiento de datos basados en componentes de *big data* e IA. Al amparo del art. 93 LOPDGDD, como ya hemos expresado, los datos pueden resultar objeto de supresión cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines

[919] En efecto, a modo de ejemplo, tomando como referencia el caso Mario Costeja analizado en el presente trabajo, el mantenimiento de la información en el periódico La Vanguardia sobre la subasta a causa de las deudas contraídas por el Sr. Costeja, continúa susceptible de captura por los algoritmos basados en IA, lo que puede conducir a que, con dicha información, el algoritmo infiera datos de connotación negativa sobre su solvencia patrimonial.

para los que se recogieron o trataron. De conformidad con el Grupo de Trabajo del art. 29, en caso de que los datos empleados en un proceso de decisión automatizada o elaboración de un perfil resultaren inexactos, cualquier decisión o perfil podrá devenir defectuosos[920]. En consecuencia, el empleo de datos personales obsoletos o incluso cuya supresión se ha solicitado por dichos motivos, puede generar predicciones inadecuadas sobre una persona en caso de continuar empleándose por el algoritmo en orden a inferir nuevos datos.

Los interrogantes manifestados adquieren virtualidad, igualmente, cuando la eliminación de la información se solicita al proveedor de la red social en vez de a un buscador *online*. Así, recordemos que debemos diferenciar dos supuestos diferentes cuando la supresión se ejercita frente a proveedores sociales al amparo del art. 94 LODPGDD: por una parte, en virtud del art. 94.1 LOPDGDD, un usuario de redes sociales, solicita la supresión de determinadas informaciones que compartió como, por ejemplo, fotografías que posteriormente se han empleado por el sistema de IA para reconocer facialmente al usuario. O Igualmente, solicita eliminar determinados comentarios que realizó y se han empleado por la plataforma para engrosar el perfil de este (ideología, gustos, etc.). Por otra parte, el art. 94.2 LOPDGDD, autoriza al usuario a solicitar la supresión de datos compartidos por terceros cuando resulten inexactos, inadecuados u obsoletos. Sin embargo, en ambas circunstancias, al solicitar la supresión de los mismos o alguno de ellos, ¿el algoritmo también abandona el empleo de dicha información o continuará tratándola al haberse empleado la misma para determinar el perfil del usuario con fines de mercadotecnia directa?

La respuesta es especialmente importante desde el punto de vista jurídico. En efecto, el RGPD propugna el principio de exactitud (art. 5.1.d) que el tratamiento de datos deberá cumplir en todo momento. Esto es, los datos deben gozar de exactitud en todo el ciclo de tratamiento y deberán actualizarse en caso necesario; en tal sentido, se adoptarán las medidas necesarias para que se supriman o rectifiquen los datos que carezcan de exactitud para los fines para los que fueron recabados. Así, advertimos que los algoritmos basados en parámetros de IA deben nutrirse en todo momento de datos exactos, por ende,

[920]Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 13.

en caso de que el usuario solicite la supresión de determinadas informaciones, estas no deben continuar alimentando el sistema de IA para la inferencia de informaciones, porque la información inferida, podrá resultar inexacta (Considerando 71 RGPD). Nuestra mayor preocupación reside en que la información que delimitó un concreto perfil de un usuario, continúe empleándose por estos sistemas para la inferencia constante de nuevos datos, ya que, supondría aceptar que estos datos se vinculen con carácter perpetuo al usuario. Además, con toda certeza continuarán empleando informaciones que, por poseer carácter idéntico al solicitado de supresión, continuar siendo publicadas en perfiles de terceras personas[921].

De este modo, los datos obsoletos que han propiciado la solicitud de supresión en virtud del art. 17.1 RGPD (datos de entrada), deben suprimirse igualmente de los servidores del proveedor de la red social para que el algoritmo los somete a tratamiento no pueda emplearlos para la inferencia de nuevas informaciones. De lo contrario, el sistema de IA continuará infiriendo informaciones basadas en datos obsoletos que no resultan acordes al principio de finalidad (art. 5.1.b RGPD) ni al principio de exactitud (art. 5.1.d RGPD). Destacamos así las aportaciones de la AEPD cuando afirma que, los datos asociados de los interesados, bien se traten de datos directamente recogidos o inferidos, han de resultar exactos[922].

A mayor abundamiento, la AEPD dispone que, cuando la etapa de entrenamiento de un sistema de IA finaliza, se debe suprimir la información empleada, a menos que se pueda justificar su tratamiento en otra base legal o resulte necesaria para refinar el sistema. Ahora bien, la AEPD afirma, asimismo que, cuando se haya solicitado la supresión de dichos datos de entrenamiento, se deberá analizar caso por caso la procedencia de su eliminación[923]. En consecuencia, el organismo no identifica los instrumentos que permitan garantizar la supresión de la mentada información personal. Esta situación, puede influir especialmente en menores de edad que desde edades

[921] Efectivamente, con acierto señala GIL MEMBRADO que los proveedores de redes sociales continuarán utilizando materiales que se encuentren publicados en perfiles de terceros, si estos terceros no proceden a su supresión. GIL MEMBRADO, C., "Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales", *op. cit.*, p. 2.
[922] Guía de la AEPD sobre la Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, febrero de 2020. Obtenido de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (última consulta el 8 de junio de 2022), p. 36
[923] Guía de la AEPD sobre la Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, febrero de 2020. Obtenido de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (última consulta 16 de julio de 2021), p. 26.

tempranas emplean Internet y redes sociales, dado que, la falta de madurez del menor puede conducir a que muchas de las informaciones vertidas en redes sociales queden obsoletas con el tiempo; sin embargo, el algoritmo puede continuar empleando este tipo de información obsoleta e inexacta de manera indefinida a pesar de solicitar la supresión de datos.

Por todo ello, la inexactitud u obsolescencia de los datos personales, debe operar también en el contexto de tratamientos basados en parámetros de IA, garantizando a tal efecto, que estos sistemas no emplearán estas informaciones para sus propósitos, con mayor razón si, además, se ha solicitado la supresión de tales informaciones. Efectivamente, ejercitar el derecho de supresión frente a proveedores de redes sociales, a nuestro juicio, no equivale únicamente a eliminar al resto de usuarios de la plataforma o la red al acceso de los datos, sino en que el proveedor de la red social se abstenga practicar en lo sucesivo, cualquier tratamiento sobre la información susceptible de supresión, en lo que deben incluirse los tratamientos basados en parámetros de IA con fines de mercadotecnia directa.

En este sentido, el principio de minimización (art. 5.1.c) RGPD) alcanza especial relevancia en relación al derecho a la supresión, pues cuanto menor resulte la información a recopilar para someter a posterior tratamiento en la consecución de los fines establecidos por el responsable, menor resultará, igualmente, la dificultad a la hora de eliminar los datos susceptibles de supresión. Véase que las redes sociales recopilan información de variadas fuentes, valorando positivamente el almacenamiento cada vez mayor de datos para su posterior tratamiento. En el contexto descrito, la dificultad para eliminar el alud de datos de entrada, unido a los datos que se generan, a su vez, de salida, resulta evidente.

En otro orden de cosas, hasta la fecha, únicamente se ha contemplado la posibilidad de que el derecho de supresión alcance la eliminación de informaciones concretas cuya supresión se solicita. Ciertamente, únicamente se ha planteado la posibilidad de solicitar la supresión de los datos que, en este nuevo paradigma de tratamiento de datos, constituirán los datos de entrada para el algoritmo. Antes bien, ante los nuevos y sofisticados tratamientos de datos personales que los proveedores de redes sociales y otros responsables ejercitan, ha de plantearse que el olvido digital deba extenderse a otro tipo

de informaciones a efectos de que el interesado continúe dotado de poder de control sobre su información personal.

Concretamente nos referimos a que, además de garantizar una supresión de los datos de entrada, se deba, a su vez, proporcionar la posibilidad de solicitar la supresión de los perfiles elaborados por los proveedores de redes sociales o anunciantes por medio de los potentes algoritmos de IA, esto es, los datos de salida. El propio Grupo de Trabajo del Artículo 29 afirma que, el derecho de supresión se aplica tanto a los datos personales de entrada (los empleados para crear el perfil) como a los datos de salida (el propio perfil formado por datos inferidos)[924]. Véase que tal perfil se elabora a partir de datos personales del usuario, que, además, incluirá informaciones inferidas a raíz de los datos primitivos. Sin duda, consideramos que, se debe garantizar al usuario la posibilidad de solicitar la supresión de los perfiles elaborados además de conservar la posibilidad de oponerse a la elaboración de los mismos (art. 21 RGPD). De lo contrario, a pesar de que la información se considera formalmente eliminada, la misma no se ha suprimido totalmente si continúa empleándose para tomar decisiones que afectan al usuario o condicionar sus pautas de consumo.

Por consiguiente, cobran especial relevancia las palabras de HERRÁN ORTÍZ cuando afirma que la ambigüedad de la que adolece el art. 17 RGPD responde a evitar que el transcurso del tiempo y el imparable avance tecnológico terminen por afectar a la regulación instaurada por el legislador[925]. Sin perjuicio de que merezca una valoración positiva dicha falta de determinación, pues de este modo podrá acomodarse el precepto a nuevas y sofisticadas situaciones que la tecnología pueda generar para la salvaguarda de la información personal del interesado, ello potencia en mayor medida que los organismos dedicados a la protección de datos personales y Tribunales emitan orientaciones con el fin de no dejar ninguna situación susceptible de olvido sin amparo. Así, percibimos un inaceptable inmovilismo, tanto de los tribunales desde el pronunciamiento del TJUE 2014, como de organismos oficiales, en torno a la adaptación del ejercicio del derecho de supresión ante el nuevo paradigma de tratamientos de datos, como el caracterizado por el *big data* o la IA.

[924] Directrices del Grupo de Trabajo sobre protección de datos del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251, p. 19.
[925] HERRÁN ORTÍZ, A.I., "¿Nuevos tiempos, nuevos derechos?:A propósito del difícil olvido en Internet" en EMALDI CIRIÓN, A., y LA SPINA, E., (Editoras), *Retos del Derecho ante un mundo global, op. cit.*, p. 43.

Ahora bien, el obstáculo principal para garantizar estos mecanismos, reside en que, tal y como ha quedado demostrado en el capítulo anterior del presente trabajo, los proveedores de redes sociales no informan con claridad en sus políticas de privacidad de la práctica de este tipo de tratamientos de datos. De modo que, resulta complejo que el usuario, principal responsable de la salvaguarda de su información personal, pueda detectar la necesidad de suprimir informaciones que no conoce que proveedores de redes social y anunciantes someten a tratamiento (perfiles e información inferida).

Por todo lo expuesto, consideramos que el contexto que generan los tratamientos de datos actuales, unido a nuestros hábitos en Internet y redes sociales, imposibilita garantizar un olvido de la información personal. Pero ello no impide que deba garantizarse la supresión de datos que no revisten exactitud o que, con el tiempo, han devenido obsoletos, máxime si el titular de los mismos es menor de edad, en cuyo caso debe facilitarse la supresión en cualquier siempre, tal y como señala el art. 94.3 LOPDGDD. No obstante, se debe garantizar una supresión de la información que alcance todos los aspectos controvertidos que plantean los tratamientos de datos que los proveedores de redes sociales practican, incluidos aquellos basados en parámetros de IA; de lo contrario, el derecho de supresión no logra su cometido.

En definitiva, prohibir la elaboración de perfiles de menores, tal y como se ha planteado en capítulos precedentes, mitigaría el riesgo de no lograr una supresión de los datos personales a futuro, dado que se protegería *ex ante* al menor de un tratamiento de datos que, por lo general, desconoce debido a la manifiesta falta de información por parte del proveedor de la red social. De este modo, no se convierte al menor en principal responsable de proteger su información personal inferida, pues estos jóvenes, de seguro, desconocen la práctica de estos tratamientos además de las consecuencias para su información personal. A mayor abundamiento, la medida serviría, con carácter preventivo, tanto para evitar el direccionamiento de menores con fines de mercadotecnia directa, como para garantizar que no deberá a futuro preocuparse de solicitar la supresión de estos datos, pues el responsable de la red social no habrá procedido a su creación. En la actualidad, constituye una prioridad para las autoridades nacionales y las administraciones públicas, tanto visibilizar los riesgos que este nuevo paradigma de tratamiento de datos acarrea para el control de la información personal, como la adopción

de medidas propuestas que tienden a garantizar el interés superior del menor en señalado contexto.

Por último, alcanzada la mayoría de edad por parte del usuario, el proveedor deberá recabar el consentimiento para realizar perfiles del usuario previo a informar transparentemente de los detalles de este tratamiento a practicar (arts. 12 a 14 RGPD). Efectivamente, creemos que de este modo se otorga mayor respuesta a los riesgos que el Considerando 75 RGPD prevé para los derechos fundamentales de los niños-que entre otras cuestiones también señaladas en el precepto- genera la elaboración de perfiles.

CONCLUSIONES

I.- La normativa internacional, europea y nacional sobre la protección jurídica de la infancia se muestra obsoleta frente al imparable avance de la sociedad de la información. En consecuencia, se precisa una revisión y actualización urgente de la misma al contexto digital.

La normativa internacional, europea y nacional sobre la protección jurídica de la infancia sufre un marcado carácter tradicional que la ha conducido a una manifiesta obsolescencia frente al arrollador avance de las TIC. A decir verdad, la normativa que ha de proporcionar protección jurídica al menor no se ha esforzado por acomodarse a la nueva era de la sociedad de la información por la que se caracteriza el siglo XXI.

En efecto, la Convención de los derechos del niño de 1989, si bien se consideró un texto de relevancia incuestionable en el reconocimiento de los derechos del menor, tras más de 30 años de vigencia, la invariabilidad de sus disposiciones la han arrastrado a una falta de actualización en plena era digital. Sin intención de desmerecer su relevancia en el pasado, lejos queda el carácter innovador de la Convención en cuanto al reconocimiento de un nuevo *status* jurídico al menor. Por otra parte, en los años posteriores a la promulgación de la Convención de los derechos del niño, las instituciones europeas también trataron de impulsar la protección jurídica del menor en el ámbito, por aquel entonces, comunitario. Sin embargo, debemos extender a la Carta de los Derechos del niño, de 8 de julio de 1992, las consideraciones realizadas hace escasas líneas: la normativa europea de referencia sobre la protección jurídica del menor permanece, al igual que la internacional, impasible ante un vertiginoso cambio de paradigma cuyo inicio podemos situar hace más de una década.

En tal sentido, en los últimos diez años y con especial énfasis a partir del año 2009, las instituciones europeas e internacionales han procurado visibilizar los riesgos que las TIC traen consigo para los derechos de los más jóvenes; sin embargo, este propósito se ha canalizado por medio de textos que no se consideran jurídicamente vinculantes. Creemos que la normativa internacional y europea jurídicamente vinculante de referencia en la protección jurídica del menor, ha de someterse a un proceso de actualización que conduzca a la misma a responder a los nuevos retos que las TIC plantean para la privacidad y en especial, de la población más joven.

Concretamente, el transcurso de dos décadas del siglo XXI, debe conducir a la actualización del Convenio de derechos del niño de 1989 al acogimiento y a la incorporación de fórmulas adaptadas a la era digital. En efecto, el art. 16 del Convenio se muestra desactualizado cuando expresa que ningún niño sufra inferencias arbitrarias o ilegales en su vida privada. Así, el Convenio de derechos del niño debe, necesariamente, incluir en su articulado el derecho fundamental a la protección de datos personales del menor. A mayor abundamiento, los Estados deben trabajar en la aprobación de un Convenio internacional jurídicamente vinculante de derechos digitales del menor que refuerce la protección de los derechos fundamentales de la infancia ante el avance de la sociedad de la información. Desde luego, este texto debería regular unos estándares internacionales sobre la elaboración de perfiles de menores, el derecho al olvido digital, así como el tratamiento de datos de menores en redes sociales, entre otros. Convenimos que esta actualización de la normativa deviene crucial para guiar a los Estados en la armonización del régimen jurídico de protección del menor dado el carácter global de las TIC. De esta suerte, podría revestir interés la aprobación de un Convenio con una inspiración similar a la del Convenio número 108 que -a pesar de emanar de un órgano de ámbito europeo- prevea su ratificación por cualquier Estado.

Por otra parte, al contrario de lo que pudiera pensarse, el legislador nacional tampoco ha sabido dotar al menor de protección jurídica suficiente en la normativa destinada a tal efecto, a pesar de que los hábitos de estos jóvenes se desarrollen en Internet y redes sociales. Si bien es cierto que el legislador modificó la LOPJM de 1996 en el año 2015 con el fin de adaptar sus disposiciones a nuevos riesgos que amenazaban la protección jurídica del menor (entre los que destaca el manejo de las TIC), no debemos sino considerar el intento de infructuoso. A pesar de lo prometedora que pudiera resultar la exposición de motivos de la Ley 8/2015, de 22 de julio, de modificación de la ley de protección jurídica de la infancia y adolescencia, al advertir que tras veinte años desde la proclamación de la LOPJM, los cambios sociales incidían en la situación de los menores y demandaban una mejora de sus instrumentos de protección jurídica con el fin de cumplir eficazmente el artículo 39 CE, el texto normativo no persigue la protección jurídica del menor ante el cambio social más destacable del siglo XXI: la irrupción de las TIC. Efectivamente, no prevé una regulación sólida a la par de eficaz que proteja al menor frente a este nuevo escenario que puede vulnerar sus derechos fundamentales como, el

honor, intimidad personal y familiar y propia imagen, así como el derecho a la protección de datos personales.

Consideramos esta falta de previsión como un manifiesto descuido, pues el devenir de los años ha demostrado cómo las TIC pueden llegar a lesionar los derechos fundamentales relacionados con la privacidad del menor sin que la normativa de referencia refuerce la protección del menor en la referida esfera. De manera tradicional, la normativa sobre protección jurídica de la infancia, proporciona protección a los derechos fundamentales del menor que puedan verse afectados en un mundo analógico. Ahora bien, en el caso de la protección de la información personal, a pesar de que el legislador quizás pretendiera otorgar tal protección por medio de la normativa específica sobre protección de datos personales, cabía esperar que la regulación sobre la protección jurídica de la infancia dispusiera en su articulado una mención al señalado derecho para visibilizar el escenario digital y garantizar que el ordenamiento jurídico avanza en coherencia con la evolución de la sociedad hacia una esfera altamente digitalizada.

En definitiva, la falta de adaptación generalizada del ordenamiento jurídico destinado a proteger jurídicamente al menor en el nuevo escenario digital, pone de relieve un manifiesto desinterés por parte del legislador que, sin duda, coloca a los más jóvenes en una posición de indefensión jurídica constante cuando manejan las TIC para las actividades de su día a día. A pesar de lo dificultoso que se pueda considerar alcanzar unos estándares internacionales para la protección digital del menor, el interés superior del menor debe erigirse como guía para el logro de un consenso. A su vez, el legislador nacional debe conducir la normativa hacia una protección jurídica íntegra del menor internauta como persona necesitada de especial protección.

II.- El creciente impulso normativo en el ámbito internacional, europeo y nacional del derecho a la protección de datos personales, no ha tenido impacto en que el menor reciba especial atención en el mismo hasta épocas muy recientes a pesar de encontrarnos inmersos en plena era digital. En orden a revertir la inseguridad a la que se expone la información personal del menor a causa de este olvido jurídico, ahora se debe otorgar un carácter reforzado a la protección de la información personal del menor.

Ha quedado de manifiesto que los ordenamientos jurídicos internacional, europeo y nacional que abogan por la protección jurídica expresa del menor, no regulan la salvaguarda de la privacidad, y en concreto, de los datos personales de este de un modo

adaptado al contexto tecnológico actual. Cabía pensar entonces, que la protección de la información personal del menor se articularía por medio de la normativa sobre protección de datos personales ante el avance imparable de las TIC.

Sin embargo, muchos de los estándares internacionales sobre tratamientos de datos personales, presentan un sesgo excesivamente obsoleto y tradicional -al permanecer invariables desde los años 80- resultando insuficientes para proteger la información personal ante los tratamientos de datos que alumbra la nueva era digital. A mayor abundamiento, el ordenamiento jurídico internacional no acoge en su seno disposiciones específicas cuando la protección de los datos personales ha de garantizarse a menores de edad. En efecto, ni siquiera la modificación acaecida en el año 2018 del Convenio 108, como principal normativa internacional de referencia en la materia, contempla ninguna disposición para la salvaguarda de la información personal concerniente a menores de edad.

En el ámbito europeo, por su parte, aunque debemos reconocer iniciativa y empeño en positivizar en una norma la protección de los datos de menores de edad, estos no se han materializado hasta años muy recientes. Véase que hasta 2018 no entra en vigor normativa europea que regule aspectos tan relevantes sobre el tratamiento de datos de menores de edad como, por ejemplo, las condiciones de validez del consentimiento al tratamiento proporcionado por estos. Esta demora, se considera incoherente, pues los jóvenes llevan varias décadas, y con especial intensidad desde 2008- irrupción de las redes sociales- navegando sin garantías que velen por una especial protección de la información concerniente a su persona.

El impulso del Estado español en torno a la positivización de la protección de la información de los menores de edad, se ve influenciada por la regulación de este derecho por la UE. La tendencia a la armonización normativa se posiciona como la principal responsable de dicha afirmación. Sin embargo, en el caso español, cierto es que la evolución de la normativa del señalado derecho fundamental, se ha visto condicionada por el intenso debate a propósito del reconocimiento del derecho a la protección de datos personales como independiente y autónomo del derecho a intimidad a lo largo del pasado siglo. Realmente, el legislador español focalizó sus esfuerzos, aunque tardíamente, tanto en reconocer el nacimiento de un nuevo derecho fundamental, como en dotar al mismo de un contenido esencial que lo diferenciara del derecho a la intimidad. Por ello, cabe

entender que la protección jurídica específica del menor en este ámbito no se configurara de modo preferente en la agenda del legislador.

Ahora bien, las manifestaciones expuestas precisan de una matización; el Estado español aboga por la protección de la información personal del menor internauta en 2007 en el Reglamento de desarrollo de la LOPD, iniciativa que debe destacarse positivamente, pues en el mismo se regulan aspectos relativos a la validez del consentimiento y al principio de transparencia cuando el interesado es menor. Lamentablemente, no podemos sino expresar decepción al comprobar, que las normativas de la nueva década, encabezadas por el RGPD y la LOPDGDD no han variado en exceso a pesar del imparable avance de la sociedad de la información. Dicha invariabilidad constituye objeto de preocupación, en el sentido que, el contexto digital del año 2007 difiere considerablemente del actual, motivo por el que la invariabilidad de la normativa en lo relativo a los tratamientos de datos de la minoría de edad, ha terminado por cuestionar la eficacia de sus postulados y generar inseguridad jurídica sobre la información personal de un colectivo especialmente necesitado de protección.

En realidad, la ausencia de preceptos específicos que imponen un tratamiento de datos más respetuoso con la privacidad del menor de edad como principal usuario de Internet y redes sociales, ha derivado en una evolución de estos servicios de un modo que no respeta el interés superior del menor. Como cabía esperar, la ausencia de una normativa cuyo fin residiera en proteger la información personal del menor como sujeto especialmente vulnerable, ha predispuesto el desarrollo de tratamientos de datos verdaderamente intrusivos sobre la información de los más jóvenes.

Resulta sorprendente comprobar, que tanto la comunidad internacional como la UE toman plena conciencia en sus Resoluciones y Recomendaciones, del ritmo trepidante al que evolucionan las TIC; y a pesar de ello, los esfuerzos legislativos de las últimas décadas no han mostrado iniciativa para procurar acomodarse a dicho ritmo en orden a continuar garantizando la seguridad y la protección de los datos personales de los menores. Cierto es que, las TIC siempre avanzan y avanzarán a un ritmo mayor que la capacidad del ordenamiento jurídico de adaptarse; circunstancia que en las últimas décadas ha quedado suficientemente probada. Sin embargo, a nuestro juicio, dicha realidad no debe emplearse a modo de justificación, más bien, al contrario, como fuente de motivación a efectos de alcanzar normativamente y a la mayor celeridad posible una normativa que cohoneste con la era digital.

Con todo, en orden a revertir la inseguridad jurídica a la que se expone el tratamiento de datos de menores en estos espacios, urge aprobar un régimen reforzado frente al tratamiento de datos de interesados que no alcancen la mayoría de edad. Por ende, dado que se debe considerar al menor como una persona especialmente vulnerable por encontrarse en tránsito hacia la madurez, podría revestir interés incluir los datos del menor entre las categorías especiales de datos, ya que, de ese modo, la información personal de los más jóvenes gozará de un régimen reforzado de protección al amparo del art. 9 RGPD.

III.- La definición de redes sociales comúnmente aceptada, no refleja la verdadera actividad que estas ocultan: el tratamiento a gran escala de datos personales con fines de publicidad y mercadotecnia directa. Proponemos una reconceptualización de la definición de estas plataformas que prevea su principal rama de actividad.

El rápido desarrollo de Internet en escasos cuarenta años ha revolucionado de un modo sin precedentes los hábitos de las personas. Lejos quedó la consideración de Internet como un espacio estático en el que el usuario solamente podía servirse de un portal informativo abierto al mundo, pero en ningún caso se le permitía convertirse en partícipe ni colaborador del mismo. La irrupción de la Web 2.0 trajo consigo una completa transformación en el modo en el que las personas se relacionaban con esta herramienta virtual.

Sin lugar a dudas, uno de los espacios más exitosos de la Web 2.0 lo constituyen las redes sociales. Desde su creación en el año 1995, su popularidad no ha parado de crecer. En la actualidad, prácticamente personas de todas las edades acceden a estos espacios con un objetivo común: socializar y entretenerse. En efecto, las redes sociales nacen, en origen, con el fin de poner a disposición de los usuarios, con carácter gratuito, una plataforma en orden a que estos interactúen y se comuniquen en un entorno más cercano. En ese devenir, estos espacios incitan a los usuarios a compartir conversaciones, opiniones, fotografías, vídeos, etc. No obstante, el aparente carácter gratuito de estos servicios no debe conducir a equívocos. Los proveedores de redes sociales han conseguido rentabilizar sus plataformas por medio del tratamiento masivo de datos de las personas usuarias de sus servicios. Ciertamente, la información personal de los usuarios se utiliza como contraprestación no monetaria en orden a acceder a estas plataformas.

Precisamente, el volumen de datos personales que recaban estos servicios, se emplea con el fin de "personalizar la experiencia del usuario" y orientar a los anunciantes en la consecución de publicidad. Ello se debe a que estos espacios han hallado la tecnología capaz de desvelar e incluso eventualmente llegar a influir en los gustos, personalidad, ideología, pautas de consumo etc., de los usuarios a raíz de la información personal recopilada y observada de su actividad. Debemos dar a conocer, que la red social no recaba los datos personales sin la intención de extraer a los mismos un valioso rendimiento económico; más bien, al contrario, el rastro que generan los internautas constituye la verdadera fuente de riqueza de los proveedores de redes sociales. Efectivamente, por medio de la personalización de la experiencia, encubren su verdadera fuente de ingresos.

Así las cosas, visibilizar estos nuevos negocios, puede facilitar la toma de precauciones ante los riesgos que esta nueva rama de actividad genera para la privacidad de los usuarios, especialmente menores de edad. Sin restar protagonismo a los riesgos más clásicos, como la preocupación por la revelación de datos personales al compartir fotografías o la publicación de datos concernientes a terceras personas, el foco debe ponerse en proteger la información personal de los usuarios de aquellos peligros derivados de esta nueva rama de actividad, menos evidentes hasta la fecha, pero que a día de hoy generan los principales problemas para la privacidad de las personas y se espera que, a futuro, cobren mayor entidad.

Por todo lo expuesto, consideramos que la definición clásica de red social, que entiende la misma como un espacio que pone a disposición del usuario una plataforma con el fin de que este socialice, no visibiliza su principal actividad. Proponemos una nueva definición que refleje la nueva rama de actividad por la que estos proveedores explotan la información personal de los usuarios desde hace más de una década: la personalización de la experiencia del usuario y la publicidad y mercadotecnia directa. En definitiva, las redes sociales se definen como un espacio en el que, de manera personalizada para cada usuario, se pone a disposición de este una plataforma para que socialice e interactúe, mientras recibe anuncios y publicidad adaptada a sus gustos y preferencias.

IV.-La prestación del consentimiento *online* implementado en la actualidad por los proveedores de redes sociales no constituye una base legal válida que legitime el tratamiento de datos personales. Urge así exigir la configuración de un consentimiento informado y mecánicamente lícito cuando este se presta en línea.

Resulta pacífico afirmar que los proveedores de redes sociales merecen la consideración de responsables del tratamiento debido a la actividad que desempeñan. En efecto, la base de su servicio requiere del tratamiento de datos de los millones de usuarios que a diario emplean estas plataformas. Por tanto, los proveedores de estos servicios deben observar una suerte de deberes jurídicos que permitan al usuario ejercer un poder de control y disposición sobre sus datos personales. En esencia, el usuario debe conservar el poder de decidir sobre el destino de la información que concierne a su persona.

Entre las facultades de las que dispone el usuario en orden a controlar su información personal, destaca la prestación del consentimiento al tratamiento de datos personales como una de las bases legales que legitiman el tratamiento de datos personales al amparo del RGPD. Por medio del consentimiento, se reserva al usuario la facultad de decidir sobre la procedencia del tratamiento de su información personal al responsable, se entiende, previa recepción de la información que aclare los detalles del tratamiento que este desea practicar. De este modo, el responsable del tratamiento debe configurar la prestación del consentimiento bajo la observancia de una suerte de garantías impuestas por la normativa de protección de datos personales, cuya ausencia conducirá a la prestación de un consentimiento carente de validez.

Antes bien, la proliferación de servicios prestados en línea y el éxodo de los hábitos de las personas a un mundo altamente digitalizado, han cuestionado la eficacia y valor del consentimiento cuando el usuario se da de alta en estos servicios. Ciertamente, mientras que al amparo del art. 4.11 RGPD, el consentimiento del interesado debe configurarse como toda manifestación de la voluntad libre, específica, informada e inequívoca por la que acepta el tratamiento de sus datos personales, los proveedores de redes sociales han instaurado un sistema que no respeta ninguna de las obligaciones que impone el señalado precepto. En efecto, han optado por mecanismos carentes de transparencia que no informan a las personas usuarias del verdadero destino de sus datos personales, mecánicamente diseñados para limitar la libertad de estas a la hora de prestar el consentimiento, además de no revestir validez en orden a garantizar un consentimiento específico ni inequívoco.

Ha quedado en evidencia en la presente tesis doctoral, que queda mucho camino por recorrer por los proveedores de redes sociales, pues después de décadas, el oscurantismo y las malas prácticas se han asentado en su *modus operandi*. Sin embargo, a pesar de que el diseño de la prestación de un consentimiento garantista se enfrente a varias dificultades, deben abandonarse las excusas en la articulación de sistemas que cumplan con la normativa vigente. Solamente de ese modo podrá garantizarse que el usuario ejerce un verdadero control sobre sus datos personales, por lo que resulta indispensable adaptar los mecanismos *online* de prestación del consentimiento a las exigencias del art. 4.11 RGPD.

En primer lugar, para que el consentimiento se considere informado, se debe conseguir que los usuarios conozcan la presencia de las políticas de privacidad y procedan a su lectura. En ese sentido, se deben prohibir los hipervínculos carentes de visibilidad que despliegan la política de privacidad por, quizás, un despliegue automático del mismo en la pantalla del usuario. De esta manera, a los usuarios les resultará más dificultoso ignorar la existencia de estos textos, pues en la actualidad se puede consentir el tratamiento de datos personales sin reparar en su existencia. Por otra parte, conscientes de que -disuadidos por la extensión que las políticas de privacidad presentan- los usuarios no se detienen a leer estos textos, la redacción de las mismas debe abordarse por capas y de un modo que no auspicie interesadamente la desinformación.

En segundo lugar, para su configuración de modo transparente, ha de exigirse a los proveedores de redes sociales acogerse a fórmulas de redacción, que no deben resultar únicamente gramaticalmente sencillas como hasta ahora, sino que deberán arrojar claridad sobre las finalidades para las que tratarán la información de los usuarios de sus servicios. Así, deben abandonar la inclusión de términos ambiguos e imprecisos, así como los tecnicismos que contribuyan a restar trasparencia y claridad al texto a pesar de su aparente sencillez. En definitiva, se debe exigir a los proveedores de redes sociales que la redacción de las políticas de privacidad se configure de tal modo que asegure la comprensión por parte de los usuarios de las finalidades de tratamiento que el prestador del servicio se propone practicar.

En tercer lugar, puesto que el consentimiento debe configurarse de modo libre, específico e inequívoco, deben garantizar la prestación de un consentimiento diferenciado de las condiciones de uso del servicio, así como para cada una de las finalidades para las que prevén proceder al tratamiento de los datos de las personas interesadas. A ello

debemos añadir, que deberán indicar las bases legales aplicables a cada una de las finalidades del tratamiento previsto, ya que, de lo contrario, la elección incorrecta de las bases legales conduce a eludir la prestación del consentimiento de los usuarios para finalidades que, en realidad, solamente pueden llevarse a término si concurre el consentimiento del interesado. Sin olvidar que, a su vez, este comportamiento también predispone al usuario no conozca qué derechos ejercitar para defenderse de cada uno de los fines de tratamiento a los que se somete su información personal.

Por último, no se debe olvidar que el consentimiento debe poder retirarse en cualquier momento y con la misma facilidad con la que se ha concedido. Nada más lejos de esa realidad, el mecanismo para retirar el consentimiento es más complejo que el implementado para su concesión. Mientras que para su concesión no se precisan más que de unos segundos, su retirada se antoja dificultosa al forzar al usuario a acudir a los ajustes de la plataforma y seguir una suerte de pasos que entorpecen lograr su retirada. Así las cosas, los proveedores de redes sociales deben garantizar una retirada rápida del consentimiento.

Para el caso de usuarios menores de edad, los esfuerzos deberán incrementarse, pues a los cambios señalados recientemente, debe añadirse la adaptación de sus políticas de privacidad al público joven con el reto que ello supone. Cuando el art. 12.1 RGPD, cuya motivación reside en el Considerando 58 RGPD, impone a los responsables del tratamiento el empleo de un lenguaje que se adapte a los menores de edad en observancia de su interés superior, exige un auténtico esfuerzo a los responsables a la hora de informar a los más jóvenes sobre las verdaderas finalidades del tratamiento, así como las consecuencias para su información personal a causa del mismo. Sin embargo, advertimos una ostensible falta de adaptación de estos textos al público menor de edad pues el proveedor de la red social solamente prevé una política de privacidad para todos los usuarios; lo que conduce, en el caso de menores, a un consentimiento que no puede considerarse informado. Deben exigirse a los proveedores de redes sociales fórmulas que faciliten la comprensión de estos textos por parte de menores de edad, pues de lo contrario, la prestación del consentimiento por parte de estos puede resultar ilusorio.

En definitiva, se debe exigir a los proveedores de redes sociales, que entre sus prioridades se encuentre recabar un consentimiento válido cuando este se presta *online*. En ese sentido, creemos que las Agencias de protección de datos, en orden a cumplir el Considerando 123 RGPD, deben asumir un papel más activo en el control, tanto en lo

referente a la redacción de las políticas de privacidad, como en la configuración mecánica del consentimiento cuando este se presta en línea. Dado que se ha tenido la oportunidad de comprobar que la intervención de estos organismos no resulta la deseada en este ámbito, convenimos que la normativa debería imponer a las Agencias de protección de datos la revisión de estas exigencias cuando el consentimiento se presta *online*. De esta manera, la instauración de fórmulas de vigilancia y colaboración entre responsables del tratamiento y estos organismos puede contribuir a que los proveedores de redes sociales se comprometan a diseñar un consentimiento prestado en línea dotado de garantías.

V.-No se pueden continuar admitiendo las excusas en la implantación de mecanismos de verificación de la edad eficaces cuando el menor consiente el tratamiento de datos al darse de alta en redes sociales. Puesto que, desde el punto de vista técnico hace años que resulta posible verificar la edad del menor, el legislador debe precisar aquellos mecanismos que, a su juicio, resulten normativamente válidos para verificar la edad de este.

Tras varias décadas de silencio por parte de la normativa sobre protección de datos personales en torno al tratamiento de información personal concerniente a menores de edad, los arts. 8 RGPD y 7 LOPDGDD, regulan las condiciones de validez del consentimiento prestado por menores de edad. Efectivamente, la normativa sobre protección de datos personales, al fin acoge en su articulado preceptos cuyo objetivo reside en conceder una especial protección al menor frente a los tratamientos que se practican sobre su información personal.

Así, tanto la normativa europea como la nacional, fuerzan a los responsables del tratamiento, entre los que se encuentran los proveedores sociales, a asegurarse de la edad del usuario de sus servicios, compeliéndoles así a implantar un sistema que permita verificar la edad del usuario (arts. 8.2 RGPD y 7.2 LOPDGDD). Por otra parte, los mencionados preceptos, también obligan a los responsables a cerciorarse de que el consentimiento se concede por los representantes legales cuando el menor no puede autónomamente prestar el mismo al no alcanzar los 14 años de edad.

Antes bien, la proliferación de servicios prestados *online*, ha dificultado ostensiblemente la posibilidad de controlar de manera efectiva el momento en el que el menor consiente el tratamiento de sus datos personales, pues ello ocurre virtualmente. En efecto, mientras que en un formato analógico el trato directo con el menor puede levantar la sospecha sobre su edad con facilidad al responsable del tratamiento, así como disuadir

a los jóvenes de realizar actos para los que no tienen habilitación legal, las fórmulas *online* en la prestación del consentimiento han imposibilitado ejercitar un control en las condiciones expuestas.

Así las cosas, a pesar de la obligación impuesta por el legislador, gran parte de los proveedores de redes sociales continúan sin implementar un mecanismo que verifique, tanto la edad del futuro usuario, como la eventual prestación del consentimiento por sus representantes legales cuando este no alcanza la edad requerida. Efectivamente, durante dos décadas, la ausencia de un sistema que verifique eficazmente la edad del menor, ha fomentado que estos jóvenes no hayan sufrido impedimento alguno al momento de acceder y consentir el tratamiento de datos a estas plataformas, bastando con faltar a la verdad sobre su edad para lograr un acceso de modo exitoso. Esta circunstancia, que en la actualidad continúa sin solución, genera desconfianza sobre una de las facultades más elementales de control de la información personal que el interesado posee: la prestación del consentimiento sobre las finalidades de tratamiento.

Normativamente, debe denunciarse una falta de efectividad de la norma. En efecto, los preceptos señalados, constituyen una obligación carente de aplicabilidad en plena era digital. Aquellos consentimientos prestados por menores de 14 años sin la asistencia de sus representantes legales, carecen de validez, al contravenir tanto el RGPD como la LOPDGDD; por lo tanto, los proveedores de redes sociales practican tratamientos sobre información personal de menores que carecen de licitud. Tras más de una década desde la irrupción de estas plataformas, se debe prohibir a los proveedores de redes sociales continuar operando en las condiciones expuestas. Prácticamente desde la irrupción de estos servicios, se atisbaron los problemas que generaría el control de la edad de los usuarios, sin embargo, no se ha priorizado por repeler el comportamiento descrito.

El avance tecnológico más que evidente del que somos testigos, unido a las capacidades de tratamiento de datos personales desarrolladas por estos servicios, deja en evidencia, que desde el punto de vista técnico ya no resulta dificultoso verificar la edad de un usuario. Por ello, se debe abandonar por parte de las autoridades y el legislador la permisibilidad que ha imperado durante estos años ante la conducta señalada. Efectivamente, se debe comenzar a exigir el cumplimiento efectivo de los arts. 8.2 RGPD y 7.2 LOPDGDD.

El principal obstáculo en la búsqueda de un sistema de verificación jurídicamente idóneo, se identifica con el debate que suscita que varios de los mecanismos valorados terminen por exigir una mayor revelación de datos personales al fin de verificar la edad del menor. En efecto, la solicitud del DNI del menor o de los progenitores, la tarjeta de crédito o débito de estos, el envío de fotografías, etc., se han tildado de sistemas que exigen un desvelo todavía mayor de datos personales a efectos cerciorarse sobre la edad.

Sin perjuicio de que el principio de minimización debe constituir un factor de relevancia en la búsqueda del sistema idóneo, creemos que para el caso de las redes sociales no se deben menospreciar sistemas de verificación que requieran compartir más información personal a efectos de verificar la edad. Por una parte, porque entre los servicios que los proveedores de redes sociales ofrecen se encuentran la publicidad, venta directa y marketing, actividades sumamente peligrosas para la información personal del menor debido al empleo de algoritmos y elaboración de perfiles que en ellas se practica. Por otra parte, porque la consideración de usuarios de redes sociales como posibles responsables del tratamiento en determinadas circunstancias, conducen a estimar que, con mayor motivo, los menores -dada su falta de madurez- no puedan asumir las mismas cuando manejan estos espacios. Así, a nuestro juicio, los sistemas de verificación meramente declarativos empleados en la actualidad, deben superarse al no proteger suficientemente la privacidad de los más jóvenes e incluso en determinadas ocasiones la de terceros.

Así las cosas, consideramos que no se deben descartar sistemas biométricos que empleen IA como el novedoso sistema de triple verificación. Este sistema, basado en la combinación de tres algoritmos (biométricos, análisis de lenguaje y voz) logra determinar la edad del menor con un 95 a 99% de probabilidades de éxito. Antes bien, tomamos conciencia de que este último sistema presenta la ventaja de identificar aquellas personas menores de edad que ya manejan el servicio (al haber accedido sin controles previos).

Mientras tanto, la falta de exigencia en la implementación de un sistema de verificación en estos espacios, en especial, para el momento en el que el menor se da de alta y consiente el tratamiento de su información personal, favorece que los jóvenes continúen accediendo a estos servicios sin control previo, lo que, a nuestro juicio obliga a la adopción de un sistema, cuanto menos, provisional de verificación. De esta suerte, la inclusión de una serie de preguntas de desafío a responder por el potencial usuario en el momento de darse de alta, que solamente una persona adulta podría contestar con éxito,

puede considerarse un mecanismo de verificación provisional válido por el momento. Véase que, no requiere de más datos personales a efectos de verificar la edad. En tal sentido, unas respuestas poco concluyentes deben orientar al proveedor de la red social para detectar la presencia de un posible usuario menor de edad, al que deberá denegar el acceso al espacio hasta que se verifique su verdadera fecha de nacimiento.

Sea como fuere, los menores de edad deben encontrarse con un impedimento efectivo a la hora de acceder a estos espacios, pues de nada sirve prohibir legalmente el uso de estas plataformas en caso no alcanzar determinada edad, si ello no se acompaña de fórmulas que eficazmente comprueben la misma. Además, de la implementación de sistemas válidos de verificación, depende la eficacia de otras medidas tendentes a garantizar la protección de la información personal del menor que, aunque superada la edad de 14 años, continúa considerándose menor de edad hasta el cumplimiento de los 18 años, como, por ejemplo, configurar su perfil por defecto de modo privado.

Somos conscientes de que la solución propuesta se encuentra lejos de considerarse el mecanismo definitivo de verificación. Antes bien, creemos que cautelarmente puede servir para conseguir disminuir la participación de menores de edad- en especial de aquellos con edades manifiestamente inferiores a la legalmente establecida- en redes sociales. Entre tanto, la efectiva implementación de mecanismos de verificación de la edad debe convertirse en una prioridad, tanto para los responsables del tratamiento, pero en especial, para el legislador. Consideramos que el legislador debe mostrarse más específico e incluir en la norma una serie de sistemas de verificación normativamente válidos que los responsables del tratamiento deberán elegir para su implantación. En efecto, la generalidad del art. 8 RGPD, no ha conseguido que se implanten sistemas de verificación en estos servicios, por tanto, el legislador debe precisar qué sistemas de verificación revisten validez a su juicio. Por último, las autoridades de control deberían exigir a los proveedores de redes sociales demostrar que se han adoptado métodos para verificar la edad y de lo contrario, sancionar a aquellas plataformas que, al amparo del principio de responsabilidad proactiva no proceden a su implantación.

VI.- La anonimización de la información personal no reviste carácter irreversible cuando el tratamiento de datos se practica mediante técnicas que emplean *big data* e IA. Debe exigirse un desarrollo de estas técnicas respetuoso con los pilares fundamentales sobre los que se sustenta la normativa de protección de datos personales y en especial, en relación con los principios de transparencia y minimización.

El excelso volumen de datos disponibles en la red generado por nuestros hábitos en línea, ha animado a las compañías más pioneras a diseñar técnicas que tratan un elevadísimo volumen de datos en tan solo segundos. En efecto, los proveedores de redes sociales han desarrollado técnicas de tratamientos de datos que emplean componentes de *big data* e IA en orden a rentabilizar sus servicios, aparentemente gratuitos. Sin embargo, las nuevas técnicas de marketing y publicidad practicadas por los proveedores de redes sociales, se han implementado a costa de vulnerar la privacidad de las personas.

En ese sentido, nos sorprende que durante estos años los proveedores de redes sociales hayan desarrollado estos tratamientos de datos habida cuenta de las obligaciones que la normativa sobre protección de datos impone desde hace prácticamente tres décadas. La razón reside en que, al escudar su práctica en la previa anonimización de los datos personales empleados en las mismas, estos tratamientos se han desarrollado al margen del cumplimiento de la normativa sobre protección de datos personales. Sin embargo, pese a que aquella información que deje de poseer la capacidad de identificar a una persona con carácter irreversible, no recaerá en el ámbito objetivo de la ley de protección de datos personales, ha quedado demostrado en el presente trabajo de investigación que el *big data* y la IA artificial no garantizan el carácter irreversible que, en todo caso, ha de revestir el proceso de anonimización de la información personal.

Mas no se debe caer en el engaño, además de considerar la anonimización como presupuesto no válido a efectos de eludir la aplicación de la normativa sobre protección de datos personales ante estos tratamientos de información a gran escala, a nuestro juicio, ha llegado el momento de considerar que cualquier dato reviste carácter personal; ya que, la conexión de datos que estas técnicas de análisis masivos de datos realizan en tan solo segundos, albergan la capacidad de asociar todo tipo de informaciones (personales e incluso aquellas presuntamente anónimas) a una persona. En efecto, estimamos que la diferencia entre datos personales y aquellos que no revisten tal carácter instaurada por el RGPD, ha quedado superada cuando se refiere a estas técnicas de tratamiento.

Con mayor motivo entonces, los tratamientos de datos bajo parámetros de *big data* e IA, deberán cumplir rigurosamente con los principios de protección de datos personales. En su lugar, estas técnicas no se adecuan a los principios más elementales sobre los que ha descansado el tratamiento de datos personales desde el pasado siglo.

A decir verdad, el consentimiento prestado por el interesado, no constituye una garantía suficiente en orden a proporcionar un control eficaz sobre la información personal en el contexto señalado. Ciertamente, los proveedores de redes sociales no informan con claridad sobre la práctica de estas técnicas de tratamiento a pesar de encontrarse obligados normativamente. En el caso de algunas redes sociales, se deduce vagamente su práctica, pero un usuario medio no advertirá que ello ocurre. Además, el cumplimiento de la normativa señala que se debe informar al interesado de manera comprensible sobre la lógica subyacente de estos tratamientos de información; exigiendo un esfuerzo añadido que estos comprendan los aspectos fundamentales del tratamiento por medio de los algoritmos y elaboración de perfiles empleados y las consecuencias que ello acarrea para su información personal.

Antes bien, la complejidad técnica en el funcionamiento de los mismos, dificulta e incluso en ocasiones imposibilita que los usuarios comprendan la lógica subyacente de los mismos, máxime si el usuario no alcanza la mayoría de edad. Efectivamente, convenimos que el menor nunca podrá comprender la lógica subyacente de estos tratamientos de datos. Sin embargo, ello no debe impedir que los proveedores de redes sociales abracen fórmulas más transparentes a la hora de transmitir las vicisitudes sobre el tratamiento a los usuarios. Ya que, en todo caso, la dificultad en el logro de una explicación satisfactoria sobre la lógica subyacente del tratamiento por medio de algoritmos y elaboración de perfiles, no debe conducir a estos al mantenimiento de fórmulas que abogan por camuflar e incluso ocultar su práctica.

A nuestro juicio, ello motiva que en el ámbito de *big data* e IA, el principio de transparencia cobre un mayor protagonismo todavía, pues la complejidad de estos tratamientos debe conducir a una transparencia de carácter reforzado. No nos referimos así a que se deba abrumar al interesado con explicaciones técnicas sobre el funcionamiento de los algoritmos y elaboración de perfiles, sino que se debe conseguir que este conozca el verdadero cometido y finalidad del tratamiento practicado por medio de las técnicas señaladas. En relación con lo expuesto, entendemos que no es necesario para el interesado que se desvele el código fuente del algoritmo, pues véase que no lo

comprenderá. Entendemos que basta con informar de manera honesta a este sobre el verdadero destino de su información personal cuando se trata con los fines señalados. Así, dado que se trata de informaciones que deben incluirse en las políticas de privacidad, las Autoridades de protección de datos deben asumir un control efectivo que asegure la transparencia sobre las explicaciones proporcionadas a los interesados en este contexto.

Por otra parte, los proveedores de redes sociales ponen en práctica tratamientos sobre información personal de usuarios con fines para los que no se ha emitido un nuevo consentimiento válido por este. Efectivamente, bajo el pretexto de que estas técnicas no albergan la capacidad de identificar a las personas, los proveedores de redes sociales reutilizan datos recabados de otras fuentes, empleándolos para fines diferentes a los inicialmente previstos cuando el usuario emitió su consentimiento. La imprecisión en la redacción de las políticas de privacidad permite constantemente la puesta en práctica de tratamientos futuros no consentidos inicialmente bajo la excusa de personalizar la experiencia del usuario en la plataforma. Los proveedores de redes sociales deben expresar claramente las finalidades de tratamiento para las que pretenden recabar la información personal y solicitar un nuevo consentimiento en caso de incorporar nuevas finalidades de tratamiento sobre la información ya recopilada.

En otro orden de cosas, los proveedores de redes sociales han implementado mecanismos de recogida rigurosa de datos, llegando incluso a monitorizar por completo la actividad de los usuarios, lo que incluye el rastreo y control de los usuarios en sus plataformas y fuera de ellas. Antes bien, el principio de minimización impone la obligación de recabar el mínimo de datos personales posible para el cumplimiento del fin de tratamiento previsto. Contemplamos con preocupación que se permita la práctica de tratamientos que, de manera evidente, pueden colisionar con el principio de minimización al no superar la ponderación de derechos e intereses en juego que el principio de proporcionalidad exige. En efecto, el tratamiento masivo de datos personales con fines de personalización, publicidad y mercadotecnia directa en redes sociales no sirve al interés general, más bien, al contrario, se encuentra al servicio de intereses particulares de un número reducido de compañías privadas. Por ello, las técnicas de tratamientos de datos a gran escala pueden superar el juicio de proporcionalidad aplicadas a determinados fines de tratamiento, como, por ejemplo, aquellos que sirven a la detección temprana de enfermedades en el campo de la salud; sin embargo, los fines de publicidad y mercadotecnia directa, así como la “personalización de la experiencia” en redes sociales

no constituyen fundamento suficiente al fin de legitimar el alud de datos personales recabado.

Además, un gran volumen de datos personales tampoco garantiza un mayor acierto en las predicciones algorítmicas, ya que, ello dependerá de que los datos posean calidad suficiente. En realidad, el principio de calidad cobra especial relevancia en el contexto de estos tratamientos de datos, puesto que, datos carentes de calidad conducirán inevitablemente a inferencias erróneas. En consecuencia, el legislador y las autoridades de control deben exigir a los proveedores de redes sociales, al amparo del principio de proporcionalidad, que recopilen menos datos de sus usuarios, aunque ello dificulte el funcionamiento de sus algoritmos predictivos y la elaboración de perfiles, además de imponerles un grado de transparencia reforzado para los tratamientos que prevean los fines expuestos. De no atenerse a las consideraciones expuestas, debe impedirse que practiquen los tratamientos señalados para los fines de personalización y mercadotecnia directa.

En definitiva, el RGPD prevé valiosos principios que debidamente exigidos pueden garantizar tratamientos de datos masivos más respetuosos con la privacidad de las personas. En consecuencia, nuevamente demandamos, por una parte, más concreción en torno a estos principios por parte del legislador, adaptándolos a la IA e imponiendo normativamente fórmulas más exigentes de transparencia en este contexto, pues el devenir de los años ha demostrado cómo las disposiciones del mismo requieren de una constante actualización y reinterpretación; por otra parte, una intervención más proactiva por parte de las Autoridades de control de protección de datos personales en orden a exigir el cumplimiento de la normativa sobre protección de datos y en especial, de los principios de transparencia y de minimización en el caso de los tratamientos de datos que empleen componentes de *big data* e IA para los fines expuestos.

VII.-Se debe prohibir normativamente a los proveedores de redes sociales y restantes responsables del tratamiento, la elaboración de perfiles, así como la toma de decisiones individuales automatizadas concernientes a menores de edad con fines de publicidad y mercadotecnia al mostrarse incompatibles con su interés superior.

La capacidad tecnológica del *big data* y la IA en la búsqueda de referencias cruzadas a partir del tratamiento de grandes volúmenes de datos, aparentemente descontextualizados, ha permitido la búsqueda de patrones de comportamiento y perfiles

verdaderamente detallados sobre las personas. A través de los potentes algoritmos predictivos, se ha descubierto el modo de anticiparse a las decisiones de las personas desde el análisis exhaustivo de su información personal. El encuadre de las personas en un concreto perfil al que se le atribuyen determinados comportamientos futuros, ha propiciado, a su vez, la posibilidad de tomar decisiones automatizadas en las que el factor humano cada vez se encuentra más ausente.

Sin desmerecer los beneficios que esta técnica puede aparejar en diversos sectores, entre los que destaca la medicina personalizada, su aplicación en técnicas de publicidad y marketing, así como la personalización de los servicios en redes sociales ha de contemplarse con recelo, especialmente cuando el usuario es menor de edad. La práctica de estas técnicas sobre menores de edad, genera un entorno peligroso, tanto para el desarrollo personal, como para los derechos fundamentales de los más jóvenes que desde edades verdaderamente tempranas transcurren gran parte del día conectados segundo a segundo en estos espacios.

A mayor abundamiento, se ha constatado la potencial manipulación a la que se puede someter al menor debido a la posibilidad de anticiparse a sus decisiones por medio del análisis exhaustivo de sus datos, lo que conduce a la eventual posibilidad de influir con facilidad en las mismas, dada su situación de tránsito hacia la madurez. Por otra parte, el deseo de personalización de estos espacios, propicia el efecto burbuja, limitando el derecho de acceso a una información libre y veraz, constitucionalmente regulado. Todavía cabe señalar, que esta personalización aplicada a técnicas de marketing puede fomentar a su vez la discriminación y exclusión de determinadas personas de la oferta de determinados bienes y servicios basada en la predicción de un concreto algoritmo. En cierto sentido, la excesiva personalización, puede conducir no solo a una merma en la libertad de elección, sino también a que los menores no crezcan en un mundo que favorece la igualdad de oportunidades.

Nos preocupa, que mientras el proceso de maduración y aprendizaje se caracteriza por equivocarse, cambiar de opinión, evolucionar, etc., toda la información volcada por estos jóvenes continuará empleándose para engrosar el perfil sobre su persona incluso cuando alcancen la edad adulta. En efecto, los algoritmos continuarán empleando informaciones obsoletas para la inferencia de nuevas informaciones, lo que repercutirá negativamente en el desarrollo personal del menor. Así, se debe prohibir a los

proveedores de redes sociales el empleo de estos datos personales al amparo del principio de calidad, pues el tratamiento debe practicarse sobre datos actualizados y exactos.

Con todo, el excesivo control al que se somete la actividad *online* tanto de adultos, pero en especial de menores de edad, debe cesar. Las redes sociales no se configuran como un espacio inofensivo a efectos de favorecer la comunicación entre niños y niñas. El verdadero cometido oculto de su actividad, conduce a considerar que los menores no puedan crecer inmersos en un entorno que puede perjudicar tanto su desarrollo, como sus derechos fundamentales.

Sin embargo, los proveedores de redes sociales entorpecen considerablemente el ejercicio de aquellos mecanismos que proporcionan la salvaguarda de la información personal de los usuarios en el presente contexto. Ciertamente, imbrican los tratamientos con estos fines: por una parte, sobre la base legal de un interés legítimo; y por otra parte, como necesario para la ejecución de un contrato. De este modo, el consentimiento del usuario no resulta preceptivo. Nada más lejos de esa realidad, la importante intromisión que estos mecanismos de tratamiento representan para los usuarios de redes sociales, impiden que el interés legítimo del responsable prevalezca sobre el derecho a la protección de datos personales del interesado. Por tanto, a nuestro juicio, se debe interpretar restrictivamente el concepto del interés legítimo, no permitiendo la validez de dicha base legal para los fines de tratamiento señalados. De igual modo, la publicidad y mercadotecnia directa no se postulan como actividades indispensables para la puesta a disposición del usuario de una plataforma que fomente sus interacciones con otras personas.

Consecuentemente, a nuestro juicio, la finalidad alegada solamente puede justificarse sobre la base legal del consentimiento del usuario, lo que cohonesta a su vez con la inclusión de los datos del menor en la categoría de datos especiales del art. 9 RGPD. Ahora bien, nos remitimos así a las consideraciones anteriormente expresadas sobre el mismo cuando este se presta *online*. A lo que debemos añadir, que aquellos usuarios que no alcancen la mayoría de edad, en ningún caso podrán comprender la lógica subyacente que inspira dichos tratamientos. Por tanto, en consonancia con el Considerando 38 del RGPD, a fin de proteger el interés superior del menor, se debe prohibir normativamente a los proveedores de redes sociales la elaboración de perfiles y la toma de decisiones individuales automatizadas sobre datos concernientes a menores de edad para los fines que prevean una personalización de la experiencia, así como la publicidad y

mercadotecnia directa. Contemplamos con esperanza la prohibición de estas prácticas que el Reglamento europeo sobre la Ley de Mercados Digitales establece; sin embargo, apremiamos de nuevo a la implementación, con carácter urgente, de un mecanismo eficaz que verifique la edad de los usuarios, ya que, de lo contrario, no podrá garantizarse que los proveedores de redes sociales se abstengan de la práctica de los señalados tratamientos al desconocer la edad de los usuarios.

VIII.- La regulación del derecho al olvido digital en redes sociales no garantiza suficientemente el ejercicio de los derechos de las personas. En consecuencia, se debe dotar de contenido esta facultad específica prevista en la normativa sobre protección de datos de tal modo que asegure de forma efectiva un olvido en la era digital.

La masiva revelación de datos a causa de nuestras interacciones en la red, pronto auguró la necesidad de contrarrestar el rastro, inicialmente indefinido, que dichos datos generaban en la red. Así las cosas, el derecho al olvido digital se erige como la principal herramienta legal para combatir la perpetua disponibilidad de la información personal en la red. Ahora bien, la vertiginosa evolución de los servicios prestados digitalmente, también ha impactado en la consecución de dicho olvido digital. Concretamente, la aparición de las redes sociales, ha erosionado las bases sentadas hasta la fecha para el logro de un eficaz olvido de la información personal. A ello debemos añadir, que en el caso de usuarios menores de edad que son propensos a compartir datos personales, el olvido de su información personal se torna cada vez más complejo a medida que adquieren más presencia en estos espacios y desde edades más tempranas.

En la actualidad, pese a que el RGPD y la LOPDGDD procuran facilitar el ejercicio del derecho de supresión cuando el usuario no alcanza la mayoría de edad (art. 17 y Considerando 65 y arts. 93 y 94 respectivamente), casi una década después de la propuesta del texto normativo señalado, tres son las principales causas que nos fuerzan a contemplar con escepticismo la posibilidad de lograr una eficaz supresión de los datos personales en estos espacios, y nos obligan a reclamar que se dote de contenido a esta facultad que el ordenamiento jurídico prevé cuando se ejercita frente a proveedores de redes sociales en el marco del art. 94 LOPDGDD.

En primer lugar, se percibe una tendencia a identificar el derecho al olvido digital con el desindexado de datos en motores de búsqueda *online*. Ciertamente, el grueso de la doctrina científica, así como organismos y tribunales se han centrado en perfilar el ejercicio del derecho de supresión ante señalados prestadores de servicios digitales. Sin

embargo, la ambigüedad en la redacción del art. 17 RGPD, así como, el art. 94 LOPDGDD expresamente, con destacado acierto, contemplan la posibilidad de ejercitar dicha supresión de datos personales ante otros prestadores de servicios digitales, entre los que se encuentran los proveedores de redes sociales. En consecuencia, la naturaleza de los servicios prestados por estos conduce a considerar que la supresión de datos personales compartidos en redes sociales no puede articularse mediante el desindexado de los mismos. Ciertamente, las funcionalidades que ofrecen un buscador *online* y una plataforma social distan considerablemente. Sin embargo, tras varios años de aplicación del derecho de supresión, no se entiende que no se encuentre interpretación alguna sobre el modo en el que ha procederse a la supresión cuando se considera responsable del tratamiento a un proveedor de red social. Por ello, ayudaría a reforzar esta garantía que el ejercicio de este derecho frente a un proveedor de la red social, deba conllevar la efectiva eliminación de la información del perfil del usuario.

En segundo lugar, una de las características que definen estos servicios más empleados de la web 2.0, consiste en el papel activo que el usuario adopta en los mismos a causa de sus hábitos y comportamiento en estos espacios. Este rol dificulta considerablemente el logro de un eficaz olvido de los datos personales. Así las cosas, los usuarios de redes sociales pueden descargar imágenes, vídeos y, en definitiva, datos mediante la captura de pantalla de sus terminales tales como ordenadores, *tablets* o *smartphones*. El señalado comportamiento, contribuye no solo a la pérdida del rastro de la información personal, sino también a imposibilitar una eficaz supresión de tales informaciones, pues no se puede conocer cuántos usuarios han procedido a la descarga de las mismas y a compartir su contenido.

En consecuencia, la supresión alcanzará a la desaparición de los datos personales del perfil del usuario, pero no podrá suprimirse por completo, pues los usuarios pueden continuar difundiéndola tras su descarga o incluso volver a compartirla en la red social. Para estos casos no amparados por la excepción doméstica, se debe articular una garantía reforzada por la que se comunique a los usuarios que se ha solicitado la supresión de determinadas informaciones y así evitar su continua difusión. Por otra parte, dado que la solicitud de supresión no alcanza a la idéntica información susceptible de supresión que se ha compartido en perfiles de terceras personas, se debe imponer a los proveedores de redes sociales que eliminen información análoga objeto de supresión.

En vista de lo expuesto, consideramos que debería prohibirse que los usuarios menores de edad cuenten con la función de descargar datos personales a través de capturas de pantalla de sus terminales. Ante su manifiesta falta de madurez que los conduce a compartir informaciones variadas, se mitigaría el riesgo de que la información se difunda con facilidad (sobrepasando la excepción doméstica del art. 2 RGPD), lo que, a su vez, genera una mayor dificultad para conseguir un olvido digital de la información. En esencia, con la medida propuesta, se protege al menor de que la información no le persiga con carácter perpetuo.

Por otra parte, el art. 17.2 RGPD pretende extender el alcance de la supresión a terceros que traten la misma cuando el responsable realizare públicos los datos personales. Sin embargo, no disponemos de ninguna interpretación sobre lo que ha de entenderse por "realizar públicos datos personales" para que opere el mentado precepto. Así, los proveedores de redes sociales realizan públicos los datos de los perfiles configurados de tal manera, además de auspiciar considerablemente la posibilidad de que toda la información volcada en redes se considere susceptible de difusión (al permitir realizar capturas de pantalla). Por ello, a nuestro juicio, deberían notificar a terceros que tratan dichos datos, bien se consideren empresas colaboradoras con el responsable, como otros usuarios, la supresión de aquellas informaciones cuya eliminación se ha solicitado por el interesado. Antes bien, los miles de colaboradores que los proveedores de redes sociales acumulan, unido a la falta de identificación de los mismos en sus políticas de privacidad a pesar de su preceptividad, imposibilitan que dicha notificación con garantías, pues en muchas ocasiones todavía no conocen colaboradores con los que entablarán una relación comercial a futuro. Consecuentemente, el art. 17.2 del RGPD carece de la aplicabilidad deseada en el contexto señalado, provocando que el usuario desconozca el destino de la información que desea suprimir. En cambio, creemos que ello no excluye que deba exigirse normativamente que una alerta automática informe a los colaboradores identificados que se ha procedido a la supresión de determinadas informaciones a solicitud del interesado.

En tercer y último lugar, aun a riesgo de resultar reiterativos, probada ha quedado la vertiginosa evolución de las TIC y las consecuencias que ello genera para la protección de los datos de las personas. Desde la configuración del derecho fundamental a la protección de datos personales, la rápida metamorfosis de las mismas ha desembocado en la necesidad de reinterpretar el haz de facultades que garantizan la salvaguarda de la

información personal. El derecho de supresión no se encuentra al margen del impacto de dicha rápida evolución de las TIC. En efecto, los tratamientos de datos basados en parámetros de IA, han dificultado, todavía más, la posibilidad de suprimir con éxito los datos personales.

Así, consideramos que el ejercicio del derecho de supresión ante un proveedor de una red social, no supone únicamente retirar los datos personales de la visibilidad de terceros usuarios, sino que este debe abandonar cualquier tratamiento que sobre la información personal practique. Efectivamente, el proveedor de la red social, debe abstenerse de tratar dicha información para cualquiera de las finalidades previstas, entre las que destaca el tratamiento de dicha información con fines de publicidad y mercadotecnia directa. Por tanto, los proveedores de redes sociales deben garantizar que los potentes algoritmos que guían los procesos de toma de decisiones para la venta de productos y servicios y contribuyen a la elaboración de perfiles, eliminen tanto de su código fuente, como de los servidores del proveedor de la red social, los datos cuya supresión se ha solicitado. De lo contrario, el algoritmo, además de continuar infiriendo informaciones inexactas ante la obsolescencia o inexactitud de mentada información objeto de supresión, tratará información ilícitamente.

Por otra parte, visibilizados los riesgos que estas técnicas suponen para la privacidad, ha llegado el momento de exigir legalmente a los proveedores de redes sociales que reconozcan a los usuarios la posibilidad de solicitar la supresión de informaciones volcadas en un perfil o incluso el perfil elaborado al completo. Hasta la fecha, solamente se ha procedido a la supresión de informaciones concretas (datos de entrada en contexto de IA), pero se ha guardado silencio sobre la posibilidad de reclamar la eliminación de los datos resultantes de un perfil. Consideramos que esta función deviene crucial ante el nuevo paradigma de tratamiento de datos personales. Al igual que cabe la posibilidad de oponerse a dicha elaboración de perfiles *ex ante* (art. 21 RGPD), también debe concederse la posibilidad de suprimir aquellos ya elaborados *ex post*. Sin embargo, el reto resulta complejo, pues los proveedores de redes sociales no informan con claridad sobre la práctica consistente en elaborar perfiles a pesar de encontrarse normativamente obligados a ello, por lo que los interesados desconocen que deban defenderse ante la práctica de tales tratamientos de datos.

En definitiva, al igual que el derecho de cancelación terminó por evolucionar al derecho de supresión, las técnicas de tratamiento de datos personales basadas en *big data*

e IA, nos fuerzan a considerar necesaria la evolución en la interpretación del derecho de supresión.

A su vez, para la mejor protección de los más jóvenes, consideramos que prohibir la elaboración de perfiles basados en sus datos, tal y como se ha propuesto anteriormente, contribuye a aplacar las consecuencias que la conducta descrita genera en la consecución de un olvido de la información personal inferida. Efectivamente, de no elaborarse perfiles sobre información concerniente a menores de edad, estos no deberán preocuparse, cuanto menos, sobre la información deducida e inferida, ya que, el responsable no habrá procedido a su creación. Se deben adoptar fórmulas que garanticen que los menores, como sujetos en formación y cambiantes, puedan equivocarse, cambiar de opinión, de ideología o ideas con la garantía de que dicha información no los clasificará en un concreto perfil incluso cuando alcancen la edad adulta.

Queda en evidencia que el logro del olvido digital se antoja muy complejo. El propio diseño de estos espacios no permite que pueda suprimirse por completo la información personal. Esta cuestión debe interiorizarse por las generaciones más jóvenes, pues todavía no han advertido las consecuencias de compartir un alud de datos personales de manera constante en las plataformas sociales, a pesar de que el Considerando 65 y art. 17 RGPD pretendan facilitar la solicitud de la supresión de datos concernientes a menores de edad. Salvo que se protagonice un cambio de tendencia, el excelso volumen de datos personales que pueden compartir estos jóvenes durante su vida, unido a las nuevas técnicas de tratamiento de información en constante evolución, pueden terminar por imposibilitar por completo la supresión de sus datos personales. Véase que los menores no tomarán conciencia de la circunstancia descrita hasta una época más adulta, cuando realmente resulte imposible garantizar la eliminación de los prácticamente infinitos datos compartidos. Con todo, la garantía de un olvido digital parece desdibujarse para los internautas más jóvenes, ya que informaciones pasadas pueden acechar constantemente su presente y su futuro.

En definitiva, a pesar de la patente dificultad para alcanzar el olvido digital en el contexto actual, consideramos que no se debe caer en el abatimiento; los esfuerzos normativos deben canalizarse en mitigar el riesgo de que la información se torne perpetua en la red. Así, los nuevos riesgos que estos servicios generan, reclaman nuevas facultades reforzadas que necesariamente, conducen a una labor intensa por parte de los Tribunales europeos y nacionales. En el sentido expuesto, además de garantizar la supresión de la

información que ha devenido obsoleta o inexacta por el transcurso del tiempo, se precisa una revisión legal urgente del alcance del derecho de supresión que arroje luz sobre los datos susceptibles de supresión, así como los contextos en los que este debe operar ante las nuevas técnicas de tratamientos de datos personales. De lo contrario, el derecho de supresión queda notoriamente vacío de contenido, al no configurarse como una herramienta legal suficiente que salvaguarde los datos personales en un mundo altamente digitalizado.

IX.- Los conocidos como derechos ARCO POL que velan por la protección de la información personal del menor en redes sociales se presentan como herramientas jurídicamente ineficaces. Corresponde una revisión y actualización de los mismos adaptada al contexto digital en el que el menor se desenvuelve.

La nueva era digital, ha forzado a las instituciones a reinterpretar, no solamente el derecho de cancelación, ahora conocido como derecho de supresión, sino también los restantes derechos contemplados en la normativa sobre protección de datos personales, con el fin de que continúen garantizando la salvaguarda de los datos personales. La patente obsolescencia a la que se enfrentaban algunos de los derechos, ha traído consigo el nacimiento de nuevos derechos, como el derecho de portabilidad, o la evolución de algunos ya existentes como el derecho de oposición.

Ahora bien, clásicas y desfasadas quedan las críticas doctrinales que aducen que el derecho de acceso arrojará infinidad de resultados en el contexto *online*; véase que ya se articuló una respuesta a la mentada situación: el derecho de portabilidad. En pleno siglo XXI, otras son las cuestiones que deben generar inquietud. En un contexto que se caracteriza por la recopilación y tratamiento masivos de datos personales, tanto aquellos que el usuario comparte, como los extraídos de la observación de su comportamiento *online*, se presenta como una necesidad de primer orden determinar las categorías de datos a las que posee el interesado derecho a acceder. Nótese que el espíritu del derecho de acceso se halla en que el usuario pueda comprobar los datos sometidos a tratamiento, para así favorecer la labor de control sobre el tratamiento que sobre ellos se practica. Por tanto, a nuestro juicio, el derecho de acceso debe alcanzar tanto los datos activos, es decir, los facilitados por el usuario, como los datos pasivos, esto es, aquellos que se recopilan sin que este lo advierta. Solamente de este modo podrá realmente tomar conciencia del gran volumen de información sobre su persona sometida a tratamiento y obrar en consecuencia.

Más aún, en contra de lo que determinado sector de la doctrina considera, creemos que el derecho de acceso también debe revelar los datos inferidos a partir de los datos obtenidos del interesado, pues estas informaciones se consideran informaciones personales y lo identifican. Efectivamente, en un contexto en el que los tratamientos de datos sometidos a parámetros de IA cobran cada vez mayor protagonismo, el derecho de acceso solamente logrará su cometido de garantizar al usuario el conocimiento de dichos resultados algorítmicos, elaboración de perfiles, resultados de puntuación crediticia, etc. De lo contrario, se potencia el oscurantismo de estas prácticas, ya que, además de no informar correctamente al interesado sobre su práctica, tampoco se proporcionará la posibilidad de ejercitar una de las facultades que permiten el control sobre la información personal propia sometida a tratamiento.

Por otra parte, la falta de transparencia más que evidente de la que adolece el tratamiento de datos en el entorno *online*, dificulta ostensiblemente el ejercicio de determinados derechos. Sirva como ejemplo, que se espera que el derecho de rectificación adquiera especial importancia ante tratamientos de datos con tecnología de IA, puesto que los datos inexactos que circulan por la red generarán inferencias o cálculos erróneos. En consecuencia, el usuario podrá atacar dichas inferencias erróneas por medio de esta herramienta. No obstante, el interesado no ejercitará aquellos derechos que defienden su información personal sobre una práctica que desconoce. La falta de transparencia incide igualmente sobre el derecho de oposición, en el sentido que, los proveedores de redes sociales no informan cabalmente sobre la práctica consistente en la elaboración de perfiles (a pesar de encontrarse obligados a ello); en consecuencia, el usuario no se opondrá a un tratamiento que desconoce que se practica.

Por último, los derechos de nueva creación, no se encuentran libres de críticas cuando su ejercicio se practica frente a proveedores de redes sociales. Mientras que la UE aclamaba con éxito la incorporación del derecho de portabilidad a la normativa sobre protección de datos personales, consideramos que el mismo debe valorarse con prudencia. Así las cosas, el fin último del derecho de portabilidad se halla en transmitir los "datos personales facilitados" por el interesado al propio usuario, así como en transmitirlos directamente a otro responsable a elección del interesado, si ello deviene posible técnicamente. Sin embargo, el principal debate se sitúa en concretar los datos susceptibles de portabilidad, pues el tenor literal del RGPD opta por una fórmula ambigua que no

clarifica qué debe comprenderse por "facilitar". En ese sentido, subrayamos que los tribunales europeos y nacionales no se han pronunciado al respecto hasta la fecha.

A nuestro juicio, la interpretación que se ajusta en mayor medida a la pretensión de garantizar al usuario un control sobre sus datos personales contempla dos posibilidades según se solicite la portabilidad de los datos para el propio usuario o una transmisión directa de responsable a responsable. En el primero de los casos, se deberán portar al usuario tanto los datos activos como pasivos que el responsable del tratamiento posea. De este modo, el usuario accederá al conjunto completo de la información personal que el interesado somete a tratamiento y decidir, en consecuencia, qué realizará con la misma. El segundo caso, en cambio, debe valorarse con especial cautela. Puesto que el usuario no conocerá qué información personal se transmitirá directamente entre responsables, nos inclinamos por la transmisión únicamente de los datos activos, pues de esta manera se protege la transmisión de informaciones que rastrean y monitorean su comportamiento sin que el usuario advierta dicha circunstancia. Por último, los datos calculados o inferidos no deberán resultar objeto de portabilidad, por lo menos entre responsables, ya que ello fomenta la pérdida de control de los datos personales que evalúan aspectos verdaderamente delicados del interesado.

En definitiva, en un entorno digital en el que la información fluye a gran escala y con manifiesta celeridad, el derecho de portabilidad puede terminar por auspiciar la pérdida de control sobre la información personal. En ese sentido, el legislador y los tribunales deben aclarar a la mayor brevedad posible, el alcance del derecho de portabilidad ante estos hábitos *online*, que llevan años sucediendo, que facilite la transmisión de datos entre diversos responsables, pero que, a su vez, asegure la protección de los datos personales de los interesados. No obstante, advertimos que el derecho de portabilidad, sin una verdadera cultura de transparencia por parte de los responsables del tratamiento, propiciará, en todo caso, la pérdida de control de la información personal.

Sin embargo, aunque los derechos señalados resultaran susceptibles de actualización y reinterpretación, el ejercicio de los mismos por personas menores de edad se enfrenta a un principal obstáculo: la falta de un método que fiscalice que quien ejerce los derechos de acceso, rectificación, supresión, oposición y portabilidad alcanza la edad establecida en la normativa para actuar autónomamente (14 años de edad).

Esta realidad, conduce a asimilar, no solamente que determinados menores puedan ejercitar los mentados derechos sin alcanzar la edad establecida, sino que, estos, ante su falta de madurez y ausencia de conciencia sobre la protección de su información personal, no ejerciten el haz de facultades que el ordenamiento jurídico pone a su disposición para su salvaguarda. A su vez, los responsables legales del menor, en caso de que el menor no alcance 14 años de edad, desconocedores en muchas ocasiones de los hábitos *online* de este, pueden no ejercitar los derechos en defensa del señalado derecho fundamental del que sus descendientes son titulares. En definitiva, la realidad recientemente expuesta, genera una situación de inseguridad e indefensión para los más jóvenes, puesto que las probabilidades de que las principales herramientas en orden a proteger sus datos personales no se accionen resultan verdaderamente elevadas.

X.- El legislador e instituciones de la Unión Europea y Estados miembro, deben reaccionar y exigir un efectivo cambio de cultura en el tratamiento de datos que los proveedores de redes sociales desarrollan y practican. Entendemos que es necesaria una intensa labor de formación a expertos en programación algorítmica sobre el impacto jurídico de los tratamientos de datos que diseñan, así como una intervención más reactiva de las autoridades de control cuando estos no se plieguen al principio de responsabilidad proactiva.

A lo largo de la presente investigación, se ha podido constatar que la más que notoria falta de transparencia se posiciona como el denominador común de una gran parte de los comportamientos contrarios a la normativa sobre protección de datos personales que los proveedores de redes sociales practican. Efectivamente, el deseo de ocultación impera entre los proveedores sociales, pues la ambigüedad e imprecisión en las explicaciones sobre las finalidades de tratamiento, unido al oscurantismo y silencio sobre la práctica de algunas de estas, desembocan en una realidad insoslayable: el usuario no ejerce un control efectivo sobre su información personal.

Durante décadas, la permisibilidad del legislador y de los organismos cuyo objetivo reside en ejercer un control sobre el derecho a la protección de datos personales, han propiciado que, paulatinamente, estos proveedores de redes sociales hayan desarrollado un tratamiento de datos cada vez más intrusivo con la información personal de millones de personas usuarias de sus servicios, incluidas aquellas que no alcanzan la mayoría de edad. Es más, advertimos que los esfuerzos de la industria se concentran, principalmente, en sortear los límites que la normativa sobre protección de datos

personales se propone instaurar. En efecto, la industria se empeña en continuar practicando estos tratamientos de datos al margen de la normativa sobre protección de datos personales. El desarrollo e implementación de técnicas de tratamiento como la elaboración de perfiles, la minería de datos o las decisiones individuales automatizadas constituyen un buen ejemplo de ello, ya que, si entre las prioridades de los responsables del tratamiento se encontrara el respeto a los principios sobre protección de datos personales, no hubieran procedido al desarrollo de las técnicas de tratamiento señaladas.

Queda en evidencia así, que los proveedores de redes sociales no han abrazado los nuevos principios que el RGPD instaura y que implican el necesario cambio de cultura en el tratamiento de datos que este propugna: la sustitución de un modelo reactivo de protección de datos personales, por otro en el que los propios responsables deben- desde un verdadero compromiso- guiar el tratamiento de datos al cumplimiento de la normativa sobre protección de datos personales. Así las cosas, el RGPD, con carácter preventivo sostiene que, al amparo del principio de responsabilidad proactiva, el propio responsable del tratamiento deberá demostrar que cumple con las obligaciones que la normativa sobre protección de datos impone. En cambio, la actitud de los proveedores de redes sociales desafía el modelo de protección de datos vigente desde 2018.

El tratamiento de datos que estos proveedores de redes sociales practican, solamente se podrá considerar más garantista con la información personal, cuando comprendan que la transparencia, la explicabilidad y, en definitiva, las obligaciones que la normativa impone a los responsables del tratamiento deben constituir una parte esencial del diseño de su servicio. No convenimos con las voces que afirman que el RGPD no puede aportar una respuesta garantista ante estas nuevas técnicas de tratamientos de a gran escala; véase que el propio Proyecto de Reglamento sobre IA remite al RGPD en lo referente al respeto a la normativa sobre protección de datos. Más bien, al contrario, el RGPD se encuentra provisto de principios verdaderamente valiosos, que debidamente actualizados y reinterpretados, pueden conducir a estos sistemas a respetar la información personal incluso en el actual paradigma digital. Ahora bien, el potencial problema reside en que, a pesar de la falta de voluntad en el cumplimiento de la normativa por los proveedores de redes sociales, tanto el legislador, como las autoridades de control no han exigido su cumplimiento.

Quizás, desde las instituciones y organismos, tanto de la UE, como nacionales, se deba fomentar con mayor intensidad el cambio cultura en el tratamiento de datos a estas

grandes empresas, obligándolas a reflexionar sobre la relevancia de cumplir de modo efectivo la normativa sobre protección de datos personales europea. Sobre este particular, puede resultar de utilidad, por una parte, formar a los expertos que programan los algoritmos en diseños éticos y respetuosos con la protección jurídica de la privacidad; por otra parte, hacer partícipes a estos expertos en IA de grandes empresas en los procesos legislativos, así como en elaboración de directrices. Ya que se puede aprobar nueva normativa más restrictiva, pero de nada servirá si esta no se acompaña de un cumplimiento efectivo de la misma. En efecto, cualquier modelo de protección de datos instaurado hasta la fecha, no ha logrado encauzar el tratamiento de datos que estas compañías practican. Antes bien, unido a los esfuerzos en el fomento de una nueva cultura de tratamiento, a nuestro juicio, las instituciones europeas y autoridades nacionales de control deberán intervenir con mayor contundencia los tratamientos con los fines expuestos cuando los proveedores de estos servicios se muestren incapaces de plegarse al principio de responsabilidad proactiva.

Como se puede apreciar, este cambio en la cultura del tratamiento de datos que proponemos, se encuentra provisto de un gran componente ético que se alinea con los últimos trabajos de la UE, en especial, relacionados con la IA. En efecto, su pretensión se identifica con que los propios responsables del tratamiento se comprometan de modo efectivo y -sin necesidad de volver a un modelo reactivo- a asumir las obligaciones de responsable y, además, se abstengan de diseñar nuevos tratamientos que no superen tal estándar ético a futuro. Así, ponemos en duda que manipular a menores e incluso a adultos con fines de personalización y mercadotecnia directa en redes sociales atienda a estándares éticos. En consecuencia, se debe imponer normativamente la prohibición de estos tratamientos a las compañías.

Sin embargo, para garantizar de manera efectiva la salvaguarda de la información personal de los interesados, se debe comenzar por generar un contexto en el que prime la transparencia. Solo si se informa adecuadamente a los usuarios podrán ejercitar aquellos derechos que tienden a defender su información personal. No obstante, la instauración de canales a través de los cuales fluya en mayor medida la información no deben establecerse solamente entre responsable e interesado. En ese sentido, y en especial con los nuevos tratamientos de datos masivos, se debe conceder la posibilidad de auditar y controlar todos los algoritmos que guían estos tratamientos.

Con estas técnicas el acceso a los datos personales es masivo, pero los resultados del tratamiento se encuentran no en pocas ocasiones, al amparo del secreto legal e industrial. Comprendemos así, que los proveedores de redes sociales no desvelen los detalles de los algoritmos a los usuarios de la red social, además, ello tampoco contribuiría a una mejor información a los usuarios ante la complejidad técnica. No obstante, creemos que las autoridades de control, así como los órganos judiciales, deben contar con la posibilidad de controlar y auditar estos algoritmos por ley. De lo contrario, se podría producir la indefensión de los titulares de los datos con los que estos funcionan, pues la falta de conocimientos técnicos sobre el funcionamiento de estas herramientas no permitiría a estos ejercer un control eficaz sobre su información personal. En ese sentido, deben incluirse expertos en algoritmos en las autoridades de control correspondientes para que puedan comprobar la adecuación de los mismos a la normativa vigente. Parece que dicha necesidad tiende a materializarse en los Estados, pues el propio Gobierno español prevé la creación de la Agencia Española de Supervisión de la Inteligencia Artificial. Sin embargo, para el logro de su cometido, se deberá forzar a los proveedores de redes sociales, a efectos de rendición de cuentas, a compartir la información relativa a estos algoritmos con las autoridades garantizando la confidencialidad de los mismos en todo momento.

Sobre este particular, debemos lamentar que el Proyecto de Reglamento sobre IA aprobado por la UE, solamente prevea medidas de transparencia y auditabilidad reforzadas para los sistemas de IA que reciban la calificación de alto riesgo, ya que, ello fomenta que los sistemas no considerados de alto riesgo se desarrollen sin transparencia. Antes bien, valoramos positivamente que, finalmente, en el texto definitivo del Proyecto remitido al Parlamento Europeo, se haya valorado incluir los sistemas de recomendación empleados por las plataformas de medios sociales en el Anexo sobre sistemas de alto riesgo en orden a reforzar la explicabilidad de estos sistemas, pues su versión inicial no contemplaba dicha posibilidad. Sin perjuicio de lo expuesto, las autoridades de control deberán asegurarse de que las explicaciones resultan adecuadas y suficientes y que cumplen con el RGPD puesto que el nuevo Proyecto de Reglamento sobre IA no conseguirá su cometido sin un cumplimiento riguroso de la normativa sobre protección de datos personales.

En definitiva, no olvidemos que el desarrollo tecnológico debe servir a la humanidad desde el respeto a los derechos fundamentales para que este no termine por

volcarse en contra de esta. Tal y como se ha puesto en práctica desde el inicio de la sociedad moderna con los avances que se sucedían en la misma, ha de valorarse que determinadas decisiones no deben inspirarse desde el deseo exclusivo de potenciar un avance (tecnológico en este caso), sino desde el respeto a los derechos fundamentales de las personas. En concreto, el cumplimiento de la normativa implicada, así como la garantía de los derechos fundamentales más elementales, han de constituir una prioridad en el diseño e implementación de los tratamientos de datos personales, tanto en los que ya se practican actualmente, como en los venideros.

Por último, esta nueva cultura de tratamiento también debe servir para concienciar a los proveedores de redes sociales de que compatibilicen sus espacios con la protección de los usuarios menores de edad. En efecto, la protección de la privacidad se ha de configurar como una prioridad para estos proveedores de redes sociales que acumulan millones de seguidores que no alcanzan la mayoría de edad y de cuya especial salvaguarda no se preocupan. Así, la salvaguarda del menor como sujeto especialmente necesitado de protección tiene que arribar al ámbito *online* de mayor presencia en su día a día: las redes sociales. De lo contrario, convenimos que se debería condicionar la actividad de estos proveedores de servicios al cumplimiento de la normativa implicada con el fin de garantizar el interés superior del menor.

XI.- La protección jurídica del menor como usuario de redes sociales constituye una asignatura pendiente en plena era de la sociedad de la información. Entendemos así la necesidad de reclamar un marco jurídico específico que vele por la información personal del menor, que comience por alfabetizar digitalmente a los más jóvenes para garantizar la autoprotección de su privacidad.

El deseo de proteger integralmente al menor en todas las facetas que puedan poner en riesgo su desarrollo personal, ha irrumpido en nuestro ordenamiento jurídico con especial intensidad desde finales del pasado siglo. Así, el fin último del ordenamiento jurídico reside en proteger a estos jóvenes que dada su falta de madurez no siempre pueden ejercitar las herramientas que les permiten defenderse autónomamente. Sin embargo, a pesar del reto que supone proteger la información personal de los usuarios de redes sociales en plena era de la sociedad de la información, se evidencia una absoluta falta de preocupación por parte del legislador e instituciones en su garantía.

Así las cosas, la principal pregunta que motiva la presente tesis doctoral, esto es, la valoración de la suficiencia en la protección jurídica de la información del menor como

usuario de redes sociales ha de responderse, desafortunadamente, en sentido negativo. El devenir de la investigación ha demostrado cómo, a causa de diferentes factores, el derecho a la protección de datos personales- no solo de menores de edad- se vulnera reiteradamente por los proveedores de redes sociales en todo el ciclo del tratamiento (desde que el usuario se da de alta y consiente el tratamiento hasta que desea la supresión de la información). En consecuencia, la actual normativa sobre protección jurídica de la infancia y aquella tendente a garantizar la salvaguarda de la información personal no constituyen garantía suficiente para una eficaz protección de la privacidad.

El inmovilismo de la normativa específica de protección jurídica de la infancia frente a la era digital, imposibilita proteger al menor ante los nuevos escenarios que las redes sociales plantean para la protección de su privacidad. Aunque cierto es que el tratamiento de datos ha alcanzado tal complejidad técnica que esta normativa no se erige como el cauce idóneo para ello. La normativa sobre protección de datos personales, por su parte, si bien debía asumir la responsabilidad de proteger manera específica la información personal del menor como sujeto vulnerable en el entorno digital, la falta de cumplimiento por parte de los proveedores de redes sociales de las reglas elementales relativas al tratamiento de datos de menores han relegado a los más jóvenes a una posición de indefensión frente a estos proveedores de servicios.

Así, los poderes públicos no deben continuar permitiendo la resignación de la población ante la evidente intromisión en su privacidad ocasionada por el transcurso de décadas sin procurar revertir comportamientos manifiestamente contrarios a la protección de la información personal de los usuarios de estos servicios.

De este modo, constituye una prioridad acabar con el completo desconocimiento que impera entre los interesados sobre el destino de su información personal cuando consienten el tratamiento de sus datos personales a proveedores de redes sociales. Dado que nuestro modelo de protección de la información personal se asienta sobre el control que el titular debe ejercer sobre sus datos, se ha de sensibilizar a la población sobre los riesgos a los que se enfrenta su privacidad cuando emplea redes sociales. Solo de este modo pueden advertir la necesidad de proteger sus datos personales a través de las valiosas herramientas que la normativa pone a su disposición. No obstante, en relación al menor, revertir la situación demanda la construcción de un marco jurídico específico que vele por la protección de su información.

En ese cometido, se debe comenzar por garantizar normativamente una alfabetización digital de los jóvenes en lo referente a la gestión de la identidad y derechos fundamentales. En efecto, los Estados deben integrar por ley esta materia en la educación escolar, llevando la misma al aula a través de los planes de estudio que deberán desplegarse desde el nivel preescolar hasta todos los cursos académicos. Parece que esta necesidad comienza a advertirse por parte del legislador. En ese sentido, el Parlamento vasco, que trabaja actualmente en el proyecto de ley vasca de protección de datos personales y Autoridad Vasca de Protección de Datos, de 23 de diciembre de 2022, visibiliza en su art. 20 la formación de la ciudadanía en datos personales. Antes bien, lamentamos que solamente prevea la formalización de acuerdos para dicho cometido en el ámbito universitario. Véase que el desarrollo de esa conciencia debe iniciarse desde edades tempranas, formando sobre los verdaderos fines de tratamiento de las redes sociales, para que esta contribuya a generar mayor inquietud en lo referente a la protección de la información personal. Asimismo, deberá formarse al profesorado con el fin de que transmitan dichos conocimientos, valores y derechos a sus estudiantes.

Por otra parte, sin olvidar que en ocasiones los menores no pueden encauzar la defensa de sus derechos autónomamente, las campañas informativas también deben llegar a los representantes legales de estos. En efecto, los progenitores o tutores, deben conocer que las redes sociales no se configuran como un espacio que fomenta la interacción de sus descendientes exclusivamente. Solamente de este modo podrán asistir a sus descendientes (art. 154 CC y art. 84 LOPDGDD) en la protección de su información personal a conciencia.

Sorprendentemente, en pleno siglo de revolución digital en el que la información se encuentra al alcance de las personas más que nunca, el desconocimiento ha terminado por convertirse en el mayor enemigo para la protección de la privacidad. Los poderes públicos no pueden continuar inmóviles ante un problema que ha aflorado hace años, pero al que no se pone remedio. Cabe esperar así, que el Gobierno cumpla con el compromiso normativo que se desprende del art. 97.2 LOPDGDD y por el cual se compromete, en el plazo de un año desde la entrada en vigor de la norma en 2018, a desarrollar un Plan de Actuación cuyo objetivo principal radica en la protección del menor en relación al uso responsable y equilibrado de Internet y redes sociales a través de la formación, concienciación y difusión de información necesarias.

En concreto, este Plan deberá contemplar la práctica de campañas que informen a los usuarios de redes sociales-especialmente menores- del verdadero destino de sus datos personales cuando emplean estos servicios. En este quehacer, la normativa debe obligar a formalizar acuerdos institucionales para que se impartan charlas, casos prácticos, etc., por expertos en la materia que aseguren que el menor recibe una formación y desarrolla una conciencia sobre el empleo diligente para con la privacidad de servicios digitales. Ciertamente, en ese deseo de formar a los usuarios más jóvenes de redes sociales, se deberá poner el foco especialmente en que los niños y niñas comprendan los efectos negativos y perversos de las estrategias de manipulación y persuasión, el procesamiento de datos por medio de algoritmos y elaboración de perfiles, la toma de decisiones individuales automatizadas, así como el excesivo control ejercido por estas plataformas.

En otro orden de cosas, como ha quedado sentado, la responsabilidad en la salvaguarda de la información personal, no debe recaer exclusivamente sobre los interesados. Ciertamente, se debe mantener correctamente actualizada la normativa sobre protección de datos personales ante el arrollador avance de las TIC. Una normativa desactualizada, puede conducir a las personas a no poder defender con garantías su información personal. Resulta necesario así, que las autoridades de control competentes de protección de datos, el legislador y los Tribunales reinterpreten constantemente las herramientas que la normativa de protección de datos prevé para la salvaguarda de la información personal de los interesados. Advertidos los problemas que generó la rigidez de la Directiva 95/96/CE ante este tipo de tratamientos, debe aprovecharse la generalidad del RGPD en varios de sus preceptos, pues unido al art. 97.5 RGPD, se abre una puerta a la constante actualización del texto frente al avance tecnológico con el fin de evitar el mismo destino de aquella; antes bien, la eficacia de este precepto debe aparejar necesariamente una intensa labor interpretativa que mantenga al día el mismo.

Por otra parte, el compromiso en el cumplimiento de la normativa señalada, debe alcanzar de igual modo a la evolución de estos espacios hacia un entorno en el que el interés superior del menor se encuentre garantizado; de lo contrario, el menor se muestra indefenso ante un medio altamente presente en su día a día. Por consiguiente, en relación a la protección jurídica del menor, el marco normativo de protección de datos acusa un marcado carácter insuficiente que demanda especificidad en orden a salvaguardar la protección jurídica del menor de edad. Así pues, urge que el legislador apruebe el señalado marco jurídico específico que vele por la protección del menor en el entorno

digital. Al igual que determinados tratamientos de datos han demandado especificidad en algunos ámbitos como el tratamiento de datos en el ámbito de la salud, consideramos que la protección de la información personal del menor, demanda idéntica particularidad en su regulación, especialmente cuando es usuario de redes sociales.

La construcción de este marco jurídico específico, se debe convertir en una prioridad para el legislador a través de la implementación medidas eficaces que salvaguarden la información personal de menores como sujetos especialmente vulnerables cuando utilizan redes sociales. Véase que el RGPD prevé garantías para el comienzo de la relación entre el responsable e interesado (transparencia y condiciones de validez del consentimiento), así como para el final de la relación (derecho de supresión); pero en lo concerniente a menores de edad, no prevé ninguna garantía específica que proteja la información personal de estos durante la prestación de los servicios. Ciertamente, estos espacios no pueden configurarse indistintamente para aquellos usuarios mayores y menores de edad, puesto que la capacidad de los más jóvenes con el fin de proteger sus datos personales no resulta análoga a la que una persona adulta puede demostrar. Ello genera un espacio potencialmente peligroso tanto para la privacidad, como para el desarrollo del menor. En efecto, determinados tratamientos, como es el caso del tratamiento de datos a través de IA con fines de publicidad y mercadotecnia, no deben practicarse sobre la información de menores en ningún caso al fin de proteger su interés superior.

En ese sentido, consideramos que, al igual que EEUU se propone formalizar un acuerdo con las grandes tecnológicas desarrolladoras de IA para buscar un compromiso de la industria para la evaluación pública de sistemas de IA generativa, la UE debería fomentar un acuerdo con los principales proveedores de redes sociales con el fin de buscar su compromiso para con el cumplimiento de las normas y directrices para el desarrollo responsable y compatible de sus servicios con los menores. Este acuerdo puede ser un mecanismo efectivo para adaptar la prestación del servicio a particularidades como: incluir los datos de menores de edad entre las categorías especiales de datos en orden a reforzar su protección; configurar el perfil de menores de edad, por defecto, de modo privado en orden a evitar su consideración como responsable del tratamiento; impedir la captura de pantalla de imágenes y vídeo con el fin de evitar que estos menores practiquen tratamientos como un responsable; asegurar el ejercicio efectivo de los derechos que prevé la normativa sobre protección de datos personales, bien por el propio menor cuando

sea capaz o sus representantes legales; o en definitiva, impedir la elaboración de perfiles sobre información personal de menores de edad con fines de mercadotecnia directa.

Con todo, aunque los últimos años hayan demostrado que la era digital se presenta a modo de reto para el legislador dada la rapidez con la que estos servicios evolucionan, el ordenamiento jurídico debe proteger y amparar los derechos de las personas a la mayor celeridad posible. En este contexto, no se debe olvidar que los más jóvenes interactúan con estas herramientas digitales desde que adquieren uso de razón, pero dicho manejo no viene acompañado de un sistema de protección integral cuando se desenvuelven en la red. Por ello, apremiamos a la construcción de este marco jurídico que vele por la protección de la información personal del menor en Internet y en especial, en las redes sociales.

BIBLIOGRAFÍA

I. REFERENCIAS BIBLIOGRÁFICAS

ABA CATOIRA, A., "Los menores ante Internet", *Congreso Internacional de Derecho y Nuevas tecnologías,* Bilbao, Universidad de Deusto, 2009.

ABRIL, P., y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana. Una visión comparativa del derecho al olvido", *Indret,* 2014, núm. 1, pp. 1-62.

ADSUARA, B., "Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento)", en RALLO LOMBARTE, A., (Director), *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales,* Valencia, Tirant lo Blanch, 2019, pp. 313-352.

AGUSTINOY GUILAYN, A., Y MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales,* Barcelona, Boch editor, 2021.

ALÁEZ CORRAL, B., *Temas clave de la Constitución Española. Minoría de edad y Derechos Fundamentales,* Madrid, Tecnos, 2003.

- "El ejercicio autónomo de los derechos fundamentales por el menor de edad", *Revista Europea de Derechos Fundamentales,* 2013, núm. 21/1er semestre, pp. 37-68.

ÁLVAREZ CARO, M., "Reflexiones sobre la Sentencia del TJUE en el asunto Mario Costeja (C131/12) sobre el derecho al olvido", *Revista Española de Derecho Europeo,* 2014, núm. 51, pp. 165-187.

- *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital,* Madrid, Reus, 2015.

- "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en RECIO GAYO, M., Y PIÑAR MAÑAS, J.L., (Directores) *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad,* Madrid, Reus, 2016, pp. 227-240.

ÁLVAREZ RIGAUDIAS, D., "El poder del usuario digital", en ARTEMI RALLO, L., y GARCÍA MAHAMUT, R., (Editores), *Hacia un nuevo derecho europeo de protección de datos,* Valencia, Tirant lo Blanch, 2015, pp. 275-310.

- "Tratamiento de Datos de Salud", en PIÑAR MAÑAS, J.L., (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad,* Madrid, Reus, 2016, pp. 171-186.

ANGULO GARZANO, A., "El derecho al olvido en los motores de búsqueda y en las redes sociales a la luz de la nueva normativa de protección de datos", *Actualidad Administrativa La Ley,* 2019, núm. 4, sin paginación.

APARICIO SALOM, J., Y SANFULGENCIO TOMÉ, S., "El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos", *Revista Aranzadi Doctrinal,* 2014, núm. 11, pp. 1-17.

ARENAS RAMIRO, M., "La encrucijada constitucional de la Unión Europea", *Revista Jurídica de Castilla y León,* 2008, núm. 16, pp. 113-168.

- "El consentimiento en las redes sociales on line", en RALLO LOMBARTE A., Y MARTÍNEZ MARTÍNEZ, R., (Coordinadores), *Derecho y Redes sociales*, Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, pp.117-144.

- "Hacia un futuro derecho al olvido de ámbito europeo", en VALERO TORRIJOS, J., *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica,* Cizur Menor, Aranzadi, 2013, pp. 325- 380.

- "El derecho de oposición (comentario al artículo 21 RGPD y al artículo 18 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 1701-1724.

ARIAS POU, M., "Transparencia e información que deberá facilitarse cuando los datos personas se obtengan del interesado. El derecho a la información desde el diseño (comentario al artículo 13 RGPD y al artículo 11.1 y 2 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 1357-1379.

ARMADA VILLAVERDE, M.E., Y LÓPEZ BUSTABAD, I.J., "El Reglamento General de Protección de Datos ante el fenómeno del "Big Data", *Revista Aranzadi de Derechos y Nuevas Tecnologías,* 2019, núm. 51, pp. 1-26.

AVIÑÓ BELENGUER, D., "El uso de cookies de publicidad comportamental desde la óptica de la protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2020, núm. 56, pp. 1-35.

AZURMENDI, A., "Derechos digitales de los menores y datos masivos. Reglamento europeo de protección de datos de 2016 y la Coppa de Estados Unidos", *El Profesional de la información,* 2018, vol. 27, núm. 1, pp. 27-35.

BARAHONA CAZURRO, V., *Derecho digital. Perspectiva interdisciplinar*, Barcelona, Boch Editorial, 2017.

BARNA, A., "Convención Internacional de los Derechos del Niño. Hacia un abordaje desacralizador", *Revista de Temas Sociales,* 2012, núm. 29, pp.1-19.

BARRIUSO RUIZ, C., "Las Redes sociales y la protección de datos hoy", *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, pp. 301-338.

BATUECAS CALETRÍO, A., "El control de los padres sobre el uso que sus hijos hacen de las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, pp. 137-170.

BELLOSO MARTÍN, N., "La concreción del interés (superior) del menor", *Anuario Facultad de Derecho- Universidad de Alcalá X,* 2017, núm.10, pp. 1-42.

BELLOTO GÓMEZ, J.M., "Explicabilidad e inteligencia artificial responsable. Recomendaciones "aterrizadas" al día a día de las empresas", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial,* Valencia, Tirant lo Blanch, 2022, p. 199- 224.

BENEDITO CAÑIZARES, M.T., "La autorregulación en el Reglamento General de Protección de Datos como solución frente al mercado digital fragmentado: el menor y los Registros", *Revista Crítica de Derecho Inmobiliario,* 2018, núm. 770, pp. 3119-3172.

- "Estadio intermedio de reflexión para una futura regulación de la ética en el espacio digital europeo: los principios de transparencia y acountability", *Revista de Derecho y Nuevas Tecnologías,* 2021, núm. 55, pp. 1-56.

BENTHAM, J., *The Panopticon Writings,* Editor Miran Bozovic, Londres, 1995.

BERCOVITZ RODRÍGUEZ-CANO, R., en su obra "Menores", *Revista Doctrinal Aranzadi Civil-Mercantil (digital),* Vol. I.

BERROCAL LANZAROT, A.I., *Derecho de supresión de datos o derecho al olvido,* Madrid, Reus, 2017.

BYUNG-CHUL, H., *La sociedad de la transparencia,* Barcelona, Herder, 2013.

CABALLERO TRENADO, L., "*Cookies* y consentimiento", *Revista Crítica de Derecho Inmobiliario,* 2020, núm.781, pp. 3227-3239.

CADENAS OSUNA, D., "El consentimiento informado y el rechazo a la intervención o tratamiento médico por el menor de edad tras la reforma de 2015: estudio comparado con el *common law*", *ADC*, 2018, Tomo LXXI fasc. III, pp. 789-852.

CARRASCO PERERA, A., *Derecho Civil (Introducción. Derecho de la persona. Derecho subjetivo. Derecho de propiedad),* Madrid, Tecnos, 1996.

CASABONA ROMEO, C.M., "Datos personales (Comentario al artículo 4.1 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 573-589.

- "Elaboración de perfiles (comentario al artículo 4.4 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 609-612.

CASAS ROMA, J., NIN GUERRERO, J., y JULBE LÓPEZ, F., *Big data: análisis de datos en entornos masivos,* Barcelona, UOC, 2019.

CASTÁN TOBEÑAS, J., *Derecho civil español, común y foral*, Tomo 1, Vol. II, Madrid, Reus, 1987.

CASTÁN VÁZQUEZ, J.M., "Cometario al Título VII del Código Civil", en ALBADALEJO, M., (Director), *Comentarios al Código civil y compilaciones forales,* Madrid, EDERSA, 1978.

CASTELLANOS CLARAMUNT, J., "La gestión de la información en el paradigma algorítmico", *Métodos de información*, 2020, núm. 21, pp. 59-82.

CASTILLA BAREA, M., "La protección de los menores el internet (Comentario al artículo 84 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 3945-3978.

COLÁS ESCANDÓN, A. Mª, "La defensa del interés del menor en el conflicto entre en derecho a la intimidad de los menores de edad y los derechos y obligaciones derivados de la patria potestad de sus progenitores", *Revista Doctrinal Aranzadi Civil-Mercantil,* 2017, núm. 9, pp. 1-45.

CONDE ORTIZ, C., *La protección de datos personales,* Madrid, Dykinson, 2006.

CORRAL TALCIANI, H., "El derecho al olvido en internet: antecedentes y bases para su configuración jurídica", *Revista jurídica digital UANDES,* 2017, núm. 1, pp. 43-66.

CORTINA ORTS, A., "Ética de la Inteligencia Artificial", *Anales de la Real Academia de Ciencias Morales y Políticas,* 2019, núm. 96, pp. 379-394.

COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata,* 2017, núm. 24, pp.131-150.

- "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho", *Revista General de Derecho Administrativo,* 2019, núm. 50, pp. 1-37.

- "Transparencia y explicabilidad de la inteligencia artificial y compañía (comunicación, interpretabilidad, iteligibilidad, auditabilidad, testabilidad, comprobabilidad y simulabilidad…). Para qué, para quién y cuánta", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial,* Valencia, Tirant lo Blanch, 2022, p. 25-70.

- "Expresión, información, creación y acceso a la cultura. Libertades y responsabilidades de usuarios y plataformas en entornos digitales (XIV, XV, XXIV)", en COTINO HUESO, L., (Coordinador) *La Carta de Derechos Digitales,* Valencia, Tirant lo Blanch, 2022, pp. 197-224.

CRAIG, T., y LUDLOFF, M., *Privacy and Big Data*, Sebastopol (California), O´Really, 2011.

CRISTEA UIVARU, L., *La protección de datos de carácter sensible: historia clínica digital y Big Data en salud,* Barcelona, Boch Editor, 2018.

DAVARA FERNÁNDEZ DE MARCOS, L., "Régimen jurídico de las redes sociales", en CAZURRO BARAHONA, V., (Coordinador), *Derecho digital, Perspectiva interdisciplinar*, Barcelona, Boch editor, 2017.

- "Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go", *XX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos*, Madrid, 2007.

- "Los menores en el Reglamento General de Protección de Datos: cuestiones de Interés (comentario al artículo 8 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021. pp. 957-989.

DE CASTRO, F., *Derecho civil,* Madrid, Instituto de Estudios Políticos, 1952.

DE FRUTOS TORRES, B., Y MARCOS SANTOS, M., "Disociación entre las experiencias negativas y la percepción de riesgo de las redes sociales en adolescentes", *El profesional de la información,* enero-febrero 2017, vol. 26, núm. 1, pp. 88-96.

DE LA SIERRA, S., "Una introducción a la Carta de Derechos Digitales", en COTINO HUESO, L., (Coordinador) *La Carta de Derechos Digitales,* Valencia, Tirant lo Blanch, 2022, pp. 27-52.

DE MIGUEL ASENSIO, P.A., *Estudios y Comentarios Legislativos (Civitas). Derecho Privado de Internet*, Cizur Menor, Editorial Aranzadi, 2015.

DE URBANO CASTRILLO, E., "Derechos de la personalidad e Internet", *Revista Aranzadi Doctrinal,* 2010, núm. 9, pp. 1-11.

DEL CASTILLO VÁZQUEZ, I.C., "Requisitos del consentimiento utilizado como fundamento jurídico para el tratamiento de los datos de carácter personal (comentario al artículo 7 RGPD y al artículo 6 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, pp. 945-956.

- "Consentimiento (Comentario al art. 4.11 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, pp. 679-692.

DÍAZ, J., "Redes sociales: Incumplimiento sistemático de los controles técnicos versus vulneración reiterada de los derechos del menor", *Diario la Ley,* diciembre 2018, núm. 9326, pp. 1-10.

DÍAZ DÍAZ, E., "El derecho de supresión. El derecho al olvido (comentario al artículo 17 RGPD y artículo 15 LOPDGDD", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 1561-1604.

- "Derecho al olvido en línea (Comentario a los artículos 93 y 94 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 4285-4292.

DIEZ PICAZO, L., y GULLÓN, A., *Sistema de Derecho civil,* Volumen IV, Tomo I, Madrid, Tecnos, 2012.

DOMÍNGUEZ REYES, J.F., "Interés superior del menor en la jurisprudencia del Tribunal Supremo", *Revista Crítica de Derecho Inmobiliario,* 2018, núm. 768, pp. 2212-2233.

DOPAZO FRAGUÍO, P., "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento General de Protección de Datos)", *Revista Española de Derecho Europeo,* 2018, núm. 68, pp. 1-37.

DUNCAN J. WATTS., *Six Degrees: the science of a connected Age*. Nueva York, W.W. Norton & Company, 2004.

DURÁN SEGURA, M., Y MEJÍAS PELIGRO, J.F., "Conocimientos y comportamientos de los usuarios de la red social Facebook relacionados con la privacidad", *Ámbitos: revista internacional de comunicación,* 2014, núm. 26, pp. 231-240.

EGUSQUIZA BALMASEDA, Mª.A., *Protección de Datos: Intimidad y Salud,* Cizur Menor, Aranzadi, 2009.

ESCRIBANO TORTAJADA, P., "Algunas cuestiones sobre la problemática jurídica del Derecho a la intimidad, al honor y a la propia imagen en Internet y en las redes sociales", en FAYOS GARDO, A., y CONDE COLMENERO, P., (Coordinadores), *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Madrid, Dikynson, 2015, pp. 61-85.

ESPARZA LEIBAR, I., "La Inteligencia Artificial y el derecho fundamental a la protección de datos personales", en BARONA VILAR, S., (Editora), *Justicia algorítmica y neuroderecho: una mirada multidisciplinar,* Valencia, Tirant lo Blanch, 2021, pp. 265-285.

FERNÁNDEZ-ALLER, C., y SERRANO PÉREZ, MªM., "¿Es posible una Inteligencia Artificial respetuosa con la protección de datos?", *Cuadernos de Filosofía del Derecho,* 2022, núm. 45, pp. 307-336.

FERNÁNDEZ CORONADO, A., Y PÉREZ ÁLVAREZ, S., "La libre formación de la conciencia del menor a través de internet", *Menores e Internet,* Cizur menor, Aranzadi, 2013, pp. 1-24.

FERNÁNDEZ PÉREZ, A., "La protección de los derechos fundamentales de los menores en internet desde la perspectiva europea". *Revista Ius et Praxis,* 2016, núm. 1, pp. 377-416.

FERNÁNDEZ-SAMANIEGO Y FERNÁNDEZ-LONGORIA, "El derecho a la portabilidad", en PIÑAR MAÑAS, J.L., ÁLVAREZ CARO, M., y RECIO GAYO, M., *Reglamento general de protección de datos: hacia un nuevo modelo de privacidad,* Madrid, Reus, 2016, pp. 257-274.

FLAQUER RIUTORT, J., "Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies: especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (e-privacy)", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2018, núm. 47, pp. 1-33.

- "La función publicitaria de las cookies: mecanismos de prevención y cautela en el Derecho español", *THEMIS-Revista de Derecho,* enero-junio 2021, núm. 79, pp. 127-140.

FLEISHER, P., "¿Qué legislación en materia de privacidad debería aplicarse en Internet a nivel mundial?", en PIÑAR MAÑAS, J.L., (Director), *Redes sociales y privacidad del menor* Madrid, Reus, 2011, pp. 311-317.

FRANZ, W., "The Right to Inform v. the Right to be Forgotten: a Transatlantic Clash", *Georgetown University. Center for Transnational Legal Studies Colloquium,* 2009, núm. 2, pp. 285-300.

FROSINI, V., "La protezione della riservatezza nella societá informatica" *Informatica e Diritto,* 1981, VIII, pp. 5-14.

- "Bancos de datos y tutela de la persona", *Revista de Estudios Políticos,* noviembre-diciembre 1982, núm. 30, pp. 21-40.

- *Cibernética, derecho y sociedad,* Madrid, Tecnos, 1982.

GÁLLEGO HIGUERAS, G.F., "Tratamiento de datos en el ámbito publicitario (Comentario al art. 23 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, p. 3701-3732.

GARCÍA DE ENTERRÍA, E., (Director) y ALONSO GARCÍA, R., *La encrucijada constitucional de la Unión Europea,* Madrid, Civitas, 2002.

GARCÍA-ATANCE GARCÍA DE MORA, M.V., "Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación (TIC)", *Revista de Derecho político UNED,* septiembre-diciembre 2017, núm.100, p. 1271-1308.

GARCÍA GARNICA, M.C., "Datos personales y menores de edad", en GONZÁLEZ PACANOWSKA, I., (Coordinadora), *Protección de datos personales,* Valencia, Tirant lo Blanch, 2020, pp. 161-238.

GARCÍA MARTÍN, I., "Aspectos psicológicos de la influencia de Internet en el libre desarrollo de la personalidad del menor", *Menores e Internet,* Cizur menor, Aranzadi, 2013.

GARCÍA MEXÍA, P., "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos" en PIÑAR MAÑAS, J.L., (Director). *Reglamento General de Protección de Datos, hacia un modelo europeo de privacidad,* Madrid, Reus, 2016, pp. 23-34.

GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales en la Era del Big Data y de la Computación ubicua,* Madrid, Dykinson, 2016.

- "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de protección de Datos de la Unión Europea", *Derechos y libertades,* 2018, núm. 38, Época II, pp. 107-139.

- "Decisiones automatizadas basadas en algoritmos y protección de datos personales", en TOMÁS MALLEN, B., GARCÍA MAHAMUT, R., y PAUNER CHULVI, C., (Editores), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español,* Valencia, Tirant lo Blanch, 2022, pp. 333-359.

GARROTE FERNÁNDEZ, I., "La regulación del derecho al olvido en los arts. 17 y 21 del RGPD y en el art. 93 de la LOPDGDD", en GONZÁLEZ PACANOWSKA, I., (Coordinadora), *Protección de datos personales,* Valencia, Tirant lo Blanch, 2020, pp. 373-437.

GETE-ALONSO Y CALERA, Mª.C., "Los derechos del menor y personas discapacitadas en el entorno digital", en MARTÍNEZ VÁZQUEZ DE CASTRO, L., (Director) y ESCRIBANO TORTAJADA, P., (Coordinadora), *Internet y los derechos de la personalidad*, *Internet y los derechos de la personalidad*, Valencia, Tirant lo Blanch, 2019, pp. 277-308.

GIL ANTON, A., *El derecho a la propia imagen del menor en Internet.* Madrid, Dykinson, 2013.

- "La privacidad del menor en Internet", *Revista de Derecho, Empresa y Sociedad,* 2013, núm. 3, pp. 60-96.

- "Redes sociales y privacidad del menor: un debate abierto", *Revista Aranzadi de Derecho y Nuevas Tecnologías parte Cuestiones,* 2014, núm. 36, pp. 1-28.

GIL GONZÁLEZ, E., "Big Data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley,* septiembre 2017, núm. 9050, pp. 1-13.

GIL MEMBRADO, C., "El consentimiento en las redes sociales", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, pp. 105-135.

- "Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales", *La Ley Derecho de Familia,* 2017, núm. 13, pp. 1-24.

- "Autonomía y tratamiento de datos personales de salud en tiempo de pandemia", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma,* Madrid, Dykinson, 2021, pp. 141-178.

- "Una nueva era: hacia el robot sanitario autónomo y su encaje en el derecho", en GIL MEMBRADO, C., (Directora y Coordinadora) *Bioderecho y retos: M-Health, genética, IA, robótica y criogenización,* Madrid, Dykinson, 2022, pp. 357-399.

GIRÓN REGUERA, E., "La protección de datos de los menores de edad en internet", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 4271-4283.

GOMES CANOTILHO VITAL MOREIRA, J.J., "Constituçao da República Portuguesa". *Lei do Tribunal Constitucional*, 1993, 3ª ediçao revista.

GÓMEZ-JUÁREZ SIDERA, I., "Reflexiones sobre el derecho a la protección de datos de los menores de edad y la necesidad de su regulación específica en la Legislación Española", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2006, núm. 11, 2ª parte, p. 1-19.

GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales", en GONZÁLEZ PACANOWSKA, I. (Coordinadora) *Protección de datos personales,* Valencia, Tirant lo Blanch, pp. 668-731.

GRIMALT SELVERA, P., "Los menores e internet: capacidad versus protección de la vida privada" en CUENCA CASAS, M., ANGUITA VILLANUEVA, J. A., ORTEGA DOMÉNECH, J., (Coordinadores), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa,* Madrid, Dykinson, 2013, pp. 179-194.

GUARDIOLA SALMERÓN, M., "Menores y redes sociales: nuevos desafíos jurídicos", *Revista de Derecho, Empresa y Sociedad,* enero-julio 2016, núm. 8, pp. 53-67.

GUICHOT, E., "El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español", *Revista de Administración Pública,* 2019, núm. 209, pp. 45-92.

HART, H.L., "¿Hay Derechos naturales?", *Derecho y Moral. contribución a su análisis*, Buenos Aires, Depalma, 1962, pp. 74-75.

HEREDERO CAMPO, Mª T., "Evolución tecnológica y derecho al olvido digital, desde sus inicios a la actualidad", en APARICIO VAQUERO, J.P., y BATUECAS CALETRÍO, A., *En torno a la privacidad y la protección de datos en la sociedad de la información,* Granada, Comares, 2015, pp. 69-103.

HERNÁNDEZ, A., Y KÜSTER, I., "Brand impact on purchasing intention. An approach in virtual social networks channels", *Economics and bussines letters,* núm. 1(2), p. 1-9.

HERRÁN ORTÍZ, A.I., *La violación de la intimidad en la protección de datos personales,* Madrid, Dykinson, 1999.

- *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales,* Madrid, Dykinson, 2002.

- "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos,* 2003, núm. 26. pp. 1-93.

- "Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?", *Revista R.V.A.P.* 2010, núm. 87-88, pp. 521-566.

- "Aproximación al derecho a la protección de datos personales en Europa. El Reglamento General de Protección de Datos personales a debate", *Revista de Derecho, Empresa y Sociedad,* 2016, núm.8, pp. 179-200.

- "¿Nuevos tiempos, nuevos derechos?:A propósito del difícil olvido en Internet", en EMALDI CIRIÓN, A., y LA SPINA, E., (Editoras), *Retos del Derecho ante un mundo global*, Valencia, Tirant lo Blanch, 2020, pp. 39-68.

- "Datos personales de salud, investigación científica, y tecnología big data. De la necesidad de un marco normativo propio en la UE", en GIL MEMBRADO, C., (Directora y Coordinadora), *E-salud, autonomía y datos clínicos. Un nuevo paradigma,* Madrid, Dykinson, 2021, pp. 179-216.

- HERRÁN ORTIZ, A.I., "Inteligencia artificial, salud y derechos humanos: ¿hacia un gobierno de los algoritmos?", en GIL MEMBRADO, C., (Directora y Coordinadora) *Bioderecho y retos: M-Health, genética, IA, robótica y criogenización,* Madrid, Dykinson, 2022, pp. 318. 297- 335.

HIERRO SÁNCHEZ-PESCADOR, L., "¿Tienen los niños Derechos? Comentario a la Convención sobre los Derechos del niño". *Revista de Educación,* 1991, núm. 294, pp. 221-233.

HOHM, K.H., Grundrechtsträgerschaft und Grundrechtsmündigkeit Minderjähriger am Beispiel öffentlicher Heimerziehung, *Neue Juristische Wochenschrift*, 1986, núm. 50.

HOLMES DAWN, E., *Big data: una breve introducción,* Barcelona, Antoni Bosch, 2017.

LACRUZ BERDEJO, J.L., *Elementos de Derecho civil I. Parte general,* Vol. II, Madrid, Dykinson, 2010.

LAMA, AYMÁ, A., *La protección de los derechos de la personalidad del menor de edad.* Valencia, Tirant lo Blanch, 2006.

LASARTE ALVAREZ, C., *Compendio de derecho de la persona y del patrimonio,* Madrid, Dykinson, 2014.

LEÓN CAMACHO, J., "Evolución desarrollo de los Derechos Humanos. Hacia una cuarta generación", en MIRANDA GONÇALVES, R., y DA SILVA VEIGA, F., (Coordinadores), *El derecho público y privado ante las Nuevas Tecnologías,* Madrid, Dykinson, 2020, pp. 221-234.

LLANEZA GONZÁLEZ, P., *Datanomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos.* Barcelona, Editorial Planeta, 2019.

LLANO ALONSO, F., "Ética de la inteligencia artificial en el marco de la Unión Europea", en VARONA VILAR, S., (Editor), *Justicia algorítmica y neuroderecho: una mirada multidiscipilinar,* Valencia, Tirant lo Blanch, 2021, pp. 109-127.

LOZANO SÁNCHEZ, Z.B., "La familia y las redes sociales en los trastornos alimenticios en adolescentes de la época contemporánea", *Revista Científica In Crescendo,* núm. 2, Vol. 3, pp. 299-311.

MANGAS MARTÍN, A., y LIÑÁN NOGUERAS, D., *Instituciones y Derecho de la Unión Europea,* Madrid, Tecnos, 2011.

MARCOS MARÍN, T., "Los derechos de la personalidad de las personas-menores en el contexto internacional y su aplicación en el ordenamiento español*", Menores e Internet,* 1ª edición, Pamplona, Editorial Aranzadi, 2013, pp. 1-20.

MARTÍNEZ DE PISON, J., "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo", *Derechos y libertades,* 2017, núm. 37, Época II, pp. 51-84.

MARTÍNEZ LÓPEZ-SÁEZ, M., "El nuevo derecho a la portabilidad de datos personales a la luz del RGPD y la LOPDGDD: ¿objetivo ambicioso o misión imposible?", en GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (Editoras), *Reglamento General de Protección de Datos. Un enfoque nacional y comparado,* Valencia, Tirant lo Blanch, 2019, pp. 265-286.

MARTÍNEZ MARTINEZ, R., "Protección de datos personales y Redes sociales: un cambio de paradigma" en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales,* Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, pp. 83-115.

MARTÍNEZ OTERO, J.M., "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google. V. AEPD y Mario Costeja", *Revista de Derecho Político,* 2015, núm. 93, pp. 103-142.

- "Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento", *Revista Española de Derecho Constitucional,* 2016, núm. 106, pp. 119-148.

MARTINEZ VÁZQUEZ, F., "La tramitación parlamentaria de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales", en RALLO LOMBARTE, A., (Coordinador), *Tratado de protección de datos personales: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales,* Valencia, Tirant lo Blanch, 2019, pp. 53-79.

MARTOS DÍAZ, N., "Las políticas de privacidad, Redes sociales y protección de datos. El problema de la verificación de la edad", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores) *Derecho y Redes sociales,* Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, pp. 145-161.

MAYER-SCHÖNBERGER, V., Y CUKIER, K., *Big Data. A revolution That Will Transform How We Live, Work and Think,* London, John Murray, 2013.

- *Big Data. La revolución de los datos masivos,* Madrid, Turnen Noema, 2015.

MEDINA GUERRERO, M., "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales", *Teoría y Realidad Constitucional,* 2022, núm. 49, pp. 141-171.

MEGÍAS QUIRÓS, J.J., "Actividades personales y domésticas excluidas del ámbito de aplicación (comentario al artículo 2.2.c) RGPD y al artículo 2.2.a) LOPDGDD)" en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 355-375.

MINERO ALEJANDRE, G., "A vueltas con el derecho al olvido. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid,* 2012, núm. 30, pp. 129-155.

- "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario jurídico y Escolariense,* 2017, núm. 50, pp. 13-58.

MIRALLES, R., "El derecho a la portabilidad de los datos personales o prestaciones premium del tradicional derecho de acceso", en VALERO TORRIJOS, J., (Coordinador), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica,* Cizur Menor, Aranzadi, 2013, pp. 273-290.

MITLLANS PERELLÓ, E., "Impacto de las redes sociales en el derecho a la protección de datos personales", *Anuario de la Facultad de Derecho-Universidad de Alcalá II,* 2009, núm. 2, pp. 107-129.

MIQUEL GONZÁLEZ, J.M., "Cláusulas generales y desarrollo judicial del Derecho", *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid,* 1997, núm.1, pp. 297-326.

MORENO BOBADILLA, A., "Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: un antes y un después para el derecho al olvido digital", *Estudios constitucionales,* 2020, núm. 2, pp. 121-150.

- "El olvido previo a Internet: los orígenes del actual derecho al olvido digital", *Revista Mexicana de Derecho Constitucional,* 2020, núm. 43, pp. 199-217.

MORENTE PARRA, V., "El Big Data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", *Derechos y libertades*, 2019, núm. 41, Época II, pp. 225-260.

MORILLAS FERNÁNDEZ, M., "El menor y su derecho a la intimidad ante los riesgos en la utilización de redes sociales", *Revista de Derecho, Empresa y Sociedad,* 2013, núm. 1 enero-abril, pp. 162-176.

MUÑOZ, J., "El llamado derecho al olvido y la responsabilidad de los buscadores", *Diario la Ley*, mayo 2014, núm. 8317, sin paginación.

MURILLO DE LA CUEVA, P., *Informática y protección de datos personales,* Madrid, CEC, 1993.

- "El objeto de la Ley Orgánica de Protección de Datos de carácter personal" en TRONCOSO REIGADA, A., (Coordinador), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal,* Cizur Menor, Editorial Aranzadi, 2010, pp. 75-96.

NARAYANAN, A., Y SHMATIKOV, V., "Robust de-anonymization of large sparse datasets", *Security and Privacy,* 2008, IEEE Symposium, pp. 111-125.

NAVAS NAVARRO, S., *La personalidad virtual del usuario en Internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*, Valencia, Tirant lo Blanch, 2015.

NÚÑEZ RIVERO, C., "La protección del menor desde un enfoque del derecho constitucional", *Revista de Derecho UNED,* 2011, núm. 9, pp. 261-294.

NÚÑEZ SEOANE, J., "El derecho de información y acceso al funcionamiento de los algoritmos que tratan datos personales", en HUERGO LORA, A., (Coordinador), *La regulación de los algoritmos,* Cizur Menor, Aranzadi, 2020, pp. 299-315.

NÚÑEZ ZORRILLA, Mª.C., "Menor de edad e inteligencia artificial avanzada. Nuevos desafíos jurídicos", *Actualidad civil,* 2019, núm. 12, pp. 1-19.

OLIVER-LALANA, D., Y MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J., (Coordinador), *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Cizur Menor, Aranzadi, 2013, pp. 153-196.

ONCÓN DOMINGO, J. "Normativa internacional de protección de la infancia", *Cuadernos de Trabajo Social,* 2006, vol. 19, pp. 113-131.

OROZCO GONZÁLEZ, M., "Inteligencia artificial y robótica. Propuestas para la configuración de un estatuto jurídico", *Revista doctrinal Aranzadi,* 2021, núm. 8, pp. 1-28.

ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de los ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada),* Granada, Comares, 1994.

ORTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores), *Derecho y Redes sociales,* Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2010, pp. 23- 36.

- "El Reglamento de e-privacy", *Diario La Ley,* 2021, núm. 8, pp. 1-7.

ORZA LINARES, R., "La regulación del derecho al olvido en la Unión Europea. Aspectos críticos", en DURÁN RUIZ, F.J., (Director), *Desafíos de la protección de menores en la sociedad digital: Internet, redes sociales y comunicación,* Valencia, Tirant lo Blanch, 2018.

PALOMAR OLMEDA, A., "La protección del menor ¿avanzamos o retrocedemos?", *Revista Aranzadi de Derecho de deporte y Entretenimiento,* 2019, núm. 62/2019, pp. 1-29.

PALOMAR OLMEDA, A., y PÉREZ GONZÁLEZ, C., *La protección de datos: su marco constitucional y el contexto del nuevo Reglamento,* Pamplona, Editorial Aranzadi, 2008.

PANUNZIO, S., *Capacità. II. Diritto Pubblico,* en Enciclopedia Giuridica. Vol. V, Istituto della Enciclopedia Italiana, Roma, 1988.

PARISIER, E., *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos*, Madrid, Taurus, 2017.

PASCUAL MEDRANO, A., "Los Derechos Fundamentales y la Ley de Protección del Menor", *Revista Jurídica de Navarra,* 1996, núm. 22, pp. 249-264.

PAVÓN PÉREZ, J.A., "La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", *Anuario de la Facultad de Derecho. Universidad de Extremadura,* 2002, s/n, pp. 235-252.

PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? A propósito de la STJUE de 13 de mayo de 2014 (Google Spain, S.L. y Google Inc./ Agencia Española de Protección de datos [AEPD] Y Mario Costeja González, C-131/12", *Indret, revista para análisis del derecho,* 2015, núm. 1, pp. 1-50.

- "El nuevo derecho a la portabilidad de los datos personales en el Reglamento (UE) 2016/679, de 27 de abril de 2016", *Revista Crítica de Derecho Inmobiliario,* 2020, núm. 779, pp. 1531-1588.

PEGUERA POCH, M., "Publicidad online basada en comportamiento y protección de la privacidad", en RALLO LOMBARTE A., Y MARTINEZ MARTINEZ, R., (Coordinadores) *Derecho y Redes sociales,* Cizur Menor, Editorial Aranzadi-Thomson Reuters, 2ª ed, 2013. Versión online sin paginación.

- "En búsqueda de un marco normativo para la Inteligencia Artificial", en CERRILLO I MARTÍNEZ, A., y PEGUERA POCH, M., (Coordinadores), *Retos jurídicos de la Inteligencia Artificial,* Cizur Menor, Aranzadi, 2020, pp. 41-56.

PÉREZ BES, F., *La publicidad comportamental online,* Barcelona, UOC, 2012.

PÉREZ DÍAZ, R., "La protección de los datos del menor en el uso de las tecnologías de la información y de la comunicación (TIC)", *Revista de Derecho privado,* 2018, núm. 102, pp. 67-109.

- "Los menores de edad en la nueva Ley de Protección de Datos Personales", en FERNÁNDEZ VILLAZÓN, L.A., (Coordinador), *Derecho y Nuevas Tecnologías,* Cizur Menor, Aranzadi, 2020, pp. 155-180.

PÉREZ ESCODA, A., "Uso de *Smartphones* y redes sociales en alumnos/as de educación primaria". *Prisma social, revista de ciencias sociales,* marzo 2018, núm. 20, pp. 77-91.

PÉREZ LUÑO, A.E., "Informática y libertad", *Revista de Estudios Políticos,* 1981, núm. 24, pp. 31-54.

- "La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo", *Anuario de Derechos Humanos,* 1986-1987, núm. 4, pp. 259-291.

- "Las generaciones de derechos humanos", *Revista del Centro de Estudios Constitucionales,* 1991, núm. 10, pp. 203-217.

- "La protección de los datos personales del menor en Internet", *Anuario de la Facultad de derecho de Alcalá II,* 2009, núm. 2, pp. 134-175.

- "Principios de la protección de datos: consentimiento del afectado. El consentimiento de los menores (1ª parte)", en TRONCOSO REIGADA, A., (Coordinador), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal,* Cizur Menor, Editorial Aranzadi, 2010, pp. 473-494.

- "El consentimiento de los menores", en TRONCOSO REIGADA, A., (Coordinador), *Comentario a la Ley Orgánica de Protección de Datos de carácter personal,* Cizur Menor, Editorial Aranzadi, 2010, pp. 473-492.

PERIS MANGUILLOT, A., "Algoritmos: ¿podemos hacerlos transparentes y trazables en su proceso?", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial,* Valencia, Tirant lo Blanch, 2022, pp. 71-84.

PIÑAR MAÑAS, J.L., "El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales" en PIÑAR MAÑAS, J.L., (Director), *Redes sociales y privacidad del menor,* Madrid, Reus, 2011, pp. 61-83.

- "Hacia un nuevo modelo europeo de protección de datos", en PIÑAR MAÑAS, J.L., (Coordinador), *Reglamento Europeo de Protección de datos: hacia un nuevo modelo europeo de privacidad,* Madrid, Reus, 2016, pp. 15-23.

POLO ROCA, A., "Geolocalización, motores de búsqueda y cookies: tres grandes retos para la protección de datos", *Revista jurídica de Castilla y León,* 2020, núm. 52, pp. 141-184.

PLATERO ALCÓN, A., *El derecho al olvido en internet. La responsabilidad civil de los motores de búsqueda y las redes sociales: estudio doctrinal y jurisprudencial*, Madrid, Dykinson, 2021.

PLAZA PENADÉS, J., "Los derechos en la era digital (Comentario al artítulo 79 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 3855-3867.

- "La moderna configuración de la transparencia en la prestación de servicios y en la contratación en Internet", en COTINO HUESO, L., y CASTELLANOS CLARAMUNT, J., (Editores), *Transparencia y explicabilidad de la Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2022, pp. 225-248.

PRENSKY, M., "Digital Natives, Digital Immigrants", *MCB University Press,* 2001, vol. 9, núm. 5, pp. 1-6.

PROSSER, W., "Privacy", *California Law Review,* 1960, núm. 3, vol. 48, pp. 383-423.

PUYOL MORENO, J., "Una aproximación a Big Data", *Revista de Derecho UNED,* 2014, núm. 14, pp. 471-505.

RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de Derecho Político UNED,* 2012, núm. 85, pp. 13-56.

- "El debate europeo sobre el derecho al olvido en Internet", en RALLO LOMBARTE, A., y GARCÍA MAHAMUT, R., (Editores) *Hacia un nuevo derecho europeo de protección de datos,* Valencia, Tirant lo Blanch, 2015, pp. 703-737.

- "De la libertad informática a la constitucionalización de nuevos derechos digitales 1978-2018", *Revista de Derecho político,* 2017, núm. 100, pp. 639-669.

- "Del derecho a la protección de datos a la garantía de nuevos derechos digitales", en RALLO LOMBARTE, A., (Director) *Tratado de protección de datos. Actualizado con la Ley 3/2018, de 5 de diciembre de 2018, de Protección de datos personales y Garantías Digitales*, Valencia, Tirant lo Blanch, 2019, pp. 23-53.

RAMÓN FERNÁNDEZ, F., "Menores y redes sociales: cuestiones legales", *Revista sobre la infancia y la adolescencia,* abril 2015, núm. 8, pp. 33-43.

- "Protección de menores y educación en el entorno digital (X y XVII)", en COTINO HUESO, L., (Coordinador) *La Carta de Derechos Digitales,* Valencia, Tirant lo Blanch, 2022, pp. 155-180.

RAMOS CHAPARRO, E., "Niños jóvenes en el derecho civil y constitución", *Derecho Privado y Constitución,*1995, núm. 7 septiembre-diciembre, pp. 167-229.

REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson, 2008.

REYES MENÉNDEZ, D., "El acceso del menor a las redes sociales y el problema de su autentificación: La necesidad de una respuesta tecnológica", *Diario La Ley,* 2019, núm. 9935, pp. 1-13.

RIGAUX, F., "L´elaboration d´un right of privacy par la jurisprudence americaine", *Revue Internationale de Droit Comparé,* XXXIII, 1980, p. 701-730.

RIVERA ÁLAVA, J., "La Ley Orgánica 1/96, de 15 de enero, de protección jurídica del menor: algunas consideraciones relevantes", *Cuadernos de Trabajo Social,* 1997, núm. 10, pp. 75-92.

RIVERO HERNÁNDEZ, F., *El interés del menor*, Madrid, Dykinson, 2002.

RODRÍGUEZ DUARTE, L., "Cookies: consentimiento, su revocación y Reglamento E-privacy", *Derecho Digital e Innovación (La Ley Digital)*, tercer trimestre 2020, núm. 6, pp. 1-11.

ROIG, A., "E-privacidad y redes sociales", *Revista de Internet, Derecho y Política*, 2009, núm. 9, p. 42-52.

ROMERO COLOMA, A.M., *Los bienes y derechos de la personalidad,* Madrid, Trivium, 1985.

- *Los derechos al honor y a la intimidad frente a la libertad de expresión e información. Problemática procesal,* Barcelona, Serlipost, 1991.

RUBÍ PUIG, A., "Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores", *Revista de educación y derecho*, 2021, núm. 24, pp. 1-24.

RUIZ MIGUEL, C., "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", *RDCE*, 2003, núm. 14, pp. 7-43.
SAIZ MORENO, F., CORTES GENERALES: *Constitución Española. Trabajos parlamentarios,* Tomo I, Madrid, Cortes Generales, 1980.

SÁNCHEZ GÓMEZ. A., "El marco normativo tradicional para la protección de los derechos de la personalidad del menor. ¿Alguna asignatura pendiente en el siglo XXI?", *Revista Doctrinal Aranzadi Civil-Mercantil,* 2016, núm. 11/ parte Doctrina, 2016, pp. 1-37.

- "Las Nuevas Tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: carencias, interrogantes y retos del legislador", *Revista de Derecho, Empresa y Sociedad,* 2016, núm. 9 julio-diciembre, pp. 78-92.

SANCHO VILLA, D., "Las decisiones individuales automatizadas, incluida la elaboración de perfiles (comentario al artículo 22 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 1725-1745.

SANTAMARÍA RAMOS, J.F., "Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (Comentario al artículo 95 LOPDGDD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 4295-4316.

SANTOS MORÓN, Mª.J., "Los contornos del derecho al olvido en España. La aplicación por los Tribunales españoles de la jurisprudencia europea", *Revista de Derecho civil,* abril-junio 2022, núm. IX, pp. 71-112.

SERRANO PEREZ, Mª.M., "El derecho fundamental a la protección de datos. Su contenido esencial", *Anuario multidisciplinar para la modernización de las Administraciones Públicas,* 2005, núm. 1, pp. 245-265.

- "El consentimiento de los menores de edad para el tratamiento de datos personales (comentario art. 7 LOPDGDD)" en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 989-1011.

SHOPON, M.; TUMPA, S.N.; BATHIA, Y.; PAVAN KUMAR, K.N.; GAVRILOVA, M.L., "Biometric Systems De-Identification: Current Advancements and Future Directions", *Journal of Cybersecurity and Privacy,* 2021, núm 1, pp. 470-495.

SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital,* Valencia, Tirant lo Blanch, 2012.

- *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014,* Boch, Barcelona, 2015.

SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Revista de Derecho Público: Teoría y Método,* 2021, vol. 3, pp. 85-127.

SOTO, Y., "Datos masivos con privacidad y no contra privacidad", *Revista Biología y Derecho,* 2017, núm. 40, pp. 101-114.

TERWAGNE, C., "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Revista de Internet, Derecho y Política*, 2012, núm. 13, pp. 53-56.

TIANA FERRER, A., "Declaración de los Derechos del Niño y Convención sobre los Derechos del Niño", *Transatlántica de educación*, 2008, vol. 5, pp. 95-112.

TOMÁS MARTÍNEZ, G., y GÓMEZ URQUIJO, L., "La protección al cliente bancario en el nuevo marco de la gobernanza financiera europea. Breve comentario a la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios", *Diario La Ley,* 2012, núm. 7842, versión online sin paginación.

TORAL LARA, E., "Menores y redes sociales: consentimiento, protección y autonomía", *Derecho privado y constitución,* 2020, núm. 36, pp. 179-218.

TORO, M., y LANIADO, H., "Big data: historia, definición, herramientas y aplicaciones en la industria", *Revista VirtualPro*, 2019, núm. 204, pp. 1-5.

TRONCOSO REIGADA, A., "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público,* (mayo- diciembre 2003), núm. 19-20, pp. 232-334.

- *La Protección de Datos Personales: en busca del equilibrio,* Valencia, Tirant lo Blanch, 2010.

- "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo,* 2012, núm. 43, pp. 1-146.

- "Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una". *Revista de los Estudios de Derecho y Ciencia de la UOC,* noviembre 2012, núm. 15, pp. 61-75.

- "La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías Digitales", *Derecom,* marzo-septiembre 2019, núm. 26, pp. 131-140.

- "Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGG)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* Tomo I, Cizur Menor, Civitas, 2021, pp. 848-907.

ULLOA RUBIO, I., "Comité Europeo de Protección de Datos (Comentario a los artículos 68 a 76 RGPD)", en TRONCOSO REIGADA, A., (Director), *Comentario al Reglamento General de Protección de Datos y a la ley Orgánica de Protección de datos personales y Garantía de los Derechos digitales,* Madrid, Civitas, 2021, pp. 2917-2945.

URABAYEN, M., *Vida privada e información: un conflicto permanente,* Pamplona, EUNSA, 1977.

VAŠÁK, K., "Les différents catégories des droits de l´homme", en LAPEYRE, A., DE TINGUY, F., Y VASAK , K., (Directores), *Les dimensions universe- lles des Droits de l´Homme,* UNESCO-Bru- ylant, Bruxelles, 1990, p. 297.

VÁZQUEZ DE CASTRO, E., "Protección de datos personales, redes sociales y menores", *Revista Aranzadi de Derecho y nuevas Tecnologías,* 2012, núm. 29/2012 parte Doctrina, pp. 1-26.

VELA SÁNCHEZ, A., "El interés superior del menor como fundamento de la inscripción de la filiación derivada del convenio de gestación por encargo". *Diario La Ley (digital),* 2013, núm. 8162.

- "La gestación por sustitución en las Salas de lo Social del Tribunal Supremo y de los Tribunales Superiores de Justicia. A propósito de la prestación por maternidad en los casos de nacimientos derivados de convenio gestacional", *Diario la Ley,* 2017, núm. 8927, pp. 1-16.

VILASAU SOLANA, M., "Las exigencias de información en el RGPD y la LO 3/2018, de protección de datos y garantía de los derechos digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?", en GARCÍA MAHAMUT, R., Y TOMÁS MALLÉN, B., (Editoras), *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado,* Valencia, Tirant lo Blanch, 2019, pp. 209-236.

WACHTER, K., "Los rasgos y atributos privados son predecibles a partir de registros digitales del comportamiento humano", *PNAS,* 2013, núm. 15, pp. 5802-5805.

WARREN, S.D., y BRANDEIS, L.D., "The Right to Privacy", *Harvard Law Review,* de 15 de diciembre de 1980, núm.5, Vol.4, pp. 193-220.

II.- REFERENCIAS ORGANISMOS OFICIALES

2.1 Documentos organismos oficiales internacionales

COMITÉ DE LOS DERECHOS DEL NIÑO. Observación general número 25, del de 2 de marzo de 2021, relativa a los derechos de los niños en relación con el entorno digital. Obtenido de: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0myCaUSrDC%2F0d3UDPTV4y05%2B9GME0qMZvh9UPKTXcO12 (última consulta el 2 de febrero de 2023).

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS. "*Report and Guidance on Privacy in Social Network Services (Memorandum Roma)*". 43ª reunión celebrada en Roma los días 3 y 4 de marzo de 2008.
OCDE. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, París, de 23 de septiembre de 1980.

OCDE. Declaración sobre flujos de datos transfronterizos, de 11 de abril de 1985. Obtenido de: https://www.oecd.org/sti/ieconomy/15590267.pdf (última consulta: 22 de septiembre de 2020).

OCDE. Declaración Ministerial elaborada por el Grupo de Trabajo sobre Seguridad de la Información e Intimidad de la Dirección de Ciencia, Tecnología e Industria relativa a la protección de la intimidad en las redes globales, Ottawa, 7 a 9 de octubre de 1998, (98)10/FINAL.

OCDE. Recomendación para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad, de 25 de julio de 2002. Obtenido de: https://www.oecd.org/sti/ieconomy/34912912.pdf (última consulta el 5 de septiembre de 2022).

OCDE. Recomendación, de 12 de julio de 2007, sobre a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad. Obtenido de: https://www.oecd.org/sti/ieconomy/34912912.pdf (última consulta el 5 de septiembre de 2022).

OCDE. Recomendación del Consejo sobre Inteligencia Artificial, de 22 de mayo de 2019, OCDE/JURÍDICO/0449.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 217 A (III), de la Asamblea General de las Naciones Unidas, por la que se adopta la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 1386 (XIV), de la Asamblea General de las Naciones Unidas sobre la Declaración de los Derechos del Niño, de 20 de noviembre de 1959.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 2450 (XXIII), de la Asamblea General de las Naciones Unidas sobre Derechos Humanos y progresos Científicos y Tecnológicos, de 19 de diciembre de 1968.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Informe final de la Comisión de Derechos Humanos sobre "El estudio de los principios rectores pertinentes a la utilización de ficheros computadorizados de datos personales", de 30 de junio de 1983.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 40/33 adoptada por la Asamblea General de las Naciones Unidas sobre Reglas mínimas de las Naciones Unidas para la administración de la justicia de menores (Reglas de Beijing), 28 de noviembre de 1985.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 45/95, por la que se aprueban los principios rectores para la reglamentación de los ficheros computadorizados de datos personales, de 14 de diciembre de 1990. Obtenido de: http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf (última consulta el 8 de marzo de 2022).

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Observación general número 14 del Comité de las Naciones Unidas de Derechos del Niño, de 29 de mayo de 2013.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 68/167, de la Asamblea General sobre el derecho a la privacidad en la era digital, de 18 de diciembre de 2013.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 69/166, de la Asamblea General sobre el derecho a la privacidad en la era digital, de 18 de diciembre de 2014.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 28/16, del Consejo de Derechos Humanos sobre la privacidad en la era digital, de 26 de marzo de 2015.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 70/125, sobre Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, de 16 de diciembre de 2015.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 20/08 del Consejo de la Asamblea General de las Naciones Unidas, sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, de 27 de junio de 2016.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 32/13, del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet, de 1 de julio de 2016.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 71/199, de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital, de 19 de diciembre de 2016.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 34/7, del Consejo de Derechos Humanos sobre la privacidad en la era digital, de 23 de marzo de 2017.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Informe del Secretario General de las Naciones Unidas, sobre la Situación de la Convención sobre los Derechos del niño, presentado en el septuagésimo segundo periodo de sesiones en relación a la Promoción y protección de los derechos del niño, de 24 de agosto de 2017.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 38/7, del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet, de 5 de julio de 2018.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución 73/179, de la Asamblea General de sobre el derecho a la privacidad en la era digital, de 17 de diciembre de 2018.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Recomendación sobre la ética de la Inteligencia Artificial del Grupo Especial de Expertos de la ONU, de 7 de mayo de 2020.

Resolución sobre la intimidad de los niños en línea, adoptada en la 30ª Conferencia Internacional de Autoridades de protección de datos y privacidad, propuesta por el Comisario de Protección de datos de Canadá, adoptada en Estrasburgo, octubre de 2008. Obtenido de https://edps.europa.eu/sites/default/files/publication/08-10-17_strasbourg_children_online_es.pdf (última consulta el 8 de marzo de 2022).

UNESCO. Recomendación sobre inteligencia artificial, adoptada el 23 de noviembre de 2021. Obtenido de: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa (ultima consulta el 18 de abril de 2023).

30ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad celebrado en Estrasburgo los días 15 a 17 de octubre de 2008, sobre la "Protección de la privacidad en los servicios de redes sociales".

Resolución sobre Estándares Internacionales aprobados en la 30ª Conferencia Internacional sobre Privacidad y Protección de Datos celebrada en Madrid, 2009. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf (última consulta: 22 de septiembre de 2020).

32nd *International Conference of Data Protection and Privacy Commissioners about Resolution on Privacy by Design*. Jerusalen (Israel) 27-29 October, 2010. Obtenido de: http://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf (última consulta el 9 de marzo de 2022).

41ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Tirana los días 21 y 24 de octubre de 2019, sobre elevación de los estándares globales de protección de datos en la era digital, Obtenido de: https://privacyconference2019.info/ (última consulta el 22 de marzo de 2023).

2.2 Documentos organismos oficiales de la Unión Europea

AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. Manual de legislación europea sobre los derechos del niño. Año 2015. Obtenido de: https://www.echr.coe.int/Documents/Handbook_rights_child_SPA.PDF (última consulta el 1 de septiembre de 2022).

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 3/2018, relativas al ámbito territorial del RGPD (artículo 3), de 12 de noviembre de 2019.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 4/2019, relativas al artículo 25 Protección de datos desde el diseño y por defecto, de 20 de octubre de 2020.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD, de 7 de julio de 2020.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 4 de mayo de 2020.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 8/2020 on the targeting of social media users*, Version 2.0, adopted on 2 september 2020.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 01/2022 on data subjet rights-Right of access*, Version 1.0, adopted on january 2022.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them*, Version 1.0, adopted on 14 March 2022.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)*, adopted on 5 december 2022. Obtenido de: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf (última consulta el 30 de enero de 2023)

COMISIÓN EUROPEA. Informe sobre "La afirmación de los Derechos fundamentales en la Unión Europea. Ha llegado el momento de actuar", de febrero de 1999, elaborado por un Grupo de Expertos bajo la Presidencia del Sr. D. Spiros Simitis. Obtenido de: https://sid.usal.es/idocs/F8/8.4.1-520/8.4.1-520.pdf (última consulta el 9 de marzo de 2022).

COMISIÓN EUROPEA. Informe de Evaluación de la Comisión, de 27 de febrero de 2001, sobre la aplicación de la Recomendación del Consejo, COM (2001) 106 Final no publicado en el DOUE.

COMISIÓN EUROPEA. Informe de la Comisión Europea, de 15 de mayo de 2003, relativo al primer informe sobre la aplicación de la Directiva sobre protección de datos 95/46, COM (2003) 265 final.

COMISIÓN EUROPEA. Informe de la Comisión Europea, de 7 de marzo de 2007 sobre el Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, COM (2007) 87 final.

COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre "Un enfoque global de la protección de datos personales en la Unión Europea", de 4 de noviembre de 2010, COM (2010) 609 final.

COMISIÓN EUROPEA. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre "Una agenda de la UE en Pro de los derechos del Niño", de 15 de febrero de 2011, COM (2011) 60 final.

COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Comité económico y social europeo y al Comité de las regiones sobre una "Estrategia europea en favor de una Internet más adecuada para los niños", del 2 de mayo de 2012, COM (2012) 196 final.

COMISIÓN EUROPEA. Propuesta de Reglamento sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), de 1 de octubre de 2017, COM (2017) 10 final.

COMISIÓN EUROPEA. Informe sobre la Propuesta de Reglamento de la Comisión Europea sobre sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), de 20 de octubre de 2017. Obtenido de: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_ES.html (última consulta el 18 de abril de 2013).

COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico Social Europeo y al Comité de las Regiones, sobre "Una Inteligencia artificial para Europa", de 25 de abril de 2018, COM (2018) 237 final.

COMISIÓN EUROPEA. Libro Blanco sobre inteligencia artificial sobre "Un enfoque europeo orientado a la excelencia y a la confianza", de 19 de febrero de 2020, COM (2020) 65 final.

CONSEJO EUROPEO. Directrices de la UE para la promoción y protección de los derechos del menor, aprobadas por el Consejo el 10 de diciembre de 2007, no publicadas en el Diario Oficial de la Unión Europea. Obtenido de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:l33604&from=ES (última consulta el 2 de septiembre de 2022).

CONSEJO DE EUROPA. Resolución 68/509/CE, de la Asamblea Parlamentaria sobre los derechos humanos y los nuevos logros científicos y técnicos, de 31 de enero de 1968.

CONSEJO DE EUROPA. Resolución R (73) 22, del Comité de Ministros relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973.

CONSEJO DE EUROPA. Resolución R (74) 29 del Comité de Ministros sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, de 20 de septiembre de 1974.

CONSEJO DE EUROPA. Recomendación (99) 5, adoptada por el Comité de Ministros durante la 660ª reunión de Delegados de Ministros sobre la protección de la vida privada en Internet. Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información", de 23 de febrero de 1999.

CONSEJO DE EUROPA. Decisión por la que se adopta el Protocolo *amending the Conovention for the Protection of Individuals with regard to Automattic Processing of Personal Data*, de 18 de mayo de 2018. Obtenido de: https://rm.coe.int/16808ac918 (última consulta el 5 de septiembre de 2022).

EURO BARÓMETRO. Especial número 359, Actitudes hacia la protección de datos y la identidad electrónica en la Unión Europea, de junio de 2011. Obtenido de: https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=es (última consulta el 20 de noviembre de 2022).

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, "*Security Issues and Recommendations for Online Social Networks*", Position paper, núm. 1, de octubre de 2007.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Recomendación 1/1999 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, de 23 de febrero de 1999, DG XV C 5093/98/final WP 17.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 1/2008 sobre cuestiones de protección de datos en relación con buscadores, de 4 de abril de 2008, WP 148.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 2/2009 sobre la protección de datos personales de los niños (Directrices generales y especial referencia a las escuelas), de 11 de febrero de 2009, WP 160.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2009 sobre las redes sociales en línea, de 12 de junio de 2009, WP 163.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 1/2009 sobre el futuro de la privacidad, de 1 de diciembre de 2009, WP 168.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 2/2010 sobre publicidad comportamental en línea, de 22 de junio de 2010, GT 171.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies, de 7 de junio de 2012, WP 194.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes, de 27 de febrero de 2013, WP 202.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 5/2014 sobre técnicas de anonimización, de 10 de abril de 2014, WP 216.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de abril de 2014, WP 217.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Dictamen 8/2014 sobre la evolución reciente del Internet de los objetos, de 16 de septiembre de 2014, WP 223.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Directrices sobre el derecho a la portabilidad de los datos, de 5 de abril de 2017, WP 242.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, de 28 de noviembre de 2017, WP 259.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, de 6 de febrero de 2018, WP 251.

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, de 11 de abril de 2018, WP 260.

Informe de CyberSec4Europe (CyberSec4Europe Network of Competence Centers for Europe) y ASAP (Adaptive Security and Privacy). Obtenido de: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9295422 (última consulta el 28 de septiembre de 2021).

PARLAMENTO EUROPEO. Set de preguntas a Mark Zuckerberg en relación a Cambridge Analytica. Obtenido de: https://www.europarl.europa.eu/resources/library/media/20180604RES04911/20180604RES04911.pdf , p. 10. (última consulta el 5 de noviembre de 2021).

PARLAMENTO EUROPEO. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Obtenido de: https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_ES.html#title2 (última consulta el 14 de abril de 2022).

PARLAMENTO EUROPEO. Declaración Europea de los Derechos y Principios Digitales para la Década Digital. Diario Oficial de la Unión Europea, de 23 de enero de 2023, C 23/1.

PARLAMENTO EUROPEO. Documento del Servicio de Investigación del Parlamento Europeo, sobre *Verification methods for children*, de febrero de 2023. Obtenido de: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf (última consulta el 8 de marzo de 2023).

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Dictamen del Supervisor Europeo de Protección de Datos sobre la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, de 16 de octubre de 2010. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_es.pdf (última consulta el 11 de febrero de 2023).

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Dictamen 4/2015 sobre Hacia una nueva ética digital. Datos, dignidad y tecnología, de 11 septiembre de 2015. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf (última consulta el 26 de enero de 2013).

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Opinión 7/2015 sobre "Hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios la protección de datos desde el diseño y la rendición de cuentas", de 19 de noviembre de 2015. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (última consulta el 13 de febrero de 2023).

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Resumen de conclusiones del dictamen del Supervisor Europeo de Protección de Datos sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital, Diario Oficial de la Unión Europea, C 463/08, 13 de diciembre de 2016. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_es.pdf (última consulta 6 de julio de 2020)

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. Opinión 6/2017 sobre la propuesta de regulación sobre la privacidad y comunicaciones electrónicas (e-privacy), de 24 de abril de 2017. Obtenido de: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf (última consulta el 8 de febrero de 2023)

2.3 Documentos organismos oficiales españoles

2.3.1 Guías, Estudios, Memorias e Informes jurídicos de organismos oficiales españoles

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Protección de datos: Guía para el ciudadano. Obtenido de https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf (última consulta 6 de mayo de 2021).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria de la Agencia Española de Protección de Datos del año 2008. Obtenido de: http://www.resi.org.mx/icainew_f/images/Biblioteca/PDP/memorias/memoria_2008.pdf (última consulta el 28 de abril de 2021).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria de la Agencia Española de Protección de Datos del año 2009. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2009.pdf , p. 11. (última consulta el 3 de abril de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS e INSTITUTO NACIONAL DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, febrero de 2009. Obtenido de: https://www.uv.es/limprot/boletin9/inteco.pdf (última consulta el 3 de diciembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Memoria de la Agencia Española de Protección de Datos del año 2010. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2010.pdf (última consulta el 3 de abril de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe sobre políticas de privacidad en Internet. Adaptación al RGPD, de septiembre de 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf (última consulta el 1 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del Reglamento Europeo de Protección de datos para responsables del tratamiento, 2018. Obtenido de: https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf (última consulta el 9 de marzo de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía de privacidad desde el diseño, octubre de 2019. Obtenido de: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf (última consulta el 7 de febrero de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía sobre el uso de las cookies, julio de 2020. Obtenido de https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (última consulta el 30 de junio de 2021).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, de febrero de 2020. Obtenido de: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (última consulta el 16 de julio de 2021).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Memoria de la Agencia Española de Protección de Datos del año 2021. Obtenido de: https://www.aepd.es/es/documento/memoria-aepd-2021.pdf, (última consulta el 13 de abril de 2022).

AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS. Principales novedades del RGPD. Obtenido de: https://apdcat.gencat.cat/es/drets_i_obligacions/rgpd/novetats/ (última consulta el 12 de mayo de 2021).

AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS. Inteligencia Artificial: decisiones automatizadas en Cataluña. Obtenido de: https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf (última consulta el 12 de enero de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; AGENCIA CATALANA DE PROTECCIÓN DE DATOS; AGENCIA VASCA DE PROTECCIÓN DE DATOS. Guía para el cumplimiento del deber de informar. Obtenido de: https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/modeloclausulainformativa-es.pdf (última consulta el 10 de mayo de 2021).

AGENCIA VASCA DE PROTECCIÓN DE DATOS. Decides tú cómo proteger tu privacidad, enero de 2007. Obtenido de: https://www.avpd.euskadi.eus/contenidos/informacion/udcd/es_udcd/adjuntos/folleto.pdf (última consulta el 12 de septiembre de 2022).

FISCALÍA GENERAL DEL ESTADO. Instrucción 2/2006, de 15 de marzo, sobre el Fiscal y la protección del derecho al honor, intimidad y propia imagen de los menores, Boletín Oficial del Estado, ref. FIS-I-2006-00002.

INSTITUTO NACIONAL DE ESTADÍSTICA (INE). Encuesta sobre el Equipamiento y uso de Tecnologías Información y Comunicación en los Hogares, de 16 de noviembre de 2020, TIC_H-2020. Obtenido de: https://www.ine.es/prensa/tich_2020.pdf (última consulta 7 de septiembre de 2021).

OBSERVATORIO ESPAÑOL DE LAS DROGAS Y DE LAS ADICCIONES, Encuesta sobre Uso de Drogas en Enseñanzas Secundarias en España (ESTUDES 2017-2018). Obtenido de: https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/sistemaInformacion/pdf/ESTUDES_2018_Informe.pdf (última consulta el 1 de septiembre de 2022).

OBSERVATORIO ESPAÑOL DE LAS DROGAS Y DE LAS ADICCIONES. Encuesta sobre Uso de Drogas en Enseñanzas Secundarias en España (ESTUDES 2018-2019). Obtenido de: https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/sistemaInformacion/pdf/ESTUDES_2018-19_Informe.pdf (última consulta el 12 de septiembre de 2022).

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. Libro blanco de los Contenidos Digitales, de 2008. Obtenido de: https://www.ontsi.red.es/sites/ontsi/files/1233569673805.pdf (última consulta 24 de marzo de 2021).

GOBIERNO DE ESPAÑA. Carta de Derechos Digitales. Obtenido de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (última consulta el 8 de febrero de 2022).

2.3.2 Resoluciones, Recursos, Informes jurídicos y Procedimientos Sancionadores de la AEPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 327/2003 sobre el carácter de dato personal de la dirección IP. Obtenido de: https://www.aepd.es/es/documento/2003-0327.pdf (última fecha de consulta el 1 de julio de 2021).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Declaración sobre buscadores de Internet de 1 de diciembre de 2007. Obtenido de: https://www.facua.org/es/documentos/declaracionsobrebuscadoresdeinternet.pdf (última consulta el 12 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución 00284/2008 del Procedimiento Sancionador 00281/2007 sobre la verificación de la edad de menores.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES. Resolución 01800/2008 por la que se resuelve el Procedimiento Sancionador 479/2008 sobre la difusión de vídeos en la plataforma Youtube.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0615/2008, Gabinete jurídico, Madrid.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recomendaciones de la sobre los Derechos de los niños y niñas y deberes de los padres y madres, año 2008. Obtenido de: https://www.adolescenciasema.org/usuario/documentos/Derechos%20y%20deberes%20padres%20y%20menores%20en%20internet%20de%20la%20agencia%20de%20proteccion%20de%20datos.pdf (última consulta el 1 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0300/2009, Gabinete jurídico, Madrid.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/00898/2010 (TD/01887/2009). Obtenido de: https://www.aepd.es/es/documento/td-01887-2009.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Recurso 01663/2010 del Procedimiento Sancionador 00023/2010.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Recurso 01680/2010 (TD/00650/2010). Obtenido de: https://www.aepd.es/es/documento/td-00650-2010.pdf (última consulta el 14 de abril de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recurso 02177/2010 del Procedimiento Sancionador 00234/2011.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02283/2010 (TD/00754/2010). Obtenido de: https://www.aepd.es/es/documento/td-00754-2010.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02958/2011 sobre el bloqueo y cancelación de datos personales. Obtenido de: https://www.aepd.es/es/documento/td-01259-2011.pdf (última consulta el 29 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución 02261/2011. Obtenido de: https://www.aepd.es/es/informes-y-resoluciones/resoluciones (última consulta el 12 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recurso 02636/2011 del Procedimiento Sancionador 00339/2011.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02806/2012 (TD/01178/2012). Obtenido de: https://www.aepd.es/es/documento/td-01178-2012.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02538/2013 (TD/1065/2013). Obtenido de: https://www.aepd.es/es/documento/td-01065-2013.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe Jurídico 0197/2013, Gabinete jurídico, Madrid.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución 01870/2017, (PS/00082/2017). Obtenido en: https://www.aepd.es/sites/default/files/2019-12/PS-00082-2017_REC.pdf (última consulta el 30 de mayo de 2022). .

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución 00512/2018, (TD/02270/2017). Obtenido de: https://www.aepd.es/es/documento/td-02270-2017.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Informe 0017/2019, de 16 de junio de 2020 sobre "Wifi Tracking".

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución /00552/2019 (TD/00195/2019). Obtenido de: https://www.aepd.es/es/documento/td-00195-2019.pdf (última consulta el 15 de septiembre de 2022).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento Sancionador PS/00388/2020. Obtenido de: https://www.aepd.es/es/documento/ps-00388-2020.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento Sancionador PS/00437/2020. Obtenido de https://www.aepd.es/es/documento/ps-00437-2020.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Procedimiento Sancionador PS/00500/2020. Obtenido de: https://www.aepd.es/es/documento/ps-00500-2020.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento Sancionador PS/00327/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00327-2021.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento Sancionador PS/00404/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00404-2021.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Procedimiento Sancionador PS/000539/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00539-2021.pdf (última consulta el 5 de enero de 2023).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Procedimiento Sancionador PS/00609/2021. Obtenido de: https://www.aepd.es/es/documento/ps-00609-2021.pdf (última consulta el 5 de enero de 2023).

2.4 Documentos oficiales de las agencias de protección de datos nacionales

CNIL. *Quatrième rapport d´activité de la CNIL*, 1982-1983, París, La Documentation Française.

CNIL. *20ème rapport d´activité de la CNIL*, 1999, París, La Documentation Française.

CNIL. *30éme rapport d´activité de la CNIL*, 2009, París, La Documentation Française.

CNIL. Informe sobre *Algorithmes: prévenir l´automatisation des discriminations*, 2020. Obtenido de: https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_algorithmes_access_0.pdf (última consulta el 1 de septiembre de 2022).

CNIL. Informe de la Comisión francesa de protección de datos (CNIL) sobre las prácticas digitales de los jóvenes entre 11 a 18 años. Obtenido de: https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf (última consulta el 20 de octubre de 2021).

CNIL. Consulta pública de la Comisión francesa de protección de datos (CNIL) sobre los derechos de los menores en el entorno digital del año 2021. Obtenido de: https://www.cnil.fr/sites/default/files/atoms/files/consultation_publique_sur_les_droits_des_mineurs_-_synthese_des_contributions.pdf (última consulta el 29 de septiembre de 2021).

CNIL. Recomendación núm. 7 realizada por la Comisión francesa de protección de datos (CNIL) en relación a los derechos digitales de los menores. Obtenido de: https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee (última consulta el 29 de septiembre de 2021).

CNIL. *Délibération núm. 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif).* Obtenido de: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337 (última consulta el 8 de febrero de 2023).

GARANTE PER LA PROTEZIONE DEL DATI PERSONALI. Decisión, de 10 de noviembre de 2004 sobre el recurso *Reti Telematiche e Internet- Motori di ricerca e provvedimenti di Autoritá indipendenti: le misure necessarie a garantire il c.d. "diritto all´oblio".* Obtenido de: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1116068 . (última consulta el 13 de abril de 2022).

INFORMATION COMMISSIONER´S OFFICE DE REINO UNIDO (ICO). Código de Edad. Obtenido de: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (última consulta el 29 de septiembre de 2021).

INFORMATION COMMISSIONER´S OFFICE DE REINO UNIDO (ICO). Contribución de la Information Commissioner´s Office del Reino Unido a la consulta de la comisión europea, Obtenido de: http://bit.ly/pBfWna (última consulta el 24 de abril de 2023).

COMISIONADO FEDERAL DE PROTECCIÓN DE DATOS Y LIBERTAD DE INFORMACIÓN. Guía sobre *cookies* de la Conferencia de Autoridades Independientes de protección de datos de los gobiernos federales y estatal alemán, de marzo de 2019. Obtenida de: 20190405_oh_tmg.pdf (datenschutzkonferenz-online.de) (última consulta el 8 de febrero de 2023).

III.DOCUMENTOS DE INTERNET

CANTANTE NATASHA Y MIKE ISAAC, "Facebook to pay 500 million to settle facial recognition suit", *The new York Times*, January 29 of 2020. Obtenido de: https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html (última consulta el 2 de noviembre de 2021).

CASTILLO, C., "La oferta y la demanda del contenido audiovisual en la era de los datos masivos", 2018. Obtenido de https://chato.cl/papers/castillo_2018_oferta_disponiblidad_contenido_audiovisual-ES.pdf (última consulta 12 de enero de 2022).

CHABERT, J.L., "A History of Algorithms: From the Pebble to the Microchip*"*, en STEINER, C., *Una breve historia de hombres y algoritmos*, 1999. Obtenido de: https://catedradatos.com.ar/media/5.-Steiner-Una-breve-historia-de.pdf (última consulta el 7 de febrero de 2022).

COMISIÓN EUROPEA. punto único de acceso en Europa para toda la información destinada a los niños en la UE sobre los derechos del niño. Obtenido de: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/rights-child/eu-action-rights-child_es (última consulta 13 de abril de 2021).

CORTÉS, U., "Hay que enseñar a los límites de la tecnología y pensamiento crítico", *Autoridad Catalana de Protección de Datos. Inteligencia Artificial: decisiones automatizadas en Cataluña.* Obtenido de: https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf (última consulta el 12 de enero de 2022).

CLAVIJO SUNTURA, H., "El interés del menor como concepto jurídico indeterminado y las técnicas de su determinación en situaciones de crisis familiares", *Pórtico Legal.* Obtenido de: *https://www.porticolegal.com/pa_articulo.php?ref=306* (Consultado el 10 de julio de 2020).

Estrategia Nacional de Inteligencia Artificial (ENIA) del Gobierno de España, de 21 de abril de 2021. Obtenido de https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf (última consulta el 26 de enero de 2022).

Federal Trade Commission para la protección de los consumidores (EEUU), reglas de protección de la privacidad en línea de los niños. Obtenido de: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4 (última consulta el 27 de octubre de 2021).

FERNÁNDEZ, C., "El Parlamento Europeo estudia someter a los sistemas como ChatGPT a las mismas obligaciones que los sistemas de IA de alto riesgo", *Diario La Ley (Ciberderecho).* Obtenido de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAEWQTW-DMAyGf01znAL00B1yKXBoRVk_2LSdJgMWRMsSFCds_Pt5VNoOfiXbrx_ZDtCS2

mYCuhDBFK5T6ZroGRtofzvO9-j3i5IiuADmiqSSbJsIGt1XDbMeIGhn9-BV4yMK3Z-qyw2NOqGNZ69tpycwSfqeSO71qi6llGnymO12UszoiYfVix7QBhSjHsaKI9xZQKSpgACqeMqbt3O5SbdFs8na8pXl-MxSl4IQfDeeYUBVaQrAG0YToHfUHPIHoOlbGPvBp91W4x3dGU4YjTkYtP3f9lRBtN14ieiXe8n8Fw69qi4MFTBNZrk6w79YPZMj5sdPPuJgc_AuEn9A_gBDWLotXQEAAA==WKE (última consulta el 4 de mayo de 2023).

FERNÁNDEZ, C., "La autoridad británica de protección de datos sanciona a TikTok con 12,7 millones de libras por tratar indebidamente datos de menores", *La Ley digital (Ciberderecho)*. Obtenido de: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAEWQTU_DMAyGf81yROkHhx1yWdtDUTf2URCckNtabURIqjgp7N_jrRIc_Eq2Xz-yHaAjlWcC-hDBlK5XaX5L9IItdLeO8wP63VVJEVwAc0ZSSZYngib3fYBFjxC0szvwqvURhR72zemCRu3RxqPXttczmCT9SCT3BnWopJRpss228lEs6ImH1ase0QYUkx6nhiOsLCDSVEIAVT4X7fux2qR52W6yrnpjeXphOVSCEHw_HWFE1WgKwBtGE2Bw1NbFA9D8I4z95NMud-OK7g0njMYCDNrhb3tqINp-OkX017Vk_gv1oJoTQwXMs7meneFf3D2zI-bHLz6itgV4F4k_IH8BxastRl0BAAA=WKE (última consulta el 4 de mayo de 2023).

FERNÁNDEZ, C., "EEUU acuerda con las grandes tecnológicas realizar una evaluación pública de los sistemas de IA generativa", *Diario La Ley (Ciberderecho).* Obtenido de: https://diariolaley.laleynext.es/Content/Inicio.aspx (última consulta el 11 de mayo de 2023).

FUNDACIÓN PFIZER. La Juventud y las redes sociales en Internet. Informe de resultados de la encuesta, septiembre 2009. Obtenido de https://www.fundacionpfizer.org/sites/default/files/informe_final_encuesta_juventud_y_redes_sociales.pdf (última consulta 7 de septiembre de 2021).

IAB SPAIN. "Estudio de redes sociales 2020". Obtenido de: https://iabspain.es/sin-acceso/download-id/39688/ (última consulta 24 de marzo de 2021).

IAB SPAIN. "Estudio de redes sociales 2022". Obtenido de: https://iabspain.es/estudio/estudio-de-redes-sociales-2022/ (última consulta 4 de enero de 2023).

IEBS SCHOOL. "Las redes sociales más utilizadas: cifras y estadísticas", de 9 de diciembre de 2020. Obtenido de: https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/#:~:text=Lideran%20el%20ranking%20de%20redes,49%25%20a%20un%2054%25. (última consulta 5 de mayo de 2021).

DOMO. Informe "Data Never Sleeps 8.0". Obtenido de: https://www.domo.com/learn/data-never-sleeps-8 (última consulta el 26 de mayo de 2021).

LLANEZA, P., Sistema "Consent Commons" creado por Paloma Llaneza. Obtenido de: https://consentcommons.com/el-sistema/ (última consulta el 28 de septiembre de 2021)

Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, 2009. Obtenido de: http://www.iijusticia.org/Memo.htm (última consulta el 8 de marzo de 2022).

MARTÍNEZ-RODRIGO, E.; MARTÍNEZ-CABEZA JIMÉNEZ, J., "Desafíos de la Protección de Menores en la Sociedad digital. Internet, redes sociales y comunicación", *Tirantonline.com.* O btenido de: https://www-tirantonline-com.proxy-oceano.deusto.es/base/tol/doctrina/searches?token_id=6311d6f994c32d00132b7051 (última consulta el 2 de septiembre de 2022).

PÉREZ, M., "Amazon crea un método para enviar pedidos antes de que se compren basado en Big Data". Obtenido de: https://blogthinkbig.com/metodo-de-envios-anticipados-de-amazon (última consulta el 7 de febrero de 2022).

QUSTODIO. "Informe anual sobre Aplicaciones y menores: un año atrapados detrás de las pantallas", 2020. Obtenido de: https://qweb.cdn.prismic.io/qweb/10de139a-cb1c-488e-b0e9-f5becb01f32f_Informe+anual+de+Qustodio+2020+Informe+sobre+los+h%C3%A1bitos+digitales+de+los+menores_ES.pdf (última consulta el 4 de mayo de 2021).

REDING, V., *Privacy matters- Why the EU needs new personal data protection rules*. Obtenido de: file:///C:/Users/estelabrion/Downloads/Viviane_Reding_Vice-President_of_the_European_Commission__responsible_for_Justice__Fundamental_Rights_and_Citizenship_Privacy_matters___Why_the_EU_needs_new_personal_data_protection_rules_The_European_Data_Pr.pdf (última consulta el 27 de abril de 2023).

RISBERG, E., "Las cinco redes sociales más poderosas en ingresos publicitarios", *Semana*. Obtenido de: https://www.semana.com/empresas/articulo/cuales-son-las-redes-sociales-con-mas-ingresos-publicitarios/291323/ (última consulta 22 de junio de 2021).

ROSEN, J., "The web means the end of forgetting", *The New York Times*, d 21 de julio de 2010. Obtenido de: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (última consulta el 13 de abril de 2022).

ROSEN, J., "The right to Be Forgotten", *Stanford Law Review Online*, 2012, núm. 88, vol. 64. Obtenido de: https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/#:~:text=According%20to%20the%20regulation%2C%20when,states%20in%20their%20local%20laws. (última consulta el 13 de abril de 2022).

SAVE THE CHILDREN. "La primera carta de los derechos del niño". Obtenido de: https://www.savethechildren.es/sites/default/files/imce/docs/primera_carta_derechos_del_nino-.pdf (última consulta el 27 de noviembre de 2022).

UNICEF. "Los e-derechos de los niños y las niñas", 2004. Obtenido de: http://www.ciberderechos-infancia.net/e-derechos-unicef.html#:~:text=Dec%C3%A1logo%20UNICEF%3A%20Los%20e%2Dderechos,%2C%20lugar%20de%20residencia%2C%20etc.&text=Derecho%20a%20la%20libre%20expresi%C3%B3n%20y%20asociaci%C3%B3n. (última consulta 17 de septiembre de 2020).

IV.REFERENCIAS NORMATIVAS

1. Internacional

CONSEJO DE EUROPA. Convenio sobre la Protección de los derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950, hecho en Roma. Instrumento de adhesión de España de 24 de noviembre de 1977, Boletín Oficial del Estado, de 10 de octubre de 1979, núm. 243.

CONSEJO DE EUROPA. Carta Social Europea, de 18 de octubre de 1961, hecha en Turín. Instrumento de Ratificación de 29 de abril de 1980, Boletín Oficial del Estado, de 26 de junio de 1980, núm. 153.

CONSEJO DE EUROPA. Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, de 28 de enero de 1981, Instrumento de ratificación de España del 27 de enero de 1984, Boletín Oficial del Estado, de 15 de noviembre de 1985, núm. 274.

CONSEJO DE EUROPA. Protocolo Adicional al Convenio para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, de 8 de noviembre de 2001, hecho en Estrasburgo. Instrumento de ratificación de España de 24 de septiembre de 2009, Boletín Oficial del Estado, de 20 de septiembre de 2010, núm. 228.

SOCIEDAD DE NACIONES. Declaración de los derechos del niño de 1924. Obtenido en: https://www.ciprodeni.org/wp-content/uploads/2018/08/Declaracion-de-Ginebra-1924.pdf (última consulta el 4 de julio de 2022).

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966, Instrumento de adhesión de España, de 28 de septiembre de 1976, Boletín Oficial del Estado, 30 de abril de 1977, núm. 103.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. Convención sobre los Derechos del niño, de 20 de noviembre de 1989, Instrumento de ratificación de España, de 26 de enero de 1990, Boletín Oficial del Estado, 31 de diciembre de 1990, núm. 313.

OFICINA PERMANENTE DE LA CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO. Convenio sobre protección del niño y cooperación en materia de adopción internacional, de 29 de mayo de 1993, hecho en La Haya. Instrumento de ratificación de España, de 27 de marzo de 1995, Boletín Oficial del Estado, 1 de agosto de 1995, núm. 182.

2. Unión Europea

Tratado de Maastricht, de 7 de febrero de 1992, por el que se aprueba el Tratado de la Unión Europea, Diario Oficial de la Unión Europea, C/191, de 29 de julio de 1992.

Tratado de Ámsterdam, de 2 de octubre de 1997 por el que se modifican el Tratado de la Unión Europea y los Tratados Constitutivos de la Comunidad Europea y determinados anexos. Obtenido en: https://www.europarl.europa.eu/topics/treaty/pdf/amst-es.pdf (última consulta el 9 de marzo de 2022).

Carta de los Derechos Fundamentales de la Unión Europea, aprobada por el Parlamento Europeo el 7 de diciembre de 2000, Diario Oficial de las Comunidades Europeas, C/364, de 18 de diciembre de 2000.

Tratado de Lisboa, de 12 de diciembre de 2007 por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, Diario Oficial de la Unión Europea, C/306/1, de 13 de diciembre de 2007.

Tratado de Funcionamiento de la Unión Europea, Boletín Oficial de la Unión Europea, C/326, de 26 de octubre de 2012.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, aprobado el 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Diario Oficial de la Unión Europea, L 119/1, de 4 de mayo de 2016.

Reglamento (UE), 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo al mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE de servicios digitales, Diario Oficial de la Unión Europea, L 277/1, de 27 de octubre de 2022.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial de la Unión Europea, L 281, de 23 de noviembre de 1995.

Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, Diario Oficial de la Unión Europea, L 24/1, de 30 de enero de 1998.

Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), Diario Oficial de la Unión Europea, L 108/51, de 24 de abril de 2002.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), Diario Oficial de la Unión Europea, L 201, de 31 de julio de 2002.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, relativa al servicio universal que modificó varias directivas del sector de las telecomunicaciones, Diario Oficial de la Unión Europea, L 337, 18 de diciembre de 2009.

Decisión del Parlamento Europeo 1351/2008/CE, de 16 de diciembre de 2008, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación, Diario Oficial de la Unión Europea, de 24 de diciembre de 2008.

Recomendación 98/560/CE del Consejo, de 24 de septiembre de 1998, Diario Oficial de la Unión Europea, L 270, de 7 de octubre de 1998.

Recomendación (99) 5, de 23 de febrero de 1999, sobre la protección de la vida privada en Internet. Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información", adoptada por el Comité de Ministros el 23 de febrero de 1999 durante la 660ª reunión de Delegados de Ministros.

Recomendación del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, Diario Oficial de la Unión Europea, C 263/10, de 25 de julio de 2018.

Carta Europea de los Derechos del Niño, aprobada el 8 de julio de 1992, Boletín de las Comunidades Europeas, C 241, de 21 de septiembre de 1992.

Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012 (INL).

Propuestas de directiva de la Comisión: COM (90) 314-SYN 287 y 288, de 24 de septiembre de 1990 y COM (92) 422 final, DOC núm. 311, de 27 de noviembre de 1992.

Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 25 de enero de 2012, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), Comunicación (COM) 2012 11 final.

Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la unión, COM (2021) 206 final.

Enmiendas de los comités parlamentarios del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial) y modifica determinados actos legislativos de la Unión, de 9 de mayo de 2023. Obtenido de: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf (última consulta el 17 de mayo de 2023).

3. España

Constitución Española de 1978, Boletín Oficial del Estado, de 29 de diciembre de 1978, núm. 311.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, Boletín Oficial del Estado, de 14 de mayo de 1982, núm. 115.

Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, Boletín Oficial del Estado, de 27 de marzo de 1984, núm. 74.

Ley Orgánica 5/1988, de 9 de junio, sobre exhibicionismo y provocación sexual en relación con los menores, Boletín Oficial del Estado, de 11 de junio de 1988, núm. 140.

Ley Orgánica 4/1992, de 5 de junio, sobre reforma de la Ley reguladora de la competencia y el procedimiento de los Juzgados de Menores, Boletín Oficial del Estado, de 11 de junio de 1992, núm. 140.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, Boletín Oficial del Estado, de 31 de octubre de 1992, núm. 262.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Boletín Oficial del Estado, de 24 de noviembre de 1995, núm. 281.

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, Boletín Oficial del Estado, de 17 de enero de 1996, núm. 15.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Boletín Oficial del Estado, de 14 de diciembre de 1999, núm. 298.

Ley Orgánica 8/2015, de 22 de julio, de modificación del sistema a la infancia y a la adolescencia, Boletín Oficial del Estado, de 23 de julio de 2015, núm. 175.

Ley Orgánica 26/2015, de 28 de julio, de modificación del sistema a la infancia y a la adolescencia, Boletín Oficial del Estado, de 29 de julio de 2015, núm. 180.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Boletín Oficial del Estado, de 6 de diciembre de 2018, núm. 294.

Ley 230/1963, de 28 de diciembre, General Tributaria, Boletín Oficial del Estado, de 28 de diciembre de 1963, núm. 313.

Ley 11/1981, de 13 de mayo, de modificación de la Filiación, Patria Potestad y Régimen Económico del Matrimonio, Boletín Oficial del Estado, de 19 de mayo de 1981, núm. 119.

Ley 13/1983, de 24 de octubre, de Reforma del código civil en materia de tutela, Boletín Oficial del Estado, de 26 de octubre de 1983, núm. 256.

Ley 30/1984, de 2 de agosto, de Medidas de Reforma de la Función Pública (LOREG), Boletín Oficial del Estado, de 3 de agosto de 1984, núm. 185.

Ley 10/1985, de 26 de abril, por la que se modifica la Ley General Tributaria, Boletín Oficial del Estado, de 27 de abril de 1985, núm. 101.

Ley 21/1987, de 11 de noviembre, por la que se modifican determinados artículos del Código Civil y de la Ley de Enjuiciamiento Civil en materia de adopción, Boletín Oficial del estado, de 17 de noviembre de 1987, núm. 275.

Ley 33/1987, de 23 de diciembre, por la que se modifica la Ley General Tributaria, Boletín Oficial del Estado, de 24 de diciembre de 1987, núm. 307.

Ley 23/1988, de 28 de julio, de Medidas de Reforma de la Función Pública (LOREG), Boletín Oficial del Estado, de 29 de julio de 1988, núm. 181.

Ley 4/1990, de 29 de junio, por la que se modifica la Ley General Tributaria, Boletín Oficial del Estado, de 30 de junio de 1990, núm. 256.

Ley 31/1991, de 30 de noviembre, por la que se modifica la Ley General Tributaria, Boletín Oficial del Estado, de 31 de diciembre de 1991, núm. 313.

Ley 1/2000, de 7 de enero de 2000, de Enjuiciamiento Civil, Boletín Oficial del Estado, de 8 de enero de 2020, núm. 7.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Boletín Oficial del Estado, de 12 de julio de 2002, núm. 166.

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica, Boletín Oficial del Estado, de 15 de noviembre de 2002, núm. 274.

Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, Boletín Oficial del Estado, de 3 de junio de 2012, núm. 132.

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, de 19 de enero de 2008, núm. 17.

Real Decreto-Ley 13/2012, de 30 de marzo por el que se transponen las directivas en materia de electricidad y gas y en materia de comunicaciones electrónicas y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctricos y gasista, Boletín Oficial del Estado, de 31 de marzo de 2012, núm. 78.

ENMIENDA NUM. 716. CONGRESO DE LOS DIPUTADOS, Diario Oficial de sesiones de las Cortes Generales, núm. 70, de 19 de mayo de 1978.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, II Legislatura, Serie D, núm. 47, de 20 de septiembre de 1984.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie D, núm. 20, de 4 de diciembre de 1986.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie B, núm. 68-1, de 27 de abril de 1987.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, III Legislatura, Serie B, núm. 120-1, de 23 de junio de 1988.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, IV Legislatura, Serie A, núm. 59-1, de 24 de julio de 1990.

CONGRESO DE LOS DIPUTADOS, Diario de Sesiones del Congreso de los Diputados, Pleno y Diputación Permanente, Sesión Plenaria, núm. 170, de 28 de septiembre de 1995.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, XII Legislatura, Serie A, núm. 13-1, de 24 de noviembre de 2017.

CONGRESO DE LOS DIPUTADOS, Boletín Oficial de las Cortes Generales, XII Legislatura, Serie A, 13-2, enmienda núm. 5, de 18 de abril de 2018.

Anteproyecto de Ley para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI, publicado en Boletín de las Cortes Generales, de 16 de septiembre de 2022, Serie A, núm. 113-1.

Orden PCM/1203/2022, de 5 de diciembre, por la que se publica el Acuerdo de del Consejo de Ministros, por el que se determina la sede física de la futura Agencia Española de Supervisión de Inteligencia Artificial, Boletín Oficial del Estado, de 6 de diciembre de 2022, núm. 292.

4. Otros Estados

Costituzione della Repubbdlica Italiana, Gazzetta Ufficiale, el 27 de diciembre de 1947, núm. 298.

Constituição da República Portuguesa, Texto originário da Constituição, aprovada em 2 de Abril de 1976. Obtenido de: https://www.parlamento.pt/parlamento/documents/crp1976.pdf (última consulta 7 de mayo de 2021).

Constitución de Finlandia, de 11 de junio de 1999, Boletín Oficial de Finlandia. Obtenido de: https://finlex.fi/sv/laki/ajantasa/1999/19990731 (última consulta el 16 de marzo de 2022).

Ley Fundamental de los Países Bajos, Constitución de 21 de diciembre de 2018, Boletín Oficial de Países Bajos. Obtenido de: https://wetten.overheid.nl/BWBR0001840/2018-12-21?VergelijkMet=BWBR0001840%3fg%3d2002-03-21%26v%3d0 (última consulta el 16 de marzo de 2022).

Loi núm. 78-17 de janvier 1978 relative à l' informatique, aux fichiers et aux libertés, *Journal Officiel de la Republique Française,* num. 227.

FEDERAL TRADE COMMISSION EEUU. Children's Online Privacy Protection Act of 1998 (COPPA), 15 USC 6501-6505 issued in November 1999 by the Federal Trade Commission (FTC) and became effective in April 2000. vid. Section 312.5, *Parental Consent.*

Local Law 2021/144, de 12 de noviembre de 2021, sobre las herramientas automatizadas en la toma de decisiones, por la que se modifica el Código Administrativo de la ciudad (*Administrative Code of the city of New York*). Obtenido de: https://www.dfs.ny.gov/system/files/documents/2022/04/NYC_Council_Automated_Employment_Decision_Tools.pdf (última consulta el 20 de enero de 2023).

California Senate Bill 568, Privacy, Internet, minors, Approved by Governor September 23. Obtenido de: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (última consulta el 21 de febrero de 2023).

Utah Bill HB 311, Social Media Usadge Amendments. Obtenido de: https://le.utah.gov/~2023/bills/hbillenr/HB0311.pdf (última consulta el 26 de abril de 2023).

V.REFERENCIAS JURISPRUDENCIALES

1. Unión Europea

Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 12 de noviembre de 1969, *Caso Stauder,* Asunto 29/69.

Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 17 de diciembre de 1970 *Internacionale Handelsgesellschaft,* Asunto 11/70.

Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 14 de mayo de 1974 *Nold,* Asunto 4/73.

Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, *Bodil Lindqvist,* Asunto C-101/01.

Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de julio de 2010, sobre traslado ilícito de menores, rec C-211/201.

Sentencia del Tribunal de Justicia de la Unión Europea, de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros,* Asuntos acumulados C-293/12 y C-594/12.

Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, *Google Spain, S.L. y Google Inc vs Agencia Española de Protección de Datos (AEPD) y Mario Costeja González,* Asunto C-131/12.

Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de octubre de 2015, *Weltimmo/NAIH,* Asunto C-230/14.

Sentencia del Tribunal de Justicia de la Unión Europea, de 28 de julio de 2016, *Verein für Konsumenteninformation/Amazon EU Sarl,* Asunto C-191/15.

Sentencia del Tribunal de Justicia de la Unión Europea, de 19 de octubre de 2016, *Patrick Breyer y Bundesrepublik Deutschland,* Asunto C-582/14.

Sentencia del Tribunal de Justicia de la Unión Europea, de 21 de diciembre de 2016, *Tele2 Sverige AB y Post-och telesty- relsen y Secretary of State for the Home Departament y otros,* Asuntos acumulados C-20315 y C-698/15.

Sentencia del Tribunal de Justicia de la Unión Europea, de 20 de diciembre de 2017, *Pedro Nowak vs. Comisionado de protección de datos,* Asunto C-434/16.

Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de junio de 2018, *Wirtschaftsakademie Schleswig-Holstein,* Asunto C-210/16.

Sentencia del Tribunal de Justicia de la Unión Europea, de 24 de septiembre de 2019, *Commission nationale de l'informatique et des libertés (CNIL) vs. Google, LLC,* Asunto C-136/17.

Sentencia del Tribunal de Justicia de la Unión Europea, de 29 de julio de 2019, *Fashion ID,* Asunto C-40/17.

Sentencia del Tribunal de Justicia de la Unión Europea, de 1 de octubre de 2019, *Planet49,* Asunto C-673/17.

Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de enero de 2022, *TQ/Staatssecretaris van Justitie en Veiligheid,* Asunto C-441/19.

Sentencia del Tribunal de Justicia de la Unión Europea, de 8 de diciembre de 2022, *TU Y RE vs. Google, LLc.,* Asunto C-460/20.

Sentencia del Tribunal de Justicia de la Unión Europea, de 12 de enero de 2023, *Österreichische Post,* Asunto C-154/21.

Sentencia del Tribunal Europeo de Derechos Humanos, de 22 de junio de 2004, sobre secuestro internacional de menores por sus propios padres, rec. 78028/2001.

Sentencia del Tribunal Europeo de Derechos Humanos, de 24 de febrero de 2009, sobre el respecto a la vida familiar con la prohibición de discriminación, rec. 29768/2005.

Sentencia del Tribunal Europeo de Derechos Humanos, de 28 de junio de 2018, *ML* y *WW vs. Alemania*, Caso 607/98/10 y 65599/10.

Sentencia del Tribunal Europeo de Derechos Humanos, de 6 de octubre de 2022, *Khural y Zeynalov vs. Azerbaiyán*, rec. 55069/11.

Petición de decisión prejudicial presentada por la Audiencia Nacional (España), de 9 de marzo de 2012- *Google Spain, S.L., Google, Inc. / Agencia de Protección de Datos (AEPD)* (Asunto C-131/12).

Conclusiones del Abogado General Niilo Jääskinen, del 25 de julio de 2013. Obtenido de: http://ep00.epimg.net/descargables/2013/06/25/56e4461f3e4296befe3a8f4a56465de4.pdf (última consulta el 14 de abril de 2022).

Conclusiones del Abogado General de la UE, Maciej Szpunar, de 6 de junio de 2019, Asunto C-18/18. Obtenido de: https://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2122873 (última consulta el 2 de junio de 2022).

2. España

Sentencia del Tribunal Constitucional 11/1981, de 8 de abril, Boletín Oficial del Estado, de 25 de abril de 1981, núm. 99, pp. 1 a 13.

Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, Boletín Oficial del Estado, de 18 de agosto de 1993, núm. 197, pp. 28 a 34.

Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo, Boletín Oficial del Estado, de 13 de junio de 1994, núm. 140, p. 46 a 51.

Sentencia del Tribunal Constitucional 11/1998, de 13 de enero, Boletín Oficial del Estado, de 12 de febrero de 1998, núm. 37, p. 48 a 53.

Sentencia del Tribunal Constitucional de 144/1999, de 22 de julio, Boletín Oficial del Estado, de 26 de agosto de 1999, núm. 204, pp. 35 a 47.

Sentencia del Tribunal Constitucional 141/2000, de 29 de mayo, Boletín Oficial del Estado, de 30 de junio de 2000, núm. 156, pp. 40 a 46.

Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre, Boletín Oficial del Estado, de 4 de enero de 2001, núm. 4, pp. 70 a 93.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, Boletín Oficial del Estado, de 4 de enero de 2001, núm. 4, pp. 104 a 118.

Sentencia del Tribunal Constitucional 54/2004, de 15 de abril, Boletín Oficial del Estado, de 18 de mayo de 2004, núm. 120, pp. 31-40.

Sentencia del Tribunal Constitucional 61/2004, de 19 de abril, Boletín Oficial del Estado, de 18 de mayo de 2004, núm. 120, pp. 92-97.

Sentencia 241/2012, de 17 de diciembre de 2012, Boletín Oficial del Estado, de 22 de enero de 2013, núm. 19, pp. 1-15.

Sentencia del Tribunal Constitucional 58/2018, de 4 de julio de 2018, Boletín Oficial del Estado, de 7 de julio de 2018, núm. 164, pp. 68409 a 68433.

Sentencia del Tribunal Constitucional 89/2022, de 29 de junio, Boletín Oficial del Estado, de 29 de julio de 2022, núm. 181, pp. 110173 a 110217.

Sentencia del Tribunal Constitucional, 105/2022, de 13 de septiembre de 2022, Boletín Oficial del Estado, de 21 de octubre de 2022, núm. 253, pp. 144496-144524.

Sentencia del Tribunal Supremo 241/2013, Sala 1ª de lo Civil, de 9 de mayo de 2013, (Ref. Aranzadi RJ 2013/3088).

Sentencia del Tribunal Supremo 835/2013, Sala 1ª de lo Civil, de 6 de febrero de 2014, (rec. 245/2012).

Sentencia del Tribunal Supremo 1229/2014, Sala 1ª de lo Civil, de 12 de febrero de 2014, (rec. 383/2012).

Sentencia del Tribunal Supremo 3896/2014, Sala 1ª de lo Civil, de 3 de octubre de 2014, (rec. 6153/2011).

Sentencia del Tribunal Supremo 545/2015, Sala 1ª de lo Civil, de 15 de octubre de 2015, (rec. 2772/2013).

Sentencia del Tribunal Supremo 864/2015, Sala 1ª de lo Civil, de 10 de diciembre de 2015, (rec. 6401/2015).

Sentencia del Tribunal Supremo 210/2016, Sala 1ª de lo Civil, de 5 de abril de 2016, (rec. 3269/2014).

Sentencia del Tribunal Supremo 4281/2016, Sala 1ª de lo Civil, de 28 de septiembre de 2016, (rec. 3682/2015).

Sentencia del Tribunal Supremo 426/2017, Sala 1ª de lo Civil, de 6 de julio de 2017, (rec. 3440/2015).

Sentencia del Tribunal Supremo 12/2019, Sala 3ª de lo Contencioso-Administrativo, de 11 de enero de 2019, (rec. 5579/2017).

Sentencia del Tribunal Supremo 277/2022, Sala 1ª de lo Civil, de 31 de marzo de 2022, (rec.1153/2022).

Sentencia de la Audiencia Nacional 4899/2010, de 29 de diciembre de 2014, (rec. 725/2010).

Sentencia de la Audiencia Provincial de Valencia 372/2019, de 27 de septiembre de 2019, (rec. 329/2019).

3. Otros Estados

Sentencia del Tribunal Federal Alemán, de 15 de diciembre de 1983, ref. 1 Bvr 209/83.

Corte Suprema de Wisconsin, de 13 de julio de 2016, *State of Wisconsin vs. Eric L. Loomis*, Caso COMPAS, núm. 2015AP157-CR.

Sentencia del Tribunal del distrito de La Haya, de 5 de febrero de 2020, *Rechtbank Den Haag*/ (*Sentencia SyRI*), C-09-550982-HA ZA 18-388.

VI. CONGRESOS

MARTINEZ MARTINEZ. R., en el III Congreso de buen gobierno y transparencia de la Comunitat Valenciana, celebrado los días 5 y 6 de septiembre de 2018, "La anonimización es imposible". Obtenido de: https://www.youtube.com/watch?v=EwwecCrJKfg&list=PLMqWVbmUv8Thcv7QFKfHfUYT8f1fogdkG&index=8 (última consulta el 1 de marzo de 2022).