Universitat Internacional de Catalunya
Facultat de Dret

Tesi doctoral

El big data. Implicaciones jurídicas para un cambio de paradigma: El derecho al olvido y el consentimiento.

Juan Antonio Gallo Sallent

Aquesta tesi doctoral està subjecta a la licencia Reconeixement-NoComercial-SenseObraDerivada 4.0 Internacional (CC BY-NC-ND 4.0)

Esta tesis doctoral está sujeta a la licencia Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional (CC BY-NC-ND 4.0)

This doctoral thesis is licensed under the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0)

TESIS DOCTORAL

EL BIG DATA. IMPLICACIONES JURÍDICAS PARA UN CAMBIO DE PARADIGMA: EL DERECHO AL OLVIDO Y EL CONSENTIMIENTO

DOCTORANDO : JUAN ANTONIO GALLO SALLENT

DIRECTORA DE TESIS: DRA. MONTSERRAT NEBRERA GONZÁLEZ

FEBRERO 2020

ABREVIATURAS

AAA Algorithmic Accountability Act

Art. Artículo/s.

Art 29 WP Article 29 Working Party.

CdE Consejo de Europa.

CEDH Convención Europea de Derechos Humanos.

COPPA Children's Online Privacy Protection Act of 1998.

CPPA Child Privacy Protection Act.

FTC Free Trade Commission.

OCDE Organización para la Cooperación del Desarrollo Económico.

Pág. Página/s.

RAE Real Academia Española.

RGPD Reglamento General de Protección de Datos

TEDF Tratado Europeo de Derechos Fundamentales

TEDH Tribunal Europeo de Derechos Humanos

TFUE Tratado de Funcionamiento de la Unión Europea.

TJUE Tribunal Superior de Justicia de la Unión Europea.

TS Tribunal Supremo

"No nos olvidemos de que las causas de las acciones humanas suelen ser inconmensurablemente más complejas y variadas que nuestras explicaciones posteriores sobre ellas."

Fiodor Dostoievski

A mi mujer. Siempre ahí

A mis tres hijos

A mis padres

A la Tata

AGRADECIMIENTOS

Ante todo, querría agradecer a mi directora de tesis, la Doctora Montserrat Nebrera González, todo el tiempo dedicado, sus consejos y su profundo conocimiento del Derecho y de las complejas interrelaciones legales. El ánimo, la pasión y los conocimientos que transmite hacen que todo sea mucho más fácil.

No quisiera olvidarme de María González Ordoñez, por dedicarme, de manera altruista, su muy escaso y valioso -en todos los términos- tiempo libre.

INTRODUCCIÓN

1. Elección del tema de la Tesis.

I

Este estudio tiene su origen en la Universitat Internacional de Catalunya, con una visión de Derecho Internacional Público, por lo que, a pesar de que tiene un aspecto técnico insoslayable al hablarse de tecnología, el manejo de conceptos y expresiones, objeto y conclusiones, pese a sus posibles errores o imprecisiones, es eminentemente de Derecho Público. El inicio de esta investigación partió de una "especial atracción" hacia los derechos individuales y en especial a la privacidad que se dan en las llamadas "nuevas tecnologías", en la que una pregunta de mi directora de tesis, la Doctora Montserrat Nebrera González, centró mi total interés: "Y la gente, ¿Es consciente de lo que ha consentido que se haga con sus datos?". En ese momento descubrí que los datos que vamos generando y lo que se publica de nosotros en Internet son dos temas íntimamente unidos ya que afectan a nuestra esfera más íntima, la personal, y que constituye un tema acotado, a pesar de que las fuentes a consultar no son asequibles y que la bibliografía no es excesivamente extensa ya se trata de un tema muy complejo y relativamente nuevo debido a que está en constante evolución. Es un tema que tiene grandes componentes técnicos que escapan al mundo jurídico.

II

Internet nos ha permitido hacer cosas que nunca hubiésemos imaginado.

Las compañías que operan en este ecosistema disponen de una ingente cantidad de datos que han ido recopilando sobre cada persona. Saben lo que se mira por Internet, lo que se ha comprado, los sitios donde has estado. Y los datos que aún no tienen, se los pueden comprar a otras compañías. Es incuestionable que las compañías saben cada vez más sobre nosotros.

Las compañías que utilizan internet para producir productos o servicios, prácticamente todas, operan en un mercado global. Pero la ley no lo es. Las leyes que regulan el uso de los datos no son globales.

Nos hemos transformado en una sociedad en donde, dada la manera en que interactuamos con nuestro entorno, toda nuestra actividad queda registrada en forma de datos. Es la sociedad del "dateo". Los datos no paran de acumularse, y la técnica actual permite "desanonimizarlos" creando perfiles personales. Existen vendedores de datos (data dealers) que comercian con los datos privados.

Nos encontramos, pues, con un problema de falta de privacidad derivada de que no somos conscientes de que hemos ido dejando esparcidos un reguero de datos. Esta falta de privacidad la mayoría de las veces no es consentida. Es más, es desconocida. Y lo perturbador es la falta de resistencia que despierta en las personas. Si bien es cierto que, en el plano teórico[1], los usuarios muestran preocupación por su seguridad, si nos movemos en el campo práctico vemos como la seguridad sobre nuestros datos no preocupa en absoluto, tal y como muestran los hábitos de uso crecientes de telefonía móvil, las compras en internet, las redes sociales, los buscadores, etc.

[1] https://www.politico.com/story/2014/01/poll-americans-privacy-security-102663 (último acceso 8 de febrero de 2018)

Toda, absolutamente toda, actividad conectiva que realicemos queda registrada, ofreciendo a terceros una realidad bastante acertada de lo que somos o hacemos. El Internet de las cosas (IOT) se encarga de proporcionar más información sobre nosotros; información de la que no somos conscientes. Información que se interrelaciona con la que nosotros mismos proporcionamos ayudando a expandir el conocimiento por terceros de nuestro perfil personal.

III

La obtención de datos cada vez es más "discreta" en su tarea; es menos perceptible por el ser humano gracias a las nuevas técnicas comerciales, de publicidad y de inteligencia artificial. Y cada vez existe mayor capacidad por parte de las empresas o gobiernos para extraer información "relevante" de esos datos: Información sobre salud, hábitos personales íntimos, contactos, comunicaciones, preferencias, política y un largo etcétera sin necesidad de que la persona de la cual se extraen determinadas conductas apruebe ningunos términos de servicio (TOS), que dicho sea de paso, son de compleja compresión incluso para expertos en la materia, redirigiendo a legislaciones extranjeras o permitiendo cambiarlos a la simple discrecionalidad de la empresa "obtenedora" sin notificación alguna.[2]. Algunas encuestas muestran que menos de un 10% de los usuarios de programas informáticos o aplicaciones móviles leen los TOS,[3]por lo que se crean problemas de consentimiento. Y eso sin tener en cuenta los datos que continuamente generan nuestras conexiones móviles.

[2] Ver Apple :https://www.apple.com/legal/internet-services/terms/site.html (última vista 7 de febrero de 2018) o Microsoft: https://tosdr.org/#microsoft (última visita 8 de febrero de 2018).
[3] https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems (última visita 9 de noviembre de 2018)

A todo esto, hay que sumarle la información personal sobre nosotros que podemos encontrar en Internet, mediante buscadores, y que escapa a nuestro control. Información que puede ser cierta o no, relevante o irrelevante, desactualizada o al día e incluso privada y no permitida o deseada por el usuario.

No olvidemos que los datos, entre los que se incluyen la información y opiniones personales, pertenecen a las personas que los generan y no a las empresas, servicios o gobiernos que los reciben.

La información recopilada en base de datos es el pecado original sobre el cual se desarrolla esta Tesis doctoral.

IV

Toda esta información sobre nosotros y que puede escapar de nuestra voluntad o conocimiento no es mala en si misma. Sin embargo, el problema radica en lo que se puede hacer con estos datos.

Los contenidos de publicidad es un buen ejemplo sobre esto ya que utilizan los datos que poseen sobre una determinada persona para tratar subrepticiamente de que tengamos una respuesta directa mediante el dirigirse personalmente a uno y "darle caza", o sobre los patrones de las páginas web que visitamos –que pueden revelar aspectos íntimos personalísimos- o nuestra geolocalización.

Estamos creando datos, sin saberlo, que las compañías venden y compran entre ellas con el fin de crear patrones de comportamiento sobre nosotros.

El tratamiento de los datos sirve para saber cómo pensamos, con quién nos reunimos, nuestros patrones de comportamiento, etc. O sirven para poder ser

espiados o controlados por gobiernos u organizaciones. Incluso Steve Irvine, entre otros, fundador y creador de LinkedIn, reconoce públicamente que se fijan en cada individuo para decidir que le van a enseñar[4].

En el fondo subyace la necesidad de crear un nuevo concepto sobre lo que conocemos como "libertad". Será difícil que esta libertad continúe existiendo como tal si muchas de nuestras opciones personales o grupales pasan a estar condicionadas por terceros.

V

Los datos personales necesitan protección legal que protejan a las personas que generen estos datos; que las personas tengan control sobre sus datos pudiendo hacer que desaparezcan, se cambien, se borren o se compartan de una única determinada manera. En definitiva, este control es el derecho a que los datos recolectados sean "olvidados" parcialmente por el ecosistema para finalidades diferentes a las deseadas y consentidas, u "olvidados" totalmente para finalidades ni deseadas ni consentidas, si así lo deseamos.

Pero no puede el lector de la Tesis doctoral observarlo de manera unidireccional. El control sobre los datos es algo también muy importante para las empresas. Muchas investigaciones científicas no se pueden llevar a cabo porque los agentes propietarios de esos datos, hospitales o centros de investigación no quieren compartir esa ingente masa de datos que poseen por los componentes legales que eso implica. Y estamos hablando de que, quizás, compartiendo esos millones de datos avanzaríamos a pasos de gigante en enfermedades hasta hoy incurables.

[4] Documental "Anuncios Hasta en la Sopa".

2. De lo que trata esta tesis y sus limitaciones.

I

Como hemos dicho anteriormente, el hecho de que toda actividad conectiva realizada proporcione datos personales no es en si mismo ni bueno ni malo. Tampoco representa mayor problema el hecho de que los datos se traten de manera que permitan una agregación con determinados fines. El problema radica en que la tecnología permite que esos datos emitidos puedan ser relacionados con una persona en concreto. Una vez se sabe a quién pertenecen, el siguiente paso es agregar esos datos con otros existentes para obtener determinados patrones o con alguna otra finalidad.

Estamos pues ante el tratamiento a gran escala de datos personales en un contexto virtual e internacional con, la mayoría de las veces, la falta de consentimiento explícito por parte del emisor de esos datos.

Game Station, para llamar la atención sobre este hecho, incluyó como condición: "*Al enviar una orden de compra por la web el primer día del cuarto mes del año 2010, Anno Domini, estás de acuerdo en concedernos la opción no transferible de reclamar, por ahora y para siempre, tu alma inmortal*." Más de 7500 personas aceptaron estos TOS.

"*Usted reconoce y acepta que no tiene ninguna expectativa de privacidad con respecto a la transmisión de cualquier contenido de usuario*", rezan los términos del servicio de Clash of Clans, un popular y divertido juego para el móvil.

El tratamiento de datos personales, así como su recolección previa no es un tema menor. El artículo 12 de la Declaración Internacional de Derechos Humanos expone que "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*"

Un aspecto importante que tiene que tener en cuenta el lector es que los comentarios, fotos, vídeos, etc que hemos hecho nosotros en Internet – u otras personas pero en los que se nos menciona o reconoce- , que están colgados en la red, y que aparecen en los buscadores, también son datos. No hay que olvidarse de este aspecto, ya que una de las partes del estudio atañe directamente a esto.

II

El tratamiento de datos a gran escala se conoce como "Big Data", aunque no existe definición legal al respecto ya que datos y tratamiento se conceptualizan como dos cosas diferentes. Y lo que también es importante: Las opiniones personales, gustos, preferencias y creencias íntimas también son tratadas como datos. Pasan de ser una categoría semántica a una categoría matemática, vaciándolos de contenido.

No existe ninguna definición legal de Big Data en los países u organismos que se consideran en la presente Tesis, pero no viene a ser más que el tratamiento agregado de todos los datos que existen sobre un recurso determinado. Es un concepto muy ligado al de metadatos sobre el cual sí que existen determinadas definiciones legales.

En España, el artículo 42 del Real Decreto 1671/200 , de 6 de noviembre, al desarrollar las disposiciones comunes sobre los documentos electrónicos, define 'metadato' como "*cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento".* Bien es cierto que los metadatos se asocian ya a cualquier tipo de archivo. No son más que grupos de datos que se incluyen en cualquier archivo y que sirven para describirlo y que proporcionan determinada información sobre ese archivo.

Una limitación importante de la tesis es el número de legislaciones estudiadas ya que no se pueden abordar todas. No obstante, se recogen las que se consideran más importantes y, por lo tanto, el resultado del estudio no se ve comprometido en modo alguno. Y mucho menos cuando de lo que se trata es de estudiar un aspecto que no puede ceñirse a legislaciones nacionales.

El estudio ha de quedar necesariamente ceñido a una serie de derechos que deben ser reconocidos a los titulares de esos datos, en que medida y frente a quién. Y todo ello en un mundo global y virtual. No se puede más que advertir al lector de que esta tesis va más allá de un estudio de Derecho comparado. Contiene elementos valorativos propios de lo que "debería ser" y aspectos relacionados con la técnica informática. Espero que el lector no se asuste por esto último. Todo lo que se tenga que explicar sobre aspectos técnicos se hará con una explicación simple y para profanos. Espero que el lector sepa valorar en su justa medida el esfuerzo añadido que ha supuesto este extremo.

Los derechos que se tratan en la presente investigación son el de protección de los datos, el consentimiento, la personalidad, el de cesión de datos, el de libertad de expresión y el derecho de no discriminación, ya que se consideran los derechos más relevantes inherentes a los datos, aunque existen otros derechos.

Hay que aclarar que más allá de cualquier condicionante local o social sobre las leyes de protección de datos o de determinados factores que contengan los diferentes sistemas jurídicos es posible extraer, a nuestro juicio, un análisis sistemático y coherente de la aplicación de esos derechos inherentes a los datos particulares que puedan ser asociados a una persona en concreto y que son recolectados de diversas maneras.

Una segunda aclaración conviene llevarla a cabo sobre la aproximación jurídica o el "hilo" que seguirá el estudio. Y tiene que ver con todo explicado anteriormente:

a) El Big Data – el tratamiento de datos- no sólo se refiere al tratamiento de datos que se puedan entender como algoritmos matemáticos derivados de una utilización de aparatos electrónicos como teléfonos móviles, sistemas de posicionamiento global, búsquedas en Internet, etc, sino que comprende también el tratamiento de aquella información derivada de nuestras expresiones u opiniones hechas en páginas webs, redes sociales, etc., así como fotos, videos, noticias o cualquier otro archivo que se pueda relacionar en concreto con una persona determinada, así como los datos que recolectan y transmiten el IOT –y en un futuro cercano el Internet de los Sentidos-.

b) Los datos personales, atribuibles a una persona concreta, son depositarios de una serie de derechos que hay que respetar.

c) Estos derechos no son iguales en todos los países, ni todos los países les atribuyen la misma importancia, aunque es cierto que existen ciertos principios inspiradores de estos derechos.

d) Nos enfrentamos a un problema complejo en dos sentidos. El tratamiento de datos se da en un entorno global sin fronteras y además existe un componente tecnológico muy alto desconocido por el legislador.

A modo de hilo conductor de la tesis, es necesario tener en cuenta que "la tecnología que estamos construyendo, sin ser por sí misma buena o mala en un sentido moral, puede ser usada para la opresión"[5]

III

Teniendo en cuenta este "cuadro de síntomas", nos ha parecido pertinente llevar a cabo este proyecto, el de las implicaciones legales del Big Data en un entorno internacional, como un estudio sistemático en el que se puedan reunir todas las vertientes mencionadas desde un punto de vista dogmático, político y práctico[6]. Y este estudio sistemático se aborda desde el punto en que estos derechos inherentes se ven violentados por una utilización no consentida, ilegal o porque los datos recopilados o tratados son falsos, irrelevantes o discriminatorios. En un mundo ideal, la tarea de este investigador no haría falta, pues si los datos se recolectasen, tratasen o se trasmitiesen de manera totalmente consentida y de acuerdo con la finalidad autorizada o de conformidad a la ley nacional del país en el cual han sido recolectados, no existiría ningún problema.

[5] LASSALLE, J.M "Ciberleviatán el colapso de la democracia liberal frente a la revolución digital" Editorial Marcial Pons.2019.
[6] SCHMIDT-ASSMANN, E, "La Teoría General del Derecho administrativo como sistema objeto y fundamentos de la construcción sistemàtica" INAP. (2013)

En este mundo ideal del cual hablamos, se deberían respetar los siguientes principios por parte de los entes recolectores de datos personales que puedan ser atribuidos a una persona en concreto:

En primer lugar, cumplir con las obligaciones legales que tienen como responsables cuando tratan datos de los usuarios ya sea a través de ellos mismos o a través de proveedores.

En segundo lugar, se debería solicitar consentimiento con carácter previo a la recogida, almacenaje y –quizás lo más importante- tratamiento de la información. El consentimiento debe ser libre, concreto e informado. Y debe ser específico para cada uno de los datos personales a los que se va a acceder y tratar, sobre todo para la localización, contactos, identidad del sujeto y del teléfono, datos biométricos, tarjeta de crédito y datos de pago, teléfonos y SMS –o sietemas de mensajes avanzados- y aplicaciones de conversación, historial de navegación, correo electrónico, redes sociales, opiniones y gustos, y consumo de bienes o servicios.

El consentimiento no legitima un excesivo y desmesurado tratamiento de los datos, sino que estos datos solo se pueden tratar para la finalidad para la cual han sido obtenidos.

Por ellos, en tercer lugar, se debe permitir de una forma inteligible y bien definida la finalidad para la que serán utilizados los datos con carácter previo a su recolección, y no modificar dichas finalidades sin que sea necesario prestar de nuevo el consentimiento, proporcionando información clara sobre si los datos serán utilizados por terceros.

En cuarto lugar, se debe permitir a los usuarios rescindir su consentimiento, así como la supresión de los datos recolectados ya que, los datos recolectados

pueden incluir aspectos íntimamente ligados a la personalidad y que son susceptibles de ser reconocidos como Derechos Fundamentales.

En quinto lugar, debería haber un único punto de contacto a donde poder dirigirse para ejercitar los derechos, facilitando una inteligible y fácilmente accesible política de privacidad, que advierta a los clientes al menos sobre: quiénes son, qué categorías de datos de carácter personal recogen y procesan, por qué deben realizar el procesamiento de datos y para qué se van a utilizar, en caso de que sean cedidos a terceros, una específica descripción acerca de a quién van a ser cedidos y los derechos de los usuarios, en lo referido a la revocación del consentimiento y la supresión de datos hayan sido estos tratados o no.

En sexto lugar, y tal como se expondrá a lo largo de la presente tesis, sería conveniente establecer un consentimiento específico sobre el tratamiento de cualesquiera datos recopilados sean estos de la naturaleza que sean.

Y todo ello para facilitar a los usuarios el ejercicio de sus derechos de acceso, rectificación, oposición y cancelación del tratamiento de datos y avisarles sobre de la existencia de estos mecanismos.

En séptimo lugar, se debería establecer un periodo razonable de conservación y expiración de los datos.

Y en octavo lugar y muy importante, en relación a los datos recolectados a través de menores de edad , como pueden ser en las aplicaciones móviles destinadas a ellos o juguetes que se conectan a Internet, se debería atender a los límites de minoría de edad fijados por las leyes nacionales, elegir el método más restrictivo para el procesamiento de datos, con total respeto a los principios de minimización de datos y restricción de la finalidad, no usar la

información con fines comerciales y abstenerse de conseguir información a través de los niños sobre las personas que se relacionan con ellos o sobre sus gustos o preferencias. En todo caso de deberán borrar de inmediato todos aquellos datos recopilados de menores de conformidad con su legislación nacional.

IV

Y dado este entorno virtual donde no existen fronteras, donde las legislaciones aplicables a las empresas son diferentes, donde los datos personales son objeto de comercio y donde los tribunales nacionales no tienen planta para obligar a empresas no radicadas en su país y donde el consentimiento que se ha dado para la recolección de los datos personales no es expreso, entiendo que no hay manera mejor de plantear el trabajo que desde la hipótesis de que los derechos de las personas en relación a sus datos personales no pueden ser ejercidos y defendidos en el ecosistema de internet más que desde lo que se conoce como Derecho al Olvido de estos datos.

Es decir, la hipótesis parte de que el derecho sobre los datos personales sólo se puede defender desde el Derecho al Olvido ya que, de otra manera es imposible a la vista de la cantidad de elementos del ecosistema que poseen los datos, muchas veces localizados en terceros países y algunos de ellos localizables en buscadores de Internet.

El Derecho al Olvido se intenta comprender desde una perspectiva que soslaya que el mundo "virtual" –online- no es igual al mundo real –offline-, y por lo tanto no se le pueden aplicar las mismas leyes.

Trataremos, igualmente, de intentar esclarecer si el Derecho al Olvido existe como tal y debe ser reconocido como un derecho fundamental inherente a las

personas y si puede ser equiparado al "derecho de protección de datos" en su sentido más amplio.

Por otro lado, veremos que existen diferentes aproximaciones legales al Derecho al Olvido en diferentes países. Intentaremos investigar cómo pueden "reconciliarse" dichas legislaciones.

En otro sesgo, hay que aceptar que es cierto que se necesita un punto de partida a partir de la legislación vigente. Pero el desarrollo tecnológico es tan rápido y discurre por unos caminos tan complicados que es imposible abordar el asunto desde la perspectiva de una única legislación nacional, pues el mundo "virtual" no entiende de fronteras.

3. De lo que no trata esta tesis.

Como se puede observar a lo largo de la tesis, ésta no pretende ahondar en determinados aspectos concretos que se conceptúan en las leyes que se citarán y que no afectan de manera directa a los temas expuestos.

Esta tesis no pretende ir más allá de unir unos conceptos que hasta ahora aparecen desperdigados por toda la legislación internacional, destacando los aspectos más relevantes de cada uno de ellos, su interacción, sus carencias conceptuales y los retos que se abordan en esta conceptuaización cosa que, sin duda, es necesaria para una correcta aproximación a los retos tecnológicos que vienen y a la realidad que ya impera.

Aunque a veces entran en juego principios de filosofía del Derecho o de Derecho natural, esta tesis no tiene como objetivo establecer ninguna guía

ética para la configuración de los temas tratados o de otros que se le aproximen como puede ser el campo de la robótica que interactúa con humanos.

Tampoco me centro en otros aspectos que pueden estar relacionados con el Big Data, el Derecho al Olvido o el consentimiento. De cada uno de estos temas se puede hacer una tesis doctoral. Mi objetivo no es otro que interrelacionarlos y tratar de demostrar las contradicciones que nos encontramos cuando estos conceptos se quieren tratar en el mundo on-line atendiendo a su conceptualización clásica. La tesis tiene como finalidad poner de manifiesto que estos conceptos tratados deberían evolucionar y qué variables deben preverse en su evolución a nivel mundial.

Esta tesis tampoco pretende ir más allá de la tecnología disponible hoy en día, pero esta claro que muchas de las cosas aquí expuestas serán aplicables a las tecnologías venideras, como puede ser el caso del Internet de los Sentidos. En todo caso, creemos que los problemas se agravarán por lo que el objeto y objetivos de la tesis se hacen aún, si cabe, más actuales y acuciantes.

4. Metodología y Estructura.

La metodología aplicada ha sido un análisis de la bibliografía existente sobre el tema, la mayoría en inglés ya que se trata de un tema muy novedoso.

En el Capítulo I, se establecen algunas cuestiones iniciales con tal de reflejar el debate central y el desarrollo actual de la tecnología ya que ésta es el factor primigenio de la presente tesis.

Es por ello que como metodología también se ha utilizado conversaciones con informáticos e ingenieros de telecomunicaciones para comprender el alcance de muchas cuestiones técnicas y del desarrollo de Internet, aunque sin hacer un análisis riguroso de estos apartados, que se van integrando en la tesis en la medida que son necesarios.

El Capítulo II, trata sobre el concepto de Big Data donde me centro en su falta de definición legal así como en la problemática que existe con los datos personales y en su relación con otros Derechos Fundamentales.

De igual manera, presento lo que he denominado las externalidades negativas del Big Data y cómo éstas pueden influir en el desarrollo del conjunto de la sociedad y en sus derechos.

En el capítulo III, se estudia el Derecho al Olvido y su aplicación al Big Data.

Se ha considerado pertinente establecer una clara diferenciación metodológica a efectos de estudio entre el Derecho al Olvido en Internet y el Derecho al Olvido en el Big Data, debido a las diferentes vertientes que presenta su estudio. Aunque con un claro propósito: Su convergencia.

Está claro de que se trata de un tema complejo que mezcla legislaciones internacionales y tecnología, y es por ello que se analiza diferente legislación internacional al respecto. Se ha estudiado en profundidad la normativa de Derecho Internacional referente a la protección de datos privados, así como la "soft law" emitida por diversos Organismos Internacionales. De igual manera, se realiza una comparativa entre las legislaciones de diversos países comparando los "conflictos" que se afrontan entre las diversas legislaciones.

El Capítulo IV es un estudio sobre el consentimiento en el mundo del Big Data y por lo tanto del Internet de las Cosas. Se hace especial referencia al consentimiento de los menores en Europa y en Estados Unidos.

CAPÍTULO I. INTERNET, LA TECNOLOGÍA MÓVIL E INTERNET DE LAS COSAS.

Comencemos con lo que hace que Internet sea especial y es que, posiblemente, es el invento más importante de los tiempos modernos.

Para el 57% de la población mundial conectada a internet en 2019, ha cambiado la forma en que se comunican, realizan transacciones, acceden a la educación y la información y, sin embargo, lo que es tan único y radical de esta tecnología es que está controlada por nadie, al menos en teoría.

En teoría, Internet se basa en la adhesión voluntaria a los protocolos técnicos y nada más.

Es una red de voluntarios que transmiten paquetes de información.

Los elementos clave de internet permanecen en manos del gobierno de los Estados Unidos como, por ejemplo, el sistema de nombres de dominio a través de su dominio sobre los cuerpos clave de Internet, ICANN, la Corporación de Internet para Nombres y Números Asignados, la agencia que asigna los nombres de dominio y controla la aprobación de nuevos dominios -la ICANN es una entidad incorporada sin fines de lucro según las leyes de California-; y IANA, Autoridad de Números Asignados de Internet, el cuerpo que asigna las direcciones IP y administra los datos que se mantienen en los servidores raíz en el corazón del sistema, lo que nos permite encontrarnos en Internet.

Este fue un compromiso alcanzado en 1998 cuando la naturaleza de la asignación de nombres de dominio centrada en los estados convirtió en el centro de la disputa entre Europa y los Estados Unidos en ese momento.

Otros países controlan las conexiones de red dentro y fuera de su jurisdicción para monitorear y restringir el contenido.

Internet evolucionó como una colaboración abierta en forma de plataforma, a pesar del hecho de que gran parte del trabajo inicial se realizó con fondos del Departamento de Defensa de los Estados Unidos.

La comunicación por Internet se realizó para operar en modo descentralizado, a diferencia del modelo tradicional de telefonía de hub y radio.

Esto significaba que, si alguna parte de la red estaba inactiva, el tráfico podría redireccionarse a través de otra ruta.

Este modelo, por supuesto, ha significado que hay una ausencia de control centralizado, o un punto de estrangulamiento, lo que hace que Internet sea difícil, aunque no imposible, de controlar desde un punto central.

El control sobre la columna vertebral significa el control sobre el acceso.

La belleza de este diseño significa que la red es esencialmente tonta, lo que significa que la inteligencia y las aplicaciones se basan en el punto final, lo que ha creado la innovación y apertura de Internet y lo distingue de las redes propietarias y cerradas.

1. El origen: Internet.

A fines de la década de 1960, la Agencia de Proyectos de Investigación Avanzada de los Estados Unidos financió la investigación de una red de computadoras experimental diseñada para facilitar la comunicación entre sitios remotos, incluso en el caso de que partes de la línea fueran destruidas en un ataque nuclear.

Esto significaba que el sistema no era el típico hub modelo de telecomunicaciones de radio, donde todos los mensajes se enroutaban a través de una central de intercambio, reencaminando los mensajes a través de una serie de enlaces impredecibles.

Aunque indirecto, el sistema fue eficaz y es de esperar, robusto. Esta red, originalmente conocida como ARPANET, se configuró para permitir la comunicación entre diferentes tipos de computadoras; en esta etapa, todos los grandes mainframes de los campus universitarios o bases militares se conectaron para permitir que se agreguen o eliminen nuevos módulos y que continúen funcionando en el evento en el que cualquier parte de la línea fuese dañada, destruida o capturada.

Durante la década de 1970, el gobierno de los Estados Unidos, en gran parte a través de fondos militares, alentó la expansión de los usuarios académicos en Internet para probar sus capacidades y expandir sus usos.

Fue utilizado como un foro para el intercambio de ideas, opiniones e información, y en particular para permitir la colaboración de los usuarios en ubicaciones remotas.

Con el tiempo, la red militar se separó de internet en general.

A principios de la década de 1990, había un creciente interés en las aplicaciones comerciales de Internet, y los usuarios comerciales eran admitidos como usuarios de pago de las líneas troncales por la Fundación Nacional de Ciencia Americana; el uso comercial de Internet estuvo prohibido hasta 1991.

Internet era anárquica, no estructurada y utilizada en gran medida por entusiastas sin necesidad de directrices, reglas o regulaciones.

El uso privado de Internet fue ofrecido por proveedores comerciales en un modelo de jardín amurallado. Los proveedores de servicios de Internet, como CompuServe, solo conectaron suscriptores mutuos y proporcionaron contenido administrado por CompuServe, excluyendo el acceso al contenido ofrecido por otros proveedores de servicios.

Tres eventos que alteraron drásticamente la naturaleza de Internet ocurrieron en 1991 y 1992.

Primero, el Protocolo de la World Wide Web fue desarrollado y publicado públicamente por Tim Berners-Lee del CERN.

En segundo lugar, se desarrolló el navegador Mosaic, más tarde llamado Netscape Navigator, que facilita la búsqueda en la web.

Y tercero, el Congreso de los Estados Unidos aprobó un proyecto de ley que permite la actividad comercial en Internet.

El desarrollo de la web efectivamente destruyó el modelo de jardín amurallado, aunque ahora, paradójicamente, estén surgiendo nuevos modelos de jardines amurallados.

A partir de este momento, la política del gobierno de los EE. UU y la de muchos gobiernos de todo el mundo, fue permitir al sector privado impulsar el desarrollo de tecnología relacionada con Internet.

1.2 ¿Cómo funciona internet?

Cuando la mayoría de las personas piensan en usar un servicio en línea, tienden a generalizarlo como navegar o navegar por la World Wide Web.

Si bien gran parte del contenido que consumimos se encuentra en las páginas web a las que accedemos a través de navegadores web, la World Wide Web es solo un servicio disponible en Internet.

Internet, como su nombre indica, es una serie de redes informáticas interconectadas que transportan una gran cantidad de información para una serie de servicios de red, como correo electrónico, internet, teléfono, audio, video, juegos, transferencias de archivos y, en particular, la Red mundial.

La web es una colección de documentos interconectados, o páginas web, y otros recursos web vinculados por hipervínculos y URL.

El Protocolo de transferencia de hipertexto, o HTTP, es el idioma utilizado en la web para la transferencia de información, sin embargo, es solo uno de los muchos idiomas o protocolos que se pueden usar para la comunicación en Internet.

Los protocolos pueden describirse como idiomas, o alternativamente, conjuntos de reglas para computadoras. Si dos computadoras obedecen estas reglas, podrán entenderse y comunicarse.

Los dos protocolos principales mediante los cuales se efectúa la comunicación entre computadoras en Internet son el Protocolo de Internet, IP y el Protocolo de Control de Transmisión, TCP. Otros protocolos o idiomas comunes incluyen SMTP (correo electrónico), FTP (transferencia de archivos), VOIP (voz) y BitTorrent (intercambio de archivos de igual a igual), o los protocolos IP (IPv4, IPv6), POP 3, ICMP, IGMP, o Appletalk entre otros.

Los datos que se envían a través del protocolo de Internet se empaquetan, es decir, se dividen en pequeños paquetes y luego se envían por medio de la IP.

Cada paquete contiene un encabezado, similar a un sobre, que contiene información que identifica la dirección o ubicación desde la cual se envía el paquete y hacia donde vas.

El paquete en sí contiene los datos, que son similares a la letra dentro de un sobre.
El Protocolo de Internet comunica información entre las computadoras mediante la asignación de direcciones IP a las computadoras que envían y reciben, y luego envían los paquetes de datos de una dirección a otra.

En la mayoría de las situaciones, los paquetes de datos no se envían directamente de una ubicación a otra. En gran parte porque cada ordenador en Internet no está conectada directamente a todas los otros ordenadores vía Internet.

Más bien, cada computadora está vinculada a otras computadoras, que a su vez se conectan a otras computadoras y así sucesivamente.

1.3 Internet y su repercusión en la vida.

Este intercambio fundamental de información ha permitido e incrementado las interacciones humanas a través de la disponibilidad de mensajería instantánea, los foros de Internet, las redes sociales, los videojuegos, etc.

Las compras en línea se han disparado como resultado de la conveniencia y la capacidad de realizar transacciones financieras en línea, y la tecnología móvil continúa avanzando a un ritmo asombroso.

Internet se ha convertido en una parte tan importante de nuestras vidas que, como resultado, tendemos a esperar que nuestros artículos cotidianos sean más inteligentes. Si bien esto ofrece mayor comodidad, a menudo no consideramos que todos los productos inteligentes sean parte de Internet.

Esto ha dado lugar al Internet de las cosas, que se extiende a cualquier cosa que pueda comunicar o recibir información.

Los dispositivos que utilizamos todos los días, como nuestros teléfonos inteligentes, automóviles que envían datos a sus fabricantes, dispositivos de seguridad, televisores inteligentes, neveras, wearables e incluso dispositivos de monitoreo cardíaco implantados envían y reciben información constantemente.

Usada de la manera correcta, esta información puede revelar mucho sobre quiénes somos, qué hacemos, decimos, pensamos y sentimos, pero no somos los únicos que tenemos acceso a esta información.

2. La tecnología celular.

Hay más de 7 mil millones de dispositivos en uso en el mundo, hoy en día es aproximadamente uno para cada hombre, mujer y niño en la faz de la tierra.

Para cualquier tecnología dada que sea un éxito abrumador, se tiene que hacer realmente bien. Ahora, una de las cosas que ha sido parte del éxito es algo que se llama convergencia celular y es un aspecto importante de lo que es "tecnología móvil": Hay una gran cantidad de tecnología de comunicación en esta plataforma móvil: el teléfono celular que hace todo tipo de cosas ya no es solo para voz. De hecho, la mayoría de nosotros lo usamos para muchas otras cosas, además de la voz, desde el correo electrónico hasta las diferentes aplicaciones, el escaneo de documentos, citas con el médico y todo tipo de cosas. Básicamente, es una plataforma única.

2.1. La tecnología celular y la transmisión de datos: Los teléfonos móviles.

La transmisión de datos a través de teléfonos móviles ya supera de lejos al tráfico de voz. Pero ahora podemos decir incluso más que eso porque con el advenimiento del 4g en adelante, la voz son simplemente paquetes de datos. La voz en realidad se maneja a través de paquetes IP, por lo que la voz y los datos son prácticamente lo mismo en lo que respecta a un teléfono móvil. Esa es realmente una de las mayores transiciones con respecto a 4G y sobre todo lo que la tecnología traiga por delante como el 5G que ya está operativo en la mayoría de países o la 6g que ya está en pruebas de implantación –se espera

que esté implantada y operativa en 2030- y que transmite información bajo el agua o permite descargas de 1 terabyte por segundo.

Los teléfonos móviles son "celulares" porque el área de cobertura de una red celular se divide en pequeñas regiones llamadas células. Los teléfonos transmiten a niveles de potencia relativamente bajos, lo que permite la reutilización de los canales de radio en teléfonos que están lo suficientemente alejados. La misma pequeña porción de espectro (o código de expansión o intervalo de tiempo, dependiendo de la tecnología específica) puede por lo tanto estar en uso para varias llamadas simultáneas diferentes. Esto es importante, ya que la cantidad de espectro inalámbrico disponible para cualquier tecnología dada es limitada. Cuanto más eficientes seamos en el uso del espectro, mayor será la población que puede ser apoyada por la tecnología en un área determinada. También hay economías de escala; cuanto mayor es la población de usuarios, mayor es el incentivo para la innovación, más baratos son los teléfonos, etc.

2.2. La evolución de los teléfonos móviles.

Los primeros teléfonos móviles eran grandes, pesados, caros y útiles solo para conversaciones de voz cortas. Sin embargo, con el tiempo, el teléfono celular evolucionó, se hizo más pequeño y adquirió una funcionalidad adicional. En 1992, se introdujeron los primeros teléfonos celulares digitales, que brindan comunicación de voz digital junto con un nuevo servicio llamado "mensajes de texto". A principios de siglo comenzamos a ver "teléfonos inteligentes", teléfonos (o plataformas celulares con mayor precisión) que

brindaban acceso rudimentario a Internet. A medida que aumentaban las velocidades de datos y el poder computacional, más funciones se abrían paso en la plataforma celular. A medida que avanzamos en las generaciones de celulares, los teléfonos móviles inteligentes son compatibles con los mensajes de texto, la navegación web, las compras minoristas, el correo electrónico, los servicios de ubicación, la banca, el control de servicios públicos, los juegos e incluso las llamadas de voz ocasionales. Esto es lo que se denomina convergencia celular: la consolidación de todas las formas de comunicación electrónica en una única plataforma celular.

A los efectos que interesan, y tal como se ha dicho, la tecnología celular es una tecnología emisora de datos; muchos de ellos privados y personales., Por ejemplo, la tecnología celular transmite la ubicación del dispositivo varias veces por minuto y el sistema puede rastrear dónde se encuentra para dirigir las llamadas a la persona, pero también para crear un registro de dónde ha estado o con quién, por ejemplo, y eso es una preocupación legal

2.3. Las aplicaciones móviles.

La Real Academia de la Lengua[7] señala que una aplicación es un programa preparado para una utilización específica, como el pago de nóminas, el tratamiento de textos, etc.

La enciclopedia Wikipedia[8] señala que una aplicación móvil, apli o app (en inglés) es una aplicación informática diseñada para ser ejecutada en teléfonos

[7] Disponible en www.rae.es
[8] Disponible en www.wikipedia.com

inteligentes, tabletas y otros dispositivos móviles y que permite al usuario efectuar una tarea concreta de cualquier tipo (profesional, de ocio, educativas, de acceso a servicios, etc.), facilitando las gestiones o actividades a desarrollar.

2.3.1. El ecosistema de las aplicaciones web.

Pero el mundo de las Apps es muchísimo más amplio de lo que en un principio pueda parecer. Cada vez más se implantan aplicaciones específicamente creadas para empresas o colectivos determinados, como por ejemplo aquella creada para un restaurante permitiendo que el camarero anote los pedidos en un teléfono móvil, o la ya habitual creada específicamente para la coordinación de los asistentes a un congreso científico y que tendrá únicamente una duración de esos días, donde los asistentes podrán chequear las ponencias, alojamientos, medios de transporte, etc., o la aplicación disponible para los alumnos de una Universidad en la que pueden consultar desde los horarios de la biblioteca hasta sus calificaciones.

También se encuentran aquellas que, de modo genérico, en mayor o menor medida, y dirigida a un público indeterminado, conllevan una responsabilidad por los datos que manejan, como las que monitorizan datos médicos (sería el caso, por ejemplo, de seguimiento de los análisis de un diabético), las que permiten efectuar denuncias ante la Policía, reservar citas para una prueba clínica, o las que suponen medios de pago aplicando la tecnología NFC de los teléfonos móviles.

2.3.2. Funcionamiento de las aplicaciones web.

Tal y como expone el Informe de Acta.es [9]sobre los aspectos jurídicos de las aplicaciones móviles, técnicamente una App es un programa informático, pero no se trata de un software al uso, creado ex novo, sino que su creación, programación e implementación está en función de unas pocas plataformas que son quienes facilitan, por así decirlo, las "plantillas" que harán posible su uso por el poseedor de un teléfono móvil.

Desde un punto de vista técnico existen tres tipos de App: Las webs, las nativas y las híbridas.

Las aplicaciones web son unas meras adaptaciones de páginas webs para que éstas puedan ser vistas desde el dispositivo móvil, es decir que en su contenido hay una coincidencia entre lo que vemos en la pantalla de un ordenador de sobremesa o portátil y el que vemos desde el teléfono o tableta, por lo que la aplicación se ve directamente en el navegador, no desde el teléfono. Ello es una ventaja ya que no ocupan espacio en el teléfono ni tampoco tenemos que estar preocupándonos de las tan molestas actualizaciones que a veces no son compatibles con nuestro teléfono o tableta ya que aquí accedemos directamente a una web que se actualizará por su cuenta.

Pero para que esta web sea perceptible sin problemas en el dispositivo móvil su arquitectura ha de basarse en el llamado "Responsive web design", es decir la adaptación de la web para su visualización correcta en un dispositivo móvil.

[9] BARBERÁN, P.: "Aspectos jurídicos de las aplicaciones móviles (apps)". Disponible en www.acta.es. En esta interesante guía se explica, de manera muy clara y compressiva todos los aspectos técnicos, que se reproducen debido a su fàcil comprensión.

Las aplicaciones son bastante utilizadas, porque su desarrollo es relativamente fácil y barato, ya que sus lenguajes de programación son los conocidos HTML, JAVASCRIPT o CCS, pero en ocasiones pueden existir problemas cuando se intentan incluir determinados aspectos propios de los dispositivos móviles y no de los ordenadores personales, como por ejemplo la coordinación con sistemas de geolocalización, ya que el móvil viaja con nosotros de modo permanente, mientras que el PC permanece en nuestro domicilio o lugar de trabajo.

El segundo tipo de Apps son las nativas, que son aquellas desarrolladas específicamente para dispositivos móviles. Esta circunstancia proporciona desde el inicio grandes ventajas, ya que al actuar unidas al sistema operativo del aparato pueden aprovecharse de todos los recursos de este (GPS, Máquina de fotos, contactos…), por lo que son ideales para aquellas aplicaciones en las que el usuario tiene que interactuar más, como puede ser un juego, las que miden nuestra actividad física en el ámbito deportivo, incluso las de redes sociales o mensajería instantánea.

Como su plataforma de divulgación es un teléfono móvil o tablet y estos dispositivos utilizan un número muy escaso de sistemas operativos (básicamente iOS de Apple para ser descargadas por Apple Store y Android para ser descargadas por Google Play), las Apps han de ser desarrolladas con las plantillas que estos sistemas ponen a disposición de los desarrolladores.

Son aplicaciones móviles más caras y difíciles de desarrollar, puesto que el desarrollador ha de tener conocimientos de programación en el sistema operativo java (la principal), visual basic, o basic4android en el caso de Android, o de objetive-c, python o swift en el caso de ios, hasta el punto de

que generalmente existen desarrolladores que están especializados en uno u otro sistema exclusivamente.

Las aplicaciones híbridas[10] son aplicaciones móviles diseñadas en un lenguaje de programación web ya sea HTML5, CSS o JavaScript, junto con un framework que permite adaptar la vista web a cualquier vista de un dispositivo móvil. En otras palabras, no son más que una aplicación construida para ser utilizada o implementada en distintos sistemas operativos móviles, tales como, iOS, Android o Windows Phone, evitándonos la tarea de crear una aplicación para cada sistema operativo. De esta manera, una aplicación híbrida puede ser adaptada a múltiples plataformas móviles sin crear nuevos códigos, pero ajustándose a algunos cambios operacionales para cada uno de ellos.

Sin embargo, a pesar de que el desarrollo de aplicaciones híbridas y nativas requiere de una construcción totalmente distinta, la forma de utilizarlas es igual. Para ello, solo debes dirigirte hasta la tienda de aplicaciones de tu dispositivo móvil, buscar la App que quieres instalar y descargarla. Aunque ambas son iguales en su forma de usabilidad, el rendimiento de una aplicación híbrida comparada con una nativa es mucho menor, debido a que estas últimas aprovechan de forma más óptima los recursos de hardware del dispositivo, por ejemplo, la cámara, el GPS, los sensores en el interior del dispositivo, entre otros. Por el contrario, las aplicaciones híbridas también pueden utilizar estos recursos de hardware, pero no al mismo nivel en comparación con las nativas.

[10] Ver https://www.nextu.com/blog/aplicaciones-hibridas-que-son-y-como-usarlas/. Ultimo acceso, marzo de 2019.

3. El Internet de las Cosas (Internet of things-IOT).

I

"Like the first railroad tracks laid down during the Industrial Revolution, the framework for a wired and connected future suddenly existed. The inventors of the Internet – including Robert E. Kahn and Vint Cerf – envisioned a world where networks connected to other networks – thus creating an interconnected fabric of networked systems. They foresaw a world with smarter machines that would spawn remarkable capabilities and incredible transformation."[11]

IOT básicamente es el concepto, la conexión de cualquier objeto físico a Internet y a cada uno de los otros objetos.

En 2012, la Unión Internacional de Telecomunicaciones (UIT)[12] definió el Internet de las Cosas como "una infraestructura global para la Sociedad de la Información, que permite servicios avanzados interconectando cosas (físicas y virtuales) basadas en tecnologías de información y comunicación interoperables, existentes y en evolución,"

En pocas palabras, el concepto básico de Internet de las Cosas es conectar básicamente cualquier dispositivo con un interruptor de encendido y apagado a Internet (y/o entre sí). Esto incluye todo, desde teléfonos móviles, cafeteras, lavadoras, coches, lámparas, dispositivos portátiles y casi cualquier otra cosa que se pueda imaginar. Esto también se aplica a los componentes de las máquinas, por ejemplo, un motor a reacción de un avión o el taladro de una

[11] GREENGARD, S "Internet of things".MIT Press Essential Knowledge serie. Versión Kindle. (2015)

[12] https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

plataforma petrolera. La firma de analistas Gartner dice que para 2020 habrá más de 26 mil millones de dispositivos conectados. Eso son muchas conexiones (algunos incluso estiman que este número es mucho mayor, más de 100 mil millones). El IoT es una red gigante de "cosas" conectadas (que también incluye a las personas). La relación que se produce será entre personas-personas, personas-cosas y cosas-cosas[13].

II

La introducción de la Comunicación[14] de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: "la construcción de una economía de los datos europea" expone que "Además, a medida que la transformación impulsada por los datos penetra en la economía y la sociedad, cada vez son mayores los volúmenes de datos generados por máquinas o procesos basados en tecnologías emergentes como la internet de las cosas (IoT, por su sigla en inglés), las fábricas del futuro y los sistemas conectados autónomos. La propia conectividad modifica la forma en que se puede acceder a los datos: aumenta la medida en que datos a los que solía accederse mediante conexiones físicas resultan ya accesibles a distancia. La enorme diversidad de fuentes y tipos de datos, y las abundantes oportunidades para aplicar el conocimiento derivado de estos datos en variados ámbitos, incluida la elaboración de políticas públicas, están solo en sus comienzos. Para sacar partido de estas oportunidades, los actores públicos y privados en el mercado de los datos necesitan tener acceso a conjuntos de datos amplios y diversos. Las cuestiones del acceso y la transmisión en

[13]https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/. Último acceso en febrero de 2019.

[14] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0009

relación con los datos generados por estas máquinas o procesos desempeñan, por consiguiente, un papel básico en la creación de una economía de los datos y exigen una evaluación detenida".

3.1 El internet de las cosas en la práctica cotidiana.

El impacto del IoT ya es muy notable en la sociedad cotidiana y seguirá aumentando para dejar su huella en la vida cotidiana.

El Consejo Nacional de Inteligencia de EE. UU. previó ya en 2008 IOT como una de las seis Tecnologías Civiles Perturbadoras con gran impacto en los Estados Unidos hasta 2025[15].

Cisco pronostica que en 2020 habrá 50.000 mil millones de "cosas" conectadas.[16] Los campos donde se puede aplicar IoT son abundantes.

La tecnología IoT se puede ver, por ejemplo, en salud, agricultura, energía, logística y transporte. Esto se refiere a la inteligencia de los procesos industriales, por lo que la implementación de Internet de las cosas es un factor importante.

En desarrollo urbano, conocemos el término Smart City, donde el concepto de IoT podría jugar un papel importante en varios campos, como la energía, el tráfico y la seguridad.

[15] Disponible en https://fas.org/irp/nic/disruptive.pdf
[16] https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

En nuestra vida cotidiana, estamos rodeados de teléfonos inteligentes, ordenadores y televisores inteligentes entre otros muchos aparatos de este tipo.

Todos estos objetos están constantemente conectando e intercambiando información y tareas. En el futuro, casi todas las máquinas estarán conectadas. El impacto del concepto IoT es enorme y tendrá un lugar importante en las sociedades futuras. La interconexión de los objetos genera y utiliza enormes cantidades de datos. A todo esto le tenemos que añadir las tecnologías futuras y relacionadas con el IoT, como puede ser, por ejemplo, el Internet de los Sentidos.

3.2. La problemática asociada al Internet de las Cosas.

En un entorno basado en la web, los datos relacionados con el consumidor que reflejan comportamientos se compilan mediante interacciones en línea en un mundo digital. Los datos pueden ser de varios tipos, como texto, imagen, video, audio, clics, visitas a la página u otros tipos de información relacionada con las cookies. Estos datos tienden a ser creados, generados o ingresados por un consumidor.

En un entorno basado en IoT, los dispositivos monitorean y registran datos relacionados con el comportamiento del consumidor en los entornos naturales y no digitales en los que se comporta un consumidor. Un consumidor no tiene que participar activamente para que el dispositivo recopile datos. Por ejemplo, un reloj inteligente recoge los pasos y pulsaciones de una persona

sin que ésta tenga que hacer nada y sin que tal vez sea consciente de que lo haga.

4. Conclusiones.

- El Big Data y el Internet de las Cosas están ya aquí. Y no ha hecho más que comenzar. Sin embargo, no existe definción jurídica para el Big Data.

- Cada vez, más y más dispositivos están conectados entre si. A su vez, las personas cada vez dependemos más de la interconexión con las máquinas o dispositivos conectados a Internet.

- Cada día cedemos, aunque no lo sepamos, miles de datos personales que son almacenados por distintos dispositivos, aplicaciones o webs.

- La computación cuántica ya es un hecho. Google ya ha anunciado que lo ha conseguido; IBM, también. Eso implicará nueva tecnología de tratamiento de datos a unas velocidades impensables hoy en día.

- Sin duda, los adelantos tecnológicos traerán grandes ventajas a la humanidad. Sin embargo, se prevén también nuevos retos en relación a la privacidad y el control de la vida personal por parte tanto de Administraciones Públicas como de empresas privadas.

- Todas estas nuevas preocupaciones, unidas a las actuales, hacen necesaria la ordenación legal de la recogida, almacenamiento y tratamiento de datos y de su protección.

- El concepto de Estado Nación que regula sobre esta materia es sobrepasado por la tecnología del mundo conectado. En el mundo de internet no existen fronteras; y en un contexto donde la movilidad de las personas es cada vez mayor, no tiene mucho sentido tratar legalmente estos temas desde un punto de vista local (aunque sea de ámbito comunitario, por ejemplo).

- El uso del Big Data y del Internet de las Cosas plantea muchas preocupaciones éticas que debieran ser tenidas en cuenta a la hora de abordar legalmente el tema.

CAPÍTULO II. El BIG DATA: SU CONCEPTUALIZACIÓN. PROBLEMÁTICA GENERAL

Antes de hablar de Big Data, echemos un vistazo a algunos de los conceptos fundamentales sobre lo que realmente son los datos.

¿Qué son los datos? Son algo que se crea cuando se está usando un ordenador, un teléfono móvil, una aplicación móvil o se tiene un aparato conectado a la Red.

Puede estar sentado allí escribiendo un documento o trabajando en una hoja de cálculo y generando algunos datos de esa manera. Y, por supuesto, aunque esa es una forma muy común de generar datos, también existen otras formas en que se crean datos.

Tal vez después del final de un día de trabajo, uno vaya a casa y se relaje jugando algunos videojuegos en línea. Y de nuevo, se están generando datos cuando se hace eso.

Tal vez uno tiene un teléfono inteligente y lo usa para enviar correos electrónicos o comunicarse con sus amigos. Y otra vez hay datos asociados con esta actividad.

Y quizás incluso uno tenga algo como un reloj inteligente que se usa cuando se hace ejercicio. Y eso va a generar datos sobre su salud y sus estadísticas y su ejercicio.

Y por supuesto, no es solo una persona. Está toda la gente con la que se interactúa en las redes sociales; donde se comenta sobre sus publicaciones o se interactúa sobre sus publicaciones.

Y, de hecho, a medida que avanzamos en nuestra vida diaria, cada vez vemos más cosas como dispositivos inteligentes que aparecen en entornos de oficina y que tienen sensores inteligentes que generan información; o bien, los dispositivos inteligentes en el hogar que generan o recopilan datos.

Y, por supuesto, la propia casa puede tener sensores incorporados. Es posible que se tenga una casa inteligente o incluso un automóvil conectado a Internet que va generando algunos datos inteligentes.

Vemos como es posible hacer un análisis con todos esos datos y obtener información de ellos.

1. La definición del Big Data.

I

No existiendo definición jurídica, la definición más popular de Big Data es aquella formada por las tres uves[17]:

a) Volumen en referencia al tamaño y escalabilidad.
b) Velocidad referida a la generación de datos y su procesamiento. El flujo de datos es masivo y constante.
c) Variedad, que se refiriere a la enorme cantidad de datos y su tamaño. Datos que son recogidos de múltiples aplicaciones como teléfonos móviles y que afectan a diferentes aspectos de la vida del individuo

[17] LANEY DOUG, "3D Data Management: Controlling Data Volume, Velocity and Variety" (Metra Group Research Note. (2001).

Últimamente se han añadido dos uves más a la definición de Big Data: Una es la referida a la veracidad de datos. La otra es la V de valor

d) Veracidad de datos. Es uno de los grandes retos del Big Data ya que es posible que todos los datos que nos lleguen no sean todo lo ciertos o correctos que deban ser debido a múltiples factores. La veracidad de los datos debe ser comprobada para que estos datos puedan ser calificados como Big Data y puedan, por tanto, ser tratados.
e) Valor. Es uno de los aspectos más característicos del Big Data y es que, para que los datos tengan valor, tienen que poder ser tratados y analizados de manera correcta: Los datos tienen que poder generar valor.[18]

II

Es importante desarrollar el concepto de valor en referencia al Big Data.

El uso de técnicas de voz y el uso de indexadores hace que el almacenamiento de datos y su tratamiento sea cada vez más eficiente y fácil. Además, ya no hace falta viajar a una localización física para poder utilizarlos.

La clave del valor de los datos es que son datos personales y podemos sacar información derivada de estos datos.

El problema radica en que la información almacenada en forma de datos y su conexión con una persona individual hace que los datos almacenados puedan ser considerados como información personal, y esto es lo que les confiere

[18] IBM. "The Four V's of Big Data¨ (2014) .

valor[19]. Existen ya compañías cuyo modelo de negocio está relacionado con estos datos personales.

Se suele pasar por alto que los datos personales son todos aquellos que son generados por una persona, sea física o jurídica, en un entorno conectado a la red.

Así, son datos personales no solamente aquellos a los que les damos un uso o aceptamos transmitir en un servicio consentido, sino aquellos datos que se forman por las actividades realizadas por la persona y que ésta no tiene conciencia de que está generando datos como por ejemplo las fotos, los archivos de Excel, las localizaciones realizados por su teléfono móvil, etc.

Hay que tener en cuenta que los datos personales pueden ser tratados una y otra vez y de acuerdo con finalidades que no estaban previstas en un inicio, asegurando así un alto impacto económico. [20]

2. Tipos de datos personales.

I

A los efectos que ahora interesan, tenemos dos tipos de datos personales: Emitidos voluntariamente y los emitidos de manera no voluntaria.

A lo anterior podemos añadir otro tipo de datos que son los datos derivados. Entendemos por datos derivados todos aquellos datos que se extraen de la

[19]VIJFVINKEL, M.M. "Technology and the right to be forgotten". Radboud University. Julio (2016).

[20] European Union Agency For Network andI information Security(ENISA).Privacy by designi Big Data (2015)

combinación de los anteriores mediante diversas operaciones analíticas y que son totalmente desconocidos por el emisor de esos datos como, por ejemplo, las previsiones de comportamiento. Debemos añadir aquí los atributos que, aunque no son datos identificadores de un sujeto determinado, en asociación o presencia de un sujeto determinado, le identifican unívocamente.

Como indica el informe de la Casa Blanca de 2014 –big data privacy report may 1 2014 - "some of the most profound challenges revealed during this review concern how Big Data analytics may ... create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms'. Unless individuals are provided with appropriate information and control, they 'will be subject to decisions that they do not understand and have no control over"[21]

II

Aquí es donde radica uno de los problemas esenciales en relación con el Big Data: Muchos de los datos personales que son tratados no gozan de nuestro consentimiento, es más, la persona no sabe que está generando datos personales ni para qué o de que forma serán utilizados estos datos.

Por lo tanto, hay una falta de voluntariedad y aceptación en la transmisión de la posesión de estos datos que sin embargo son controlados por alguna organización.

En definitiva, hay una pérdida de control de los datos personales por parte del individuo. Esto puede traer muchísimas consecuencias y ya no solo estamos

[21] Article 29 Working Party Opinion 3/2013 on purpose limitation (2013)

hablando de la pérdida del control y del poder sobre los datos personales y sobre la privacidad.

3. Una aproximación a la definición legal de Big Data. Limitaciones.

I

El Big Data, como decíamos antes, no es un concepto jurídico. Por lo tanto, hay que tratarlo de manera técnica, aunque, como veremos, tiene grandes repercusiones jurídicas.

En sentido etimológico, Data viene del latín siendo en esta lengua el participio del verbo dō. Por lo tanto, Data, en español tiene el sentido de dado u ofrecido[22].

En los tiempos modernos, la asociación Gartner describió el Big Data como "high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization"[23].

El mundo académico más autorizado, por su parte, lo define como "*Big Data is shorthand for the combination of a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times. The process involves mining the data for patterns, distilling the patterns into*

[22] https://en.wiktionary.org/wiki/datus

[23] GARTNER M. B. Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data (Gartner 2011) . Disponible en https://www.gartner.com/en/newsroom. ¨Última visita 18 de diciembre de 2018. Anteriormente, en 2001, el mismo grupo, conocido como META, había dado una primera versión de esta definición.

predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a technique for converting data flows into a particular, highly data-intensive type of knowledge"[24].

II

No existiendo definición legal del concepto Big Data, se presenta ya una limitación a la presente Tesis.

En términos legales, como veremos, la definición de Big Data puede llevar a resultados injustos que conducen a la discriminación, o a la transformación del individuo o de la sociedad.

Tales desafíos normativos motivan una preocupación que se puede resumir en términos de trazabilidad, que va de la mano con cuestiones de la responsabilidad moral y los dilemas de la automatización, es decir, la aceptabilidad de reemplazar o aumentar la toma de decisiones humanas con algoritmos[25] o el hecho de excluir a ciertas personas de determinadas ventajas o de posibles desarrollos sociales.

[24] COHEN, J., What Privacy Is For, 106 Harv. L. Rev 1904, p.1920-21 (2013).

[25] PAGALLO, U Y DURANTE M, "The Pros and Cons of Legal Automation and its Governance" 7(2) European Journal of Risk Regulation 323-334. (2016).

4. El tratamiento de los datos como parte esencial del Big Data y su relación con Derechos Fundamentales. Especial estudio de la privacidad.

Los datos son cualquier tipo de información que se registra de alguna manera. Puede que se hayan recopilado de múltiples maneras y formas de forma que sean inteligibles tanto para los seres humanos como para los sistemas de tratamiento electrónico, o para alguno de ambos. Hay que tener en cuenta que no todos los datos son datos personales.

Sólo cuando estos datos se pueden asociar a una persona se puede considerar que son datos personales.

4.1 La definición de datos personales en la legislación europea.

A nivel europeo, el Reglamento General de protección de Datos (RGPD)[26] define los datos personales como " *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

[26] https://www.boe.es/doue/2016/119/L00001-00088.pdf

4.2 La definición de datos personales en la legislación de Estados Unidos.

A nivel de Estados Unidos [27], la Ley de la Comisión Federal de Comercio (15 USC §§41-58[28]) no regula categorías específicas de datos. En su lugar, prohíbe actos o prácticas desleales o engañosas que involucren prácticas que no protegen la información personal de los consumidores. Los Principios de Publicidad de Comportamiento de la Federal Trade Commission, que publican mediantes una suerte de órdenes como la de publicidad del año 2009 –ya no en vigor-, se aplican al seguimiento de las actividades de un consumidor en línea a lo largo del tiempo, incluidas las búsquedas del consumidor, las visitas a las páginas web y el contenido visualizado, para entregar publicidad dirigida a los intereses del consumidor individual y sobre los datos que se consideran sensibles como edad, raza, religión, etc.

La Ley de Modernización de Servicios Financieros (15 USC §§6801-6827) se aplica a la información personal no pública recopilada por una institución financiera que se proporciona, resulta de, o se obtiene de otra manera en relación con los consumidores y clientes que obtienen productos o servicios financieros principalmente para fines personales, familiares o domésticos de una entidad financiera.

Para los fines de la Ley de Modernización mencionada, un consumidor es una persona que ha obtenido un producto o servicio financiero, pero no tiene una relación continua con la institución financiera. Un cliente es un subconjunto de consumidores y se refiere a alguien con una relación continua

[27] ver https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1
[28] Disponible en su versión modificada en https://www.ftc.gov/es/enforcement/statutes/federal-trade-commission-act

con la institución. La información personal no pública que es objeto de esta ley se aplica a la información que no está disponible públicamente y que es capaz de identificar personalmente a un consumidor o cliente.

La Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) (42 USC §1301 et seq.) regula el historial clínico, que es información médica y de salud individualmente identificable que es mantenida o transmitida por una entidad cubierta o su socio comercial.

La Ley de Notificación de Infracción de Seguridad de California[29] regula la información personal, lo que significa el nombre o la inicial del apellido de una persona en combinación con uno o más de los siguientes elementos de datos, cuando el nombre o los elementos de datos no están encriptados:

- Número de seguro social.
- Número de licencia de conducir o número de tarjeta de identificación de California.
- Número de cuenta, número de tarjeta de crédito o débito, en combinación con cualquier código de seguridad, código de acceso o contraseña que permita el acceso a la cuenta financiera de un individuo.
- Información médica.
- Información del seguro de salud.

La información personal también incluye un nombre de usuario o dirección de correo electrónico, en combinación con una contraseña o pregunta y respuesta de seguridad que permitirían el acceso a una cuenta en línea. La

[29] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386

información personal no incluye información disponible públicamente que esté legalmente disponible para el público en general a partir de registros del gobierno federal, estatal o local.

La Ley de protección de la privacidad en línea de California[30] define la información de identificación personal como la información de identificación individual sobre un consumidor individual recopilada en línea por el operador de esa persona y mantenida por el operador en una forma accesible, que incluye cualquiera de los siguientes de manera no exhaustiva:

- Un nombre y apellido.
- Una casa u otra dirección física, incluido el nombre de la calle y el nombre de una ciudad o pueblo.
- Una dirección de correo electrónico.
- Un número de teléfono.
- Un número de seguro social.
- Cualquier otro identificador que permita el contacto físico o en línea de una persona específica.

La información sobre un usuario que el sitio web o el servicio en línea recopila se mantiene en forma de identificación personal en combinación con un identificador descrito anteriormente.

La conocida como FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) (Family Educational Rights and Protection Act) prohibe entre otras cosas mostrar a

[30] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

terceros – no a los padres- las notas de los alumnos u otra información sin su consentimiento.

5. Sobre los datos personales y la privacidad de los datos en general.

I

Cuando se trata de la protección de datos, la existencia de diferentes sistemas legales y culturas significa que hay diferentes términos utilizados para referirse a lo mismo o cosas relacionadas. Tomemos la protección de datos en sí, por ejemplo. En algunos lugares, se lo denomina "privacidad de datos". Así, el término protección de datos debería considerarse intercambiable con la privacidad de datos.

Si bien la información sobre las personas, o la información que puede llevar a la identificación de una persona, ha existido a lo largo de la historia humana, el concepto de datos personales solo se definió formalmente en la década de 1970 - el primero fue la ley del estado alemán de Hesse en 1970 y en 1973 la ley de Suecia. -A finales de la década de 1980, varios estados europeos (Francia, Alemania, los Países Bajos y el Reino Unido) también habían adoptado leyes sobre protección de datos con el advenimiento de las primeras tecnologías digitales. Y los elementos básicos de esta definición han permanecido más o menos consistentes hasta el día de hoy: Los datos personales son simplemente cualquier información que se relaciona con una persona identificada o identificable.

II

En términos generales, existen cuatro categorías de datos que se incluyen en esta definición de datos personales:

a) Información que identifica explícitamente a un individuo. Esto podría significar, por ejemplo, un nombre completo, una dirección de correo electrónico que contiene el nombre completo del usuario o los registros del rostro de una persona.

b) Información que no identifica explícitamente a un individuo por sí misma pero es exclusiva de un individuo y permite que se identifique, si se considera más información.

Puede ser un número de teléfono, una identificación nacional o un conjunto de huellas dactilares.

c) información que puede no ser exclusiva de una persona pero que solo la posee una pequeña cantidad de personas, como las fechas de nacimiento y las direcciones de IP, que podrían identificar a las personas si se combinan con otros datos.

d) Información que no identifica a una persona como tal pero que proporciona información sobre una persona o sus actividades. Esto podría incluir información relacionada con la salud de una persona o sus registros de empleo. O podrían ser datos de geolocalización, su historial de búsqueda, actividad de redes sociales o sus compras en línea.

5.1 El Tratamiento de datos en la legislación europea.

A nivel europeo, el RGPD[31] realiza una profusa descripción acerca del tratamiento de datos y las actividades, situaciones, o personas que están relacionadas con esta actividad.

De esta manera, el artículo 4 del RGPD nos aporta las siguientes definiciones:

"2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional,

[31] https://www.boe.es/doue/2016/119/L00001-00088.pdf

siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del

encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «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;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

5.2 El tratamiento de datos en la legislación de Estados Unidos.

A nivel de Estados Unidos, no hay una definición legal general sobre tratamiento de datos, sino que hay que acudir a las diferentes regulaciones sectoriales[32]. Algunas de las leyes federales de privacidad más prominentes incluyen, las siguientes:

- La Ley de la Comisión Federal de Comercio (15 USC §§41-58)[33] (Ley FTC) es una ley federal de protección al consumidor que prohíbe las prácticas desleales o engañosas y se ha aplicado a las políticas de privacidad y seguridad de datos fuera de línea y en línea. La Comisión Federal del Comercio (FTC) ha interpuesto numerosas acciones de ejecución contra empresas que no cumplen con las políticas de privacidad publicadas y por la divulgación no autorizada de datos personales. La FTC también es la principal aplicadora de la Ley de protección de la privacidad en línea de los niños (COPPA) (15 USC §§6501-6506), que se aplica a la recopilación de información en línea de los niños, y de los Principios de autorregulación para la publicidad conductual.

- La Ley de Modernización de Servicios Financieros (15 USC §§6801-6827) regula la recopilación, el uso y la divulgación de información financiera. Puede aplicarse ampliamente a instituciones financieras como bancos, firmas de valores y compañías de seguros, y a otras empresas que proporcionan productos y servicios financieros. Esta ley limita la divulgación de información personal no pública y, en algunos casos, exige que las

[32] ver https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1
[33] Ib. Supra

instituciones financieras notifiquen sus prácticas de privacidad y brinden a los interesados la oportunidad de que no compartan su información. Además, existen varias Reglas de privacidad promulgadas por las agencias bancarias nacionales y la Regla de salvaguardias, la Regla de eliminación y la Regla de banderas rojas emitidas por la FTC que se relacionan con la protección y disposición de datos financieros.

- La Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) (42 USC §1301 et seq.) Regula la información médica. Puede aplicarse ampliamente a los proveedores de atención médica, procesadores de datos, farmacias y otras entidades que entran en contacto con la información médica. Los Estándares para la Privacidad de la Información de Salud Individualmente Identificable (Regla de Privacidad de HIPAA) (45 CFR Partes 160 y 164) se aplican a la recopilación y el uso de información de salud protegida (PHI). Las Normas de seguridad para la protección de la información electrónica de salud protegida (Regla de seguridad de HIPAA) (45 CFR 160 y 164) proporcionan normas para proteger los datos médicos. Los Estándares para Transacciones Electrónicas (Regla de Transacciones HIPAA) (45 CFR 160 y 162) se aplican a la transmisión electrónica de datos médicos. Estas reglas de HIPAA se revisaron a principios de 2013 bajo la "Regla ómnibus" de HIPAA.

- La Regla Omnibus de HIPAA también revisó la Regla de Notificación de Infracción de Seguridad (45 CFR 164) que requiere que las entidades cubiertas envíen una notificación de violación de información médica protegida. Según la regla revisada, en términos generales, una entidad cubierta debe proporcionar un aviso de adquisición, acceso, uso o divulgación de la histroa clínica de una manera no permitida por la Regla de privacidad.

- Leyes de Igualdad de oportunidades, entre las que se incluyen Equal Credit Opportunity Act ("ECOA"); el Título VII of the Civil Rights Act of 1964; Americans with Disabilities Act; the Age Discrimination in Employment Act ("ADEA"); the Fair Housing Act ("FHA"); y la Genetic Information Nondiscrimination Act ("GINA") que prohiben discriminar a nadie en función de determinados parámetros como raza, sexo, edad, religión, etc y que ordena a las empresas que tomen precacuiones cuando analice con Big Data esos datos ya que pueden llevar a discriminar personas.

- La Ley de información crediticia equitativa (15 USC §1681) (y la Ley de transacciones de crédito justas y precisas (Pub. L. No. 108-159) que modificó la Ley de información crediticia equitativa) se aplica a las agencias de informes de consumidores, aquellos que utilizan los informes de consumidores y aquellos que proporcionan información de información al consumidor. Los informes de consumidores son cualquier comunicación emitida por una agencia de informes de consumidores que se relaciona con la solvencia crediticia, el historial de crédito, la capacidad crediticia, el carácter y la reputación general de un consumidor que se utiliza para evaluar la elegibilidad de un consumidor para obtener crédito o seguro.

- La Ley de control del abuso de pornografía no solicitada y comercialización (Ley CAN-SPAM) (15 USC §§7701-7713 y 18 USC §1037) y la Ley de protección al consumidor por teléfono (47 USC §227 y siguientes) regulan la recolección y uso de direcciones de correo electrónico y números de teléfono, respectivamente.

- La Ley de privacidad de las comunicaciones electrónicas (18 USC §2510) y la Ley de fraude y abuso de computadoras (18 USC §1030) regulan la

interceptación de las comunicaciones electrónicas y la manipulación de las computadoras, respectivamente. Una demanda colectiva presentada a fines de 2008 alegó que los proveedores de servicios de Internet (ISP) y una compañía de publicidad dirigida violaron estos estatutos al interceptar los datos enviados entre las computadoras de los individuos y los servidores de los ISP (lo que se conoce como inspección profunda de paquetes). Esta es la misma práctica realizada por varias compañías de telecomunicaciones del Reino Unido que dio lugar a una investigación de la Comisión Europea.

- En 2016, el Congreso promulgó la Ley de reparación judicial[34], que otorga a los ciudadanos de ciertas naciones aliadas (en particular, los estados miembros de la UE) el derecho a solicitar una reparación en los tribunales de los EE. UU por violaciones de privacidad cuando su información personal se comparte con las agencias policiales.

5.3 Cuestiones sobre el tratamiento de datos personales

I

En términos generales, el tratamiento de datos se refiere a la recopilación, el almacenamiento, el uso o la difusión de datos. Si bien las definiciones varían a lo largo de las legislaciones, los elementos descritos son comunes a las definiciones.

[34] ver https://www.sciencedirect.com/science/article/pii/S1405919316000196

La recopilación es simplemente obtener los datos. La recopilación de datos puede ser relativamente manual y simple; por ejemplo, hacer que una persona complete un formulario o una encuesta. Pero los datos también se pueden recopilar de forma completamente automática por los aparatos electrónicos, sin que el sujeto de los datos o un controlador de datos humanos específico lo sepan, por ejemplo, a través de un navegador web o una cámara de vigilancia.

En referencia al almacenamiento ha que decir que una vez recopilados, los datos personales deben guardarse en algún lugar. Esto podría estar en un archivador, en una base de datos o en una aplicación en la nube.

El uso de los datos cubre las diversas operaciones que podrían realizarse con los datos obtenidos. Por ejemplo, comparándolo con otras bases de datos, haciendo que los datos sean anónimos, convirtiéndolos en un formato de archivo diferente, u ordenándolos de otra manera.

La difusión se refiere a las formas en que los datos se comparten con otros. La difusión de datos puede significar exportar una base de datos de información a una hoja de cálculo o presentarla en un PowerPoint por ejemplo. O puede significar también que una compañía comparta la información recopilada sobre el comportamiento de los usuarios.

II

Es indudable que el tratamiento de los datos aporta grandes ventajas, pero también riesgos.

La protección de datos se ocupa específicamente del tratamiento de datos personales que puede suponer riesgos para la privacidad de las personas y,

por tanto, estos datos están protegidos por varios instrumentos legales a nivel nacional e internacional.

El procesamiento de datos no personales, porque no puede afectar el derecho a la privacidad, no está cubierto por los marcos de protección de datos, aunque puede regirse por otros marcos regulatorios.

El problema radica en que la ley desconoce que los datos no personales pueden convertirse en personales.

III

La rápida difusión de Internet, de las aplicaciones móviles y la que va a generar el Internet de las Cosas o de los Sentidos han creado nuevos desafíos en torno a la aplicación de la protección de datos. En particular, ha dificultado el ejercicio de los derechos de los usuarios. Esto se debe en primer lugar a la creciente complejidad de los flujos de datos ya que estamos todo el día conectados generando datos masivamente y el usuario no lo sabe, menoscabando el derecho a saber que datos está cediendo y conforme que legislación y los marcos de protección que operan en dichas legislaciones.

En segundo lugar, y consecuencia en parte de lo primero es la dificultad de consentir esa recopilación y tratamiento de los datos. Una de las razones del posible vicio del consentimiento, o la posible analogía legal en cada sistema jurídico es que la aceptación, si la hay, de los términos del servicio o del consentimiento, se hace en bloque. Es decir, los usuarios no tienen más remedio que aceptar el acuerdo si desean utilizar el servicio. En la práctica, entonces, esta situación otorga a los usuarios muy poco poder sobre el tratamiento de sus datos.

En tercer lugar el problema radica en el concepto dinámico que presenta el propio concepto de datos personales ya que datos que, en principio, no lo son, acaban entrando de lleno en esta categoría.

Con la creciente digitalización de todos los aspectos de la vida humana, es posible utilizar datos personales para crear una imagen mucho más detallada y compleja de las personas. Hoy en día, al igual que la información personal detallada se recopila de forma rutinaria por las administraciones, las tecnologías de consumo pueden revelar los movimientos exactos de una persona en un día determinado, lo que han comprado, su historial de búsqueda en línea y lo que "me gusta" en las redes sociales. Al mismo tiempo, los avances en las tecnologías digitales significan que estos diversos conjuntos de datos se pueden comparar y agregar cada vez más de manera significativa.

6. El tratamiento de los datos y su relación con los Derechos Humanos.

I

La cantidad cada vez mayor de datos que se procesan y el análisis más sofisticado de los datos, a parte de las ventajas, también significa riesgos para los derechos humanos que se relacionan con el procesamiento de datos.

En este contexto, la regulación de la protección de datos debiera tener como objetivo proteger los derechos humanos, incluido el derecho a la privacidad, al otorgar a las personas la capacidad de controlar el procesamiento de sus datos e imponer obligaciones a quienes los procesan. Obligaciones tanto de hacer como de no hacer.

En los últimos años han surgido varias soluciones propuestas con diferentes enfoques.

II

En Europa, el RGPD introduce una gama de medidas legales que se basan en la regulación de protección de datos existentes hasta ahora incluidos la ampliación de los derechos de los usuarios, el aumento de las obligaciones legales de los controladores de datos y la introducción de una definición ampliada de datos personales.

La protección de datos, se establece como un derecho fundamental. Así el considerando primero del reglamento establece que "*La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea*[35] *y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE)*[36] *establecen que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y continúa en el considerado cuarto estableciendo que "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del*

[35] http://www.europarl.europa.eu/charter/pdf/text_es.pdf
[36] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT

domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.".

Todos estos considerandos quedan plasmados, a mi entender de manera muy sucinta, en el artículo dos del RGPD que establece que "*El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. "*

Este enfoque propuesto por el RGPD viene derivado porque las medidas legalmente exigibles son necesarias para enfrentar los desafíos al derecho a la privacidad que plantea el tratamiento masivo de datos personales derivados del Big Data[37].

Sólo aplicando estas medidas, se considera que pueden proporcionar suficiente protección. Los considerandos de las RGPD argumentan que garantizar el derecho a la privacidad a través de una regulación más fuerte no disminuye los beneficios económicos y sociales del procesamiento de datos, e incluso podría mejorarlos, por ejemplo, al reducir el riesgo de violaciones de datos y daños a la reputación de las empresas. En definitiva, mejora el "mercado interior".

[37] De hecho, no hace más que seguir las conclusiones de la Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A Comprehensive Approach on Personal Data Protection in the European Union

III

Sin embargo, este enfoque ha atraído la oposición de algunos sectores, quienes sostienen que un enfoque en la regulación inclina la balanza demasiado en una dirección[38]. Algunos destacan las pérdidas económicas que, en restricciones más estrictas en el procesamiento de datos, por ejemplo, medidas para permitir que los usuarios minimicen o bloqueen el acceso a sus datos personales, pueden incurrir las empresas mientras se utilizan los servicios en línea. También señalan el aumento de los costos incurridos por el cumplimiento de tales obligaciones[39].

Otros se oponen a las propuestas para permitir que los usuarios soliciten la eliminación de datos personales, argumentando que esto podría socavar los derechos a la libertad de expresión y el acceso a la información[40].

Y algunos[41], especialmente en la comunidad de datos abiertos, temen que estas medidas podrían limitar el uso de datos para mejorar y fomentar la innovación en los servicios sociales y públicos.

Aquellos que prefieren mantener el status quo prefieren confiar en la "autorregulación" que, en este contexto, significa que los controladores de datos eligen voluntariamente implementar medidas para proteger los datos. Este enfoque se encuentra a menudo en países donde los regímenes de

[38]Por ejemplo, https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos-201805242219_noticia.html. Acceso febrero 2019

[39] Por ejemplo, http://www.expansion.com/juridico/opinion/2018/09/12/5b99424546163f7e888b45a0.html. Acceso marzo 2019

[40] Por ejemplo, https://retina.elpais.com/retina/2018/10/18/innovacion/1539869909_018530.html. Acceso febrero 2019

[41] Entre muchos otros ver, KELLER, D,"Iintermediaries and free expression under the gdpr, Standford University;comunicaciones de Center for Internet and Society at Stanford Law Schooll; Internet Society. (2015)

protección de datos son sectoriales, así como en países donde los actores del sector privado no están sujetos a la regulación de protección de datos[42].

IV

Interesante es el análisis que hace Latonero[43] sobre la influencia del Big Data en los Derehos Humanos.

Para Latonero, son varias las actividades que conforman el Big Data sobre las que se tiene que poner un especial cuidado:

a) El descubrimiento de fuentes de datos, la búsqueda y el rastreo son actividades que implican encontrar fuentes de datos que pueden contener información relevante para un propósito, dominio o población. Las fuentes de datos pueden estar disponibles públicamente; por ejemplo, tweets de Twitter, artículos en sitios de noticias en línea o imágenes compartidas libremente en las redes sociales[44]. Otras fuentes, como las publicaciones de Facebook, son casi públicas en el sentido de que contienen datos que pueden ser accesibles solo para miembros específicos de una comunidad en línea con las credenciales y permisos de inicio de sesión adecuados. Otras fuentes de datos, como los mensajes de correo electrónico de cuentas privadas, no se pueden buscar públicamente. Incluso la recopilación de datos que está disponible públicamente puede violar las expectativas de privacidad de los usuarios de

[42] Se puede encotrar la información enhttp://oiprodat.com/2015/11/25/no-uniformidad-legislativa-paises-con-legislacion-en-proteccion-de-datos-y-sin-legislacion-especifica/ . Último acceso enero 2019.

[43] LATONERO, M. (2018). Big Data Analytics and Human Rights. In M. Land & J. Aronson (Eds.), *New Technologies for Human Rights Law and Practice* (pp. 149-161). Cambridge: Cambridge University Press. doi:10.1017/9781316838952.007

[44] LATONERO, M cita a ARONSON, J "Mobile Phones, Social Media, and Big Data in Human Rights Fact-Finding: Possibilities, Challenges, and Limitations," in P. Alston and S. Knuckey (eds.), *The Transformation of Human Rights Fact-Finding* (Oxford: Oxford University Press, 2015).

Internet cuyos datos se recopilan. Estos usuarios tienen sus propias expectativas de privacidad incluso cuando publican en sitios que son de fácil acceso para el público. Los usuarios pueden sentir que sus publicaciones son privadas, solo para sus amigos y otros usuarios de una comunidad en línea.

b) Lo que se conoce técnicamente como scrapping de datos (desguace o raspado de datos) implica la recopilación real de datos de fuentes en línea para ser copiados y almacenados para su recuperación futura. La práctica del desguace también puede tener un impacto en los usuarios individuales de Internet. Con el raspado, los datos de los usuarios pueden ser recopilados por una entidad desconocida para ellos, incumpliendo sus expectativas de privacidad o normas comunitarias o sociales.

c) La clasificación e indexación implican categorizar los datos recopilados de manera estructurada para que puedan buscarse y referenciarse. Los datos se pueden clasificar según las categorías sociales creadas por el recopilador o titular de datos, como el nombre, el género, la religión o la afiliación política. La clasificación extiende el riesgo de privacidad a los usuarios individuales de Internet cuyos datos se han recopilado. Los datos de los sujetos, colocados en una base de datos, ahora están organizados de una manera que puede no representar correctamente a esos sujetos o puede exponerlos si los datos se divulgan inadvertidamente. Colocar los datos de identificación personal de los sujetos en categorías que pueden ser incorrectas puede arrojar a los del conjunto de datos de forma falsa.

d) El almacenamiento y la retención de grandes cantidades de datos son cada vez más frecuentes a medida que el almacenamiento se vuelve menos costoso. Esta situación significa que más entidades pueden conservar más

datos durante más tiempo. Una publicación que alguien haya pensado que era fugaz o eliminada puede persistir en numerosas bases de datos invisibles de manera efectiva a perpetuidad. El almacenamiento de datos durante largos períodos de tiempo expone a los usuarios a riesgos de privacidad imprevistos. La seguridad de la información débil puede conducir a fugas o infracciones que revelan datos personales a otros a quienes los recolectores o los usuarios no tenían la intención de informar. Esto podría exponer a las personas a la vergüenza, extorsión, violencia física u otros daños, continúa señalando Latonero en su obra.

Latonero, continúa estableciendo que

e) El uso de análisis de Big Data implica el despliegue de una serie de técnicas y herramientas diseñadas para encontrar patrones, indicadores de comportamiento o identidades de individuos, grupos o poblaciones. La estructuración de datos, la realización de modelos estadísticos y la creación de visualizaciones transforman conjuntos de datos de otro modo incomprensibles en información procesable.

Para Latonero, con el cual coincido plenamente, la amenaza a la privacidad por el uso de análisis de big data es clara. La entidad que realiza el análisis podría aprender más sobre la vida de una persona de lo que esperaría un ciudadano típico, violando así el derecho a determinar el flujo y el uso de la información personal. Al combinar fuentes de datos dispares, estas entidades pueden vincular identidades en línea con identidades del mundo real o descubrir los hábitos o la información personal de una persona[45].

[45] LATONERO cita "The 'mosaic theory' describes a basic precept of intelligence gathering: Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information." POZEN D.E., "The

Para Latonero, también existe el riesgo de que el análisis sea incorrecto. Los conjuntos de datos y los análisis llevados a cabo en ellos siempre conllevan algún tipo de sesgo, y dichos análisis pueden conducir a falsos positivos y negativos sobre los que los responsables de la toma de decisiones pueden actuar más adelante. Desplegar recursos en el lugar equivocado o en el momento equivocado puede causar un daño significativo a las personas. Incluso si el análisis es correcto para identificar una violación de los derechos humanos, las víctimas pueden correr un mayor riesgo si se identifican públicamente debido al estigma de la comunidad o las represalias de los perpetradores.

Finaliza el autor estableciendo que:

f) El acceso y el uso compartido se aplican tanto al uso como a la recopilación de datos. La forma en que los datos se indexan o clasifican o el tipo de datos recopilados ya puede revelar información considerada privada. El intercambio y el acceso no autorizados presentan una violación importante de las normas de privacidad en el contexto de los derechos humanos.

El análisis de Latonero no hace más que recoger lo que la propia Federal Trade Commission[46], del Gobierno Americano, reconoce como principales preocupaciones del tratamiento de datos a gran escala.

Mosaic Theory, National Security, and the Freedom of Information Act" (Note) 115 *Yale Law Journal* 628–79.(2005)

[46] Ver informe FTC de enero de 2016 " Big Data: A tool for inclusion or exclusion? Uderstanding the issues"

7. El tratamiento de los datos y su relación con el derecho a la privacidad.

I

El derecho al respeto de la vida privada y el derecho a la protección de datos personales, aunque están estrechamente relacionados, son derechos distintos. El derecho a la privacidad, referido en la ley europea como el derecho al respeto de la vida privada, surgió en la Declaración Universal de los Derechos Humanos (DUDH), adoptada en 1948, como uno de los derechos humanos fundamentales protegidos. Poco después de la adopción de la DUDH, Europa también afirmó este derecho: en el Convenio Europeo de Derechos Humanos (CEDH), un tratado que es legalmente vinculante para sus Partes Contratantes y que se redactó en 1950. El CEDH establece que toda persona tiene derecho a Respeto por su vida privada y familiar, hogar y correspondencia. La interferencia con este derecho por parte de autoridad pública está prohibida, excepto cuando la interferencia es conforme a la ley, persigue intereses públicos importantes y legítimos y es necesaria en una sociedad democrática.

II

La DUDH y el CEDH fueron adoptados mucho antes del desarrollo de Internet y del surgimiento de la sociedad de la información. En respuesta a estos desarrollos surge la necesidad de normas específicas que rijan la recopilación y el uso de información personal. De ahí surgió un nuevo concepto de privacidad, conocido en algunas jurisdicciones como "privacidad informativa" y en otras como el "derecho a la autodeterminación

informativa"[47]. Este concepto condujo al desarrollo de regulaciones legales especiales que proveen protección de datos personales.

III

El Big data plantea grandes riesgos de privacidad. La recopilación de grandes conjuntos de datos personales y el uso de análisis de última generación implican crecientes problemas de privacidad. La protección de la privacidad será más difícil a medida que la información se multiplique y se comparta cada vez más ampliamente entre múltiples partes de todo el mundo. A medida que se comparte más tipo de información de salud, ubicación, la actividad en línea de las personas, etc, surgen inquietudes con respecto a la elaboración de perfiles, el seguimiento, la discriminación, la exclusión, la vigilancia gubernamental y la pérdida de control[48].

Así tenemos que los efectos agregadores de datos, la decisión automatizada, el análisis predictivo tienen marcadas implicaciones para las personas susceptibles a enfermedades, delitos, etc. Sin duda, el análisis predictivo se puede utilizar para objetivos socialmente beneficiosos. Sin embargo, todo esto puede cruzar fácilmente el umbral de "escalofrío"[49] y la falta de acceso

[47] El Tribunal Constitucional Federal de Alemania afirmó el derecho a la autodeterminación informativa en una sentencia de 1983 en Volkszählungsurteil, BVerfGE Big Data. 65, S. 1ff. El tribunal consideró que la autodeterminación informativa se deriva del derecho fundamental al respeto de la personalidad, protegido por la Constitución alemana. La ECtHR reconoció en una sentencia de 2017 que el art. 8 de la CEDH "prevé el derecho a una forma de autodeterminación informativa". Ver ECtHR, Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finlandia, No. 931/13, 27 de junio de 2017, párr. 137. Información proporcionada por la Comisión Europea y traducida y adaptada por el autor.

[48] TENE, HAIM Y POLONETSKY "Big Data for All: Privacy and User Control in the Age of Analytics". Northwestern Journal of Technology and Intellectual Property Volumen 11.(2013)

[49] Íbidem supra que citan a Danah Boyd, Senior Researcher, Microsoft Research, Speech at the DataEDGE Conference 2012 (citado en Quentin Hardy, Rethinking Privacy in an Era of Big Data, N.Y. TIMES, June 4, 2012, http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-

de las personas a la generación de datos y su exclusión, tal y como se explica en la presente tesis, proporcionan serias preocupaciones sobre la privacidad debido a su falta de transparencia.

Así, en febrero de 2019, en Estados Unidos, más de 40 grupos de Derechos Civiles, Libertades Civiles enviaron una carta al Congreso en que, debido al Big Data, piden a los legisladores que protejan los derechos civiles –la privacidad-, la equidad y la igualdad de oportunidades en el ecosistema digital. Los grupos expusieron que no se debe permitir que las plataformas y otros servicios en línea utilicen los datos de los consumidores para discriminar a las clases protegidas o negarles oportunidades en el comercio, la vivienda y el empleo, o la plena participación en la democracia y apoyaban la "transparencia algorítmica" que no es más que el derecho de las personas a conocer los procesos de datos que impactan sus vidas para que puedan impugnar las decisiones tomadas por algoritmos

8. La relación entre el Big Data y otros Derechos Fundamentales.

La protección de datos también tiene vínculos con otros derechos humanos. El crecimiento exponencial en el procesamiento de datos y el aumento de los riesgos que esto ha generado, ha impulsado la protección de los derechos humanos en la agenda de los legisladores. En algunos Estados, incluso ha habido avances hacia el reconocimiento de la protección de datos como un derecho humano distinto y separado. Pero ya sea como un elemento del derecho a la privacidad o como un derecho humano o un derecho

an-era-of-big-data) (stating that “privacy is a source of tremendous tension and anxiety in Big Data. It’s a general anxiety that you can’t pinpoint, this odd moment of creepiness.”).

fundamental diferente, la protección de datos sólida y efectiva también ayuda a proteger otros derechos humanos, tal y como vienen fundamentando el TEDH y el TJUE que han declarado repetidamente que es necesario un ejercicio de equilibrio con otros derechos al aplicar e interpretar el Artículo 8 del CEDH y el Artículo 8 de la Carta.[8]

8.1. El Big Data y la Libertad de expresión.

I

Uno de los derechos que interactúa más significativamente con el Big Data es el derecho a la libertad de expresión, no solo desde el punto de vista de la legislación europea sino de Estados Unidos[50], donde la primera enmienda de la Constitución[51] le dota de un mayor énfasis a este principio que la legislación europea.

En Europa, la libertad de expresión está protegida por el Artículo 11[52] de la Carta Europea de Derechos Fundamentales[53] (CEDF). Este derecho incluye la "libertad de mantener opiniones y recibir e impartir información e ideas sin interferencia de la autoridad pública y sin importar las fronteras".

[50] Muy ilustrativo sobre el tema es la tesis de BALKIN, M. J "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" disponible en https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&https redir=1&article=6159&context=fss_papers. Acceso en enero 2019.

[51] El Congreso no podrá hacer ninguna ley con respecto al establecimiento de la religión, ni prohibiendo la libre práctica de la misma; ni limitando la libertad de expresión, ni de prensa; ni el derecho a la asamblea pacífica de las personas, ni de solicitar al gobierno una compensación de agravios.

[52] 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades pœblicas y sin consideración de fronteras. 2. Se respetan la libertad de los medios de comunicación y su pluralismo

[53] http://www.europarl.europa.eu/charter/pdf/text_es.pdf

La libertad de información, de acuerdo con el Artículo 11 de la CEDF y el Artículo 10 del Convenio Europeo de Derechos Humanos[54], protege el derecho no solo de impartir sino también de *recibir* información.

Las limitaciones a la libertad de expresión deben cumplir con los criterios establecidos en el Artículo 52[55] de la CEDF.

De conformidad con el Artículo 52 de la CEDF, en la medida en que contiene derechos que corresponden a los derechos garantizados por el CEDH, "el significado y alcance de esos derechos serán los mismos que los establecidos en dicha Convención (la CEDH)". Cabe recordar en este punto, que otro de los derechos garantizados en la CEDH es el recogido en el artículo 14, de no discriminación, que expone que "El goce de los derechos y libertades reconocidos en el presente Convenio ha de ser asegurado sin distinción alguna, especialmente por razones de sexo, raza, color, lengua, religión, opiniones políticas u otras, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación.", cosa que parece haberse olvidado el legislador europeo.

La relación entre la protección de datos personales y la libertad de expresión se rige por el artículo 85 del Reglamento General de Protección de Datos, titulado "Procesamiento y libertad de expresión e información". Según este artículo, los Estados miembros conciliarán el derecho a la protección de datos personales con el derecho a la libertad de expresión e información. En particular, las exenciones y excepciones a capítulos específicos del Reglamento General de Protección de Datos se realizarán con fines

[54] Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir ode comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.
[55] Sobre el alcance de los derechos garantizados

periodísticos o con fines de expresión académica, artística o literaria, siempre que sean necesarios para conciliar el derecho a la protección de datos personales con la libertad de expresión e información.

II

La jurisprudencia europea sobre protección de datos personales derivados del tratamiento de datos es, a mi juicio, no conforme con la realidad actual y futura derivada del uso de aplicaciones móviles y de Internet de las Cosas ya que son parámetros que aún no se han tenido en cuenta por parte de los tribunales. No se puede poner en duda que, a través de las aplicaciones móviles y el uso que hacemos de determinados dispositivos conectados a la red expresamos, quizá de la manera más genuina posible, nuestras opiniones y deseos más íntimos.

III

La jurisprudencia europea se ha expresado en referencia a la libertad de expresión como paradigma de la libertad de prensa[56] En particular, el TEDH tuvo que verificar si el procesamiento de datos personales obtenidos lícitamente por un periódico debe considerarse como una actividad realizada únicamente con fines periodísticos. Después de haber concluido que las actividades de la empresa eran el "procesamiento de datos personales", señaló la importancia del derecho a la libertad de expresión en todas las sociedades democráticas y sostuvo que las nociones relacionadas con esa libertad, como el periodismo, deberían interpretarse de manera amplia. Luego observó que, para lograr un equilibrio entre los dos derechos fundamentales, las excepciones y limitaciones del derecho a la protección de datos deben

[56] TEDH Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finlandia, No. 931/13.

aplicarse solo en la medida en que sea estrictamente necesario. En tales circunstancias, el TEDH sostuvo que las actividades como las realizadas por las empresas en cuestión con respecto a los datos de documentos que son de dominio público en virtud de la legislación nacional pueden clasificarse como "'actividades periodísticas" si su objeto es la divulgación al público de información, opiniones o ideas, independientemente del medio utilizado para transmitirlas. Importante es también el hecho de que también dictaminó que estas actividades no se limitan a empresas de medios y pueden llevarse a cabo con fines de lucro.

El Tribunal recuerda en la sentencia los criterios de la jurisprudencia que deberían guiar a las autoridades nacionales y al propio TEDH al equilibrar la libertad de expresión con el derecho al respeto de la vida privada. Cuando se trata de un discurso político o un debate sobre una cuestión de interés público, hay poco margen para restringir el derecho a recibir y difundir información, ya que el público tiene derecho a estar informado, "y este es un derecho esencial en una sociedad democrática".

Sin embargo, no se puede considerar que los artículos de prensa destinados únicamente a satisfacer la curiosidad de un lector en particular con respecto a los detalles de la vida privada de una persona contribuyan a un debate de interés público.

Importa señalar que, para el TEDH, la derogación de las reglas de protección de datos para fines periodísticos tiene por objeto permitir a los periodistas acceder, recopilar y procesar datos para poder realizar sus actividades periodísticas. Por lo tanto, hay interés público en proporcionar acceso y permitir que las empresas solicitantes recopilen y procesen las grandes

cantidades de datos tributarios en juego. En contraste, el Tribunal encontró que no había ningún interés público en la difusión masiva de tales datos sin procesar por parte de los periódicos, en forma inalterada y sin ninguna aportación analítica. La información dada por el periódico, que se refería a temas tributarios, podría haber permitido a los curiosos miembros del público clasificar a las personas según su situación económica y satisfacer la sed del público de obtener información sobre las vidas privadas de otros. Esto no podría considerarse como una contribución a un debate de interés público.

En definitiva, y siguiendo la argumentación realizada por el TEDH es posible que las empresas privadas recopilen nuestros datos de consumo, gustos, políticos, etc para poder trabajar con ellos, aunque no puedan difundirlos.

Es mi opinión que el TEDH deberá profundizar más en el tema de la protección de datos personales recogidos y tratados por o mediante dispositivos comunicados en la Red.

IV

En definitiva, en el ámbito europeo, tampoco parece que el Tribunal Europeo de Derechos Humanos tenga en cuenta la realidad del Big Data en cuanto a la conciliación del derecho a la protección de datos con el derecho a la libertad de expresión.

El TEDH viene estableciendo en diversas sentencias[57] los criterios que deben considerarse al equilibrar el derecho a la libertad de expresión con el derecho al respeto de la vida privada, según lo establecido en su jurisprudencia: En

[57] Por todas ellas TEDH, *Axel Springer AG c. Alemania* [GC], No. 39954/08, 7 de febrero de 2012, párrs. 90 y 91 y TEDH Coudec y Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 de noviembre de 2015.

primer lugar, si lo publicado era de interés general; en segundo lugar, si la persona interesada era una figura pública; y en tercer lugar hay que tener en cuenta cómo se obtuvo la información y si era confiable.

En la jurisprudencia del TEDH, uno de los criterios cruciales para el equilibrio de estos derechos es si la expresión en cuestión contribuye o no a un debate de interés público general, cosa que poco tiene que ver con el Big Data.

Interesante sentencia del TEDH[58] es aquella referida a una violación del derecho a la privacidad, ya que se le había negado la oportunidad de solicitar un recurso judicial antes de la publicación de unas fotos por un periódico sin darle aviso anticipado de la publicación.

El TEDH señaló que, aunque la difusión de dicho material era generalmente para fines de entretenimiento más que para educación, la notificación previa del uso de su imagen personal – que recordemos que son datos tratables por Big Data- podría dar lugar a un efecto "escalofriante", concluyendo que no era necesaria la existencia de un requisito de notificación previa legalmente vinculante en virtud del artículo 8 del Convenio Europeo de Derechos Humanos[59].

En otras sentencias, el TEDH[60] ha recordado que la protección de los datos

[58] TEDH, Mosley v. Reino Unido, No. 48009/08, 10 de mayo de 2011, párrs. 129 y 130.
[59] 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.
[60] TEDH Biriuk v. Lituania, No. 23373/03, 25 de noviembre de 2008.

personales, y sobre todo los datos datos médicos, es de fundamental importancia para el derecho al respeto de la vida privada en virtud de la CEDH. La confidencialidad de los datos de salud es particularmente importante, ya que la divulgación de datos médicos puede afectar dramáticamente la vida privada y familiar de una persona, su situación laboral e inclusión en la sociedad.

El derecho a la libertad de expresión y el derecho a la protección de datos personales no siempre están en conflicto. Hay casos en que la protección efectiva de los datos personales garantiza la libertad de expresión.

V

Más en línea con la problemática que presenta el Big Data, cabe destacar una de las consideraciones que realiza el TJUE[61], donde fundamenta que "Además (…) el hecho de que los datos se conserven y se utilicen posteriormente sin que el suscriptor o el usuario registrado estén informados es probable que genere en las mentes de las personas afectadas la sensación de que sus vidas privadas son objeto de vigilancia constante ".

El TEDH también encontró que la retención generalizada de los datos de tráfico y ubicación, como se hace en algunos países por parte de los gobiernos o realizan dteerminadas aplicaciones, podría tener un efecto en el uso de las comunicaciones electrónicas y, en consecuencia, en el ejercicio por parte de los usuarios de su libertad de expresión garantizada en el Artículo 11 de la CEDF. En ese sentido, al exigir estrictas salvaguardas para que la retención de datos no se lleve a cabo de manera generalizada, las reglas de protección de

[61] TEDH, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB v. och telestyrelsen y Secretario de Estado para el Departamento del Hogar c. Tom Watson y otros [GC], 21 de diciembre de 2016, párr. 37 y 101;

datos contribuyen en última instancia al ejercicio de la libertad de expresión.

VI

En Estados Unidos, unos de los ejemplos más famosos de jurisprudencia sobre la libertad de expression, recogida en la primera enmienda[62] de su Constitución, son las sentencias New York Times Co. v. Sullivan y New York Times Co. v. United States.

La privacidad, la dignidad y el honor personal tienen una más amplia importancia en la jurisprudencia europea que en la de los Estados Unidos.

En muchos casos después de New York Times Co v. Sullivan, la Cort Suprema de los Estados Unidos ha subordinado la protección de la privacidad, la dignidad y el honor personal para brindar una protección amplia a la libertad de expresión y de prensa, mientras que, en Europa, como vemos, no siempre es así.

8.2. El Big Data y el Secreto profesional.

I

En los países miembros de la Unión, de acuerdo con las legislaciones de cada uno de los estados, ciertas comunicaciones pueden estar sujetas a la obligación del secreto profesional. El secreto profesional puede entenderse como un deber ético especial que incurre en una obligación legal inherente a ciertas profesiones y funciones, que se basan en la fe y la confianza[63]. Las

[62] Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances
[63] European Commission. "Guide on data Protection" (2018).

personas e instituciones que cumplen estas funciones están obligadas a no revelar información confidencial recibida por ellos en el curso de la realización de sus funciones. El secreto profesional se aplica especialmente a la profesión médica y al privilegio de abogado-cliente, y muchas jurisdicciones también reconocen una obligación de secreto profesional en otros sectores como el financiero. El secreto profesional no es un derecho fundamental, pero está protegido como una forma del derecho al respeto por la vida privada. Por ejemplo, el TJUE ha dictaminado[64] que en ciertos casos, "puede ser necesario prohibir la divulgación de cierta información que se clasifica como confidencial, para proteger el derecho fundamental de una empresa a respetar su vida privada consagrada en el Artículo 8 CEDH y artículo 7[65] de la CEDF". Cabría preguntarse si los datos recopilados por el IoT debieran estar sujetos al secreto profesional.

II

Interesante es el hecho de que el TEDH[66] también ha sido llamado a decidir si las restricciones al secreto profesional constituyen una infracción del artículo 8 del CEDH estableciendo que la intercepción de las conversaciones de un abogado con su cliente infringe el secreto profesional o su derecho al respeto de la vida privada o la violación de la correspondencia y que el acceso a los extractos bancarios del solicitante constituía una injerencia en su derecho al respeto de la confidencialidad profesional, que está dentro del alcance de la vida privada. La interferencia de las comunicaciones en este

[64] TJUE asunto T-462/12 R, Pilkington Group Ltd contra Comisión Europea, Auto del Presidente del Tribunal General, 11 de marzo de 2013.
[65] Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
[66] Entre otras, TEDH, Pruteanu v. Rumania, No. 30181/05, 3 de febrero de 2015 (párrafo 56 y siguientes y TEDH, Brito Ferrinho Bexiga Villa-Nova v. Portugal, No. 69436/10, 1 de diciembre de 2015.

caso tenía una base legal, y perseguía un objetivo legítimo. Sin embargo, al examinar la necesidad y la proporcionalidad de la interferencia, el TEDH señaló el hecho de que los procedimientos para levantar la confidencialidad se llevaron a cabo sin la participación o el conocimiento del solicitante. Por lo tanto, la demandante no pudo presentar sus argumentos. Además, el solicitante no tenía la opción de impugnar efectivamente el levantamiento de la confidencialidad, ni ningún remedio por el cual impugnar la medida. Debido a la falta de garantías procesales y al control judicial efectivo sobre la medida que suspende el deber de confidencialidad, el TEDH concluyó que se había violado el artículo 8 del CEDH.

III

En Estados Unidos, el secreto profesional en el ámbito legal se conoce como el privilegio abogado-cliente, que protege las comunicaciones entre un cliente y su abogado y mantiene esas comunicaciones confidenciales.

Sin embargo, en los Estados Unidos, no todos los tribunales estatales tratan las comunicaciones de abogados como privilegiadas. Así, la ley del estado de Washington y los tribunales federales cuando aplican la ley federal solo protegen las comunicaciones de los abogados que revelen comunicaciones con su cliente o que versen sobre éste.

En contraste, la ley del estado de California protege las comunicaciones confidenciales del abogado, independientemente de si contienen, se refieren o revelan las comunicaciones del cliente.

Además, el Tribunal Supremo de Estados Unidos ha dictaminado que el privilegio generalmente no termina con la muerte del cliente.

Hay que recordar en este punto que el secreto profesional en EEUU es más amplio que en Europa, pues se considera un deber moral[67] que puede ser establecido mediante contrato.

III

Es relevante el hecho de que los operadores del ecosistema del Big Data interceptan nuestros datos de manera masiva a través de múltples aplicaciones. La interacción entre el secreto profesional y la protección de datos es a menudo ambivalente. Por un lado, las normas de protección de datos y las garantías establecidas en la legislación ayudan a garantizar el secreto profesional. Por ejemplo, las reglas que requieren que los controladores y procesadores implementen medidas de seguridad de datos sólidas buscan evitar, entre otras cosas, la pérdida de confidencialidad de los datos personales protegidos por el secreto profesional.

El RGPD, en el ámbito europeo, permite el procesamiento de datos sanitarios, que constituyen categorías especiales de datos personales que merecen una mayor protección, pero están sujetos a la existencia de medidas adecuadas y específicas para salvaguardar los derechos de los interesados, en particular el secreto profesional.[68]

Por otra parte, las obligaciones de secreto profesional impuestas a los controladores y procesadores con respecto a ciertos datos personales pueden limitar los derechos de los interesados, especialmente el derecho a recibir información. Aunque el RGPD contiene una extensa lista con información que, en principio, debe proporcionarse al interesado cuando los datos

[67] BARDES, G. F. “Problems of profesional secrecy”. Boston College.(2015).
[68] RGPD, art. 9 (2) (h) y 9 (3).

obtenidos no son datos personales, este requisito de divulgación no se aplica cuando los datos personales deben permanecer confidenciales debido a una obligación de secreto profesional exigida por las leyes nacionales o de la UE[69]

El RGPD prevé la posibilidad de que los Estados miembros adopten, mediante ley, normas específicas para salvaguardar las obligaciones de secreto profesional u otras equivalentes y conciliar el derecho a la protección de datos personales con la obligación de secreto profesional[70].

8.3 El Big Data y la Libertad Pensamiento, Conciencia y Religión.

La libertad de religión y creencias está protegida por el artículo 9 del CEDH y el artículo 10[71] de la CEDF. Los datos personales que revelan creencias religiosas o filosóficas se consideran "datos confidenciales" según las leyes Europeas y del Consejo de Europa, y su procesamiento y uso están sujetos a una mayor protección. De igual manera, el artículo 18 de la Declaración Universal de Derechos Humanos contempla estos derechos. El párrafo 2 del artículo 18 prohíbe las medidas coercitivas que puedan menoscabar el derecho a tener o a adoptar una religión o unas creencias. El párrafo 3 del artículo 18 permite restringir la libertad de manifestar la religión o las creencias con el fin de proteger la seguridad, el orden, la salud o la moral

[69] RGPD art. 14 (5) (d).
[70] RGPD Considerando 164 y art. 90
[71] 1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión. Este derecho implica la libertad de cambiar de religión o de convicciones, así como la libertad de manifestar su religión o sus convicciones individual o colectivamente, en público o en privado, a través del culto, la enseæanza, las prácticas y la observancia de los ritos. 2. Se reconoce el derecho a la objeción de conciencia de acuerdo con las leyes nacionales que regulen su ejercicio

públicos, o los derechos y libertades fundamentales de los demás, con ciertas condiciones.

El TEDH ha reiterado[72] que la libertad religiosa implica la libertad de manifestar la religión de una persona en comunidad con otros, en público y dentro de ella con las personas que comparten la misma fe, pero también a solas y "en privado". El derecho a manifestar la propia religión también confiere lo contrario, es decir, el derecho a no estar obligado a revelar sus creencias.

Conforme al art. 91 RGPD, los datos que revelan las creencias religiosas son datos confidenciales, y las iglesias deben ser responsables de su manejo y procesamiento. En consecuencia, y con más motivo – aunque esto no aperece en el articulado del RGPD -, aquellas empresas que puedan llegar a saber nuestra creencia religiosa a través de la "captura" de nuestros datos -y más teniendo en cuenta si la información procesada puede afectar a niños- debieran abstenerse de tratar o incorporar estos datos, cosa que parece bastante difícil.

El problema no parece radicarse en los datos que posean las iglesias, sino en los datos que puedan poseer y tratar terceros, como un Estado, para saber las creencias religiosas de sus ciudadanos y actuar en consecuencia con tal de vulnerar el artículo 18 de la Declaración Universal de Derechos Humanos sobre la libertad de religión o conciencia.

[72] TEDH, Sinan Işık v. Turquía, No. 21924/05, 2 de febrero de 2010

8.4. El Big Data y el Derecho a la libertad de las artes y las ciencias.

Estos derecho son consecuencia del derecho a la libertad de pensamiento y expresión y debe ejercerse teniendo en cuenta la dignidad humana y debe equilibrarse con los derechos al respeto de la vida privada y a la protección de datos es la libertad de las artes y las ciencias, explícitamente protegida en virtud del Artículo 13CEDF[73].

El TEDH considera que la libertad de las artes está protegida por el artículo 10 del CEDH[74] El derecho garantizado por el Artículo 13 CEDF también puede estar sujeto a las limitaciones de conformidad con el Artículo 52 CEDF[75], que también puede interpretarse a la luz de del Artículo 10 (2) del CEDH.

El RGPD también reconoce el valor especial de la ciencia para la sociedad, al igual que el Convenio modernizado 108, que permiten la retención de datos durante períodos más largos ya que entiende que los datos personales se procesarán únicamente con fines de investigación científica o histórica. Además, e independientemente del propósito original de una actividad de procesamiento específica, el uso posterior de datos personales para investigación científica no se considerará un propósito incompatible[76] · Al mismo tiempo, se deben implementar las garantías adecuadas para dicho procesamiento para proteger los derechos y libertades de los interesados. La legislación de la UE o del Estado miembro puede proporcionar, entre otros,

[73] Las artes y la investigación científica son libres. Se respeta la libertad de cátedra.
[74] TEDH, müller y otros v. Suiza, No. 10737/84, 24 de mayo de 1988. 121 Explicaciones relativas a la Carta de los Derechos Fundamentales, DO 2007, C 303.
[75] Íb.Supra
[76] Regulación general de protección de datos, art. 5 (1) (b) and Modernised Convention 108, Art. 5 (4) (b).

excepciones al derecho de acceso, rectificación, restricción de procesamiento y al de objetar cuando se trata de procesar sus datos personales para investigación científica, histórica etc.

8.5 El Big Data y el Derecho a la propiedad intelectual.

En Europa, el derecho a la protección de la propiedad está consagrado en el artículo 1 del Primer Protocolo de la Convención Europea de Derechos Humanos[77] y también en el artículo 17 CEDF[78]. Un aspecto importante del derecho a la propiedad es la protección de la propiedad intelectual, mencionada explícitamente en el Artículo 17 CEDF.

La jurisprudencia del TJUE establece que la protección del derecho fundamental a la propiedad debe equilibrarse con la protección de otros derechos fundamentales, en particular el derecho a la protección de datos[79]

Ha habido casos en que las instituciones de protección de derechos de autor exigieron que los proveedores de acceso a Internet divulgaran la identidad de los usuarios de las plataformas de intercambio de archivos de Internet protegidos por derechos de autor. Pero además de lo anterior se debería aclarar los derechos del productor de datos que, a la postre, genera una base de datos y que debiera estar sujeta a propiedad industrial en virtud de la

[77] Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/009
[78] 1. Toda persona tiene derecho a disfrutar de la propiedad de sus bienes adquiridos legalmente, a usarlos, a disponer de ellos y a legarlos. Nadie puede ser privado de su propiedad mÆs que por causa de utilidad pœblica, en los casos y condiciones previstos en la ley y a cambio, en un tiempo razonable, de una justa indemnización por su pérdida. El uso de los bienes podrá regularse por ley en la medida que resulte necesario para el interés general. 2. Se protege la propiedad intelectual.
[79] TJUE asunto, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU [GC],

Directiva de protección de las bases de datos CE 96/9 de 11 de marzo de 1996, o como mínimo a ciertos derechos de exclusividad, al abrir la posibilidad de que las empresas utilicen sus datos y, por ende, contribuyan a desbloquear los datos generados por máquinas. Sin embargo, las excepciones deberían estar claramente especificadas, en particular el suministro de acceso no exclusivo a los datos por parte del fabricante o de las autoridades públicas.

9. Las externalidades negativas del Big Data.

I

Las externalidades negativas es algo bien conocido por la ciencia económica. Existen externalidades cuando los costos o los beneficios privados no son iguales a los costes o los beneficios sociales.

Las externalidades son efectos indirectos de las actividades de consumo o producción, es decir, los efectos sobre agentes distintos al originador de tal actividad y que no funcionan a través del sistema de precios. En una economía competitiva privada, los equilibrios no estarán, en general, en un óptimo de Pareto, ya que solo reflejará efectos privados (directos) y no los efectos sociales (directo más indirecto), de la actividad económica.[80]Técnicamente esto se interpreta como: «cualquier efecto indirecto que ya sea una actividad de producción o consumo tiene sobre una

[80] LAFFONT, J.J. "Externalities" In: The New Palgrave Dictionary of Economics. Second Edition. Eds. Steven N. Durlauf and Lawrence E. Blume. Palgrave Macmillan, 2008. The New Palgrave Dictionary of Economics Online. Palgrave Macmillan. 29 de marzo (2011).

función de utilidad o sobre un conjunto de consumo o conjunto de producción»[81]

II

Sobre el aspecto de las externalidades negativas del Big Data, hay que acudir al estudio publicado por Jonas Lerman[82] en donde se ilustra sobre los efectos ante la igualdad social que tendrá el uso masivo del Big Data.

Según Lerman[83], "*miles de millones de personas en todo el mundo permanecen en la periferia de Big Data. Su información no se recopila o analiza con regularidad, ya que no se involucran de manera rutinaria en actividades que los datos grandes están diseñados para capturar. En consecuencia, sus preferencias y necesidades corren el riesgo de ser ignoradas rutinariamente cuando los gobiernos y la industria privada utilizan Big Data y analíticas avanzadas para dar forma a la política pública y al mercado. El Big Data representa una amenaza única para la igualdad, no solo para la privacidad.*"

El Big Data hace posibles abusos de las libertades civiles por parte del gobierno, la erosión de las normas de privacidad e incluso daños ambientales ya que las "granjas de servidores" utilizadas para procesar grandes volúmenes de datos consumen enormes cantidades de energía.

El Big Data representa un riesgo para aquellas personas que son "excluidas" por el tratamiento de datos, cuya información no se recopila, cultiva o extrae

[81]HANMING F, "Externality Versus Public Goods ". Duke University. (2014).

[82] LERMAN, J. "Big Data and its exclusions". 66 STAN. L. Rev. online 55 September 3.(2013)

[83] LERMAN, J. Íb ud supra. Artículo traducido y adaptado por el autor.

regularmente. De momento, sólo un 57% de la población mundial tiene acceso a internet[84].

Será necesaria una definición legal apoyada por una doctrina para proteger a aquellas personas a quienes la gran revolución del Big Data corre el riesgo de dejar de lado. Lerman lo define como la "antisubordinación" de los datos.

El Big Data surge de una idea simple: reúne suficientes detalles sobre el pasado, aplica las herramientas analíticas correctas y puedes encontrar conexiones y correlaciones inesperadas, que pueden ayudarte a hacer predicciones inusualmente precisas sobre el futuro: cómo los compradores deciden entre productos, cómo operan los terroristas, cómo se propagan las enfermedades, etc.

Si el Big Data determina cada vez más la toma de decisiones del gobierno y las empresas, entonces se podría asumir que se presta mucha atención a quién y qué da forma al Big Data. Sin embargo, en general, los expertos expresan una sorprendente indiferencia sobre la precisión o la procedencia de los datos. De hecho, abrazan el "desorden" como una virtud[85].

Tal "desorden" supone que los errores inevitables que se arrastran en las operaciones de grandes conjuntos de datos son aleatorios y absorbibles, y pueden ser considerados en el análisis final.

Pero también hay otro tipo de error que puede infectar conjuntos de datos: la omisión sistémica y no aleatoria de las personas que viven en los márgenes de

[84] https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates. acceso 19 de febrero de 2019.

[85] MAYER-SCHÖNBERGER,V Y CUKIER, K "Big data:arevolución that will transform how we live,work," Amazon. (2013).

Big Data, ya sea debido a la pobreza, la geografía o el estilo de vida, y cuyas vidas son menos "informadas" que las de la población general. En sectores clave, su marginación corre el riesgo de distorsionar el Big Data y, por consiguiente, sesgar el análisis del que dependen cada vez más los actores públicos y privados. Lerman lo define como “exclusiones de Big Data”.

Lerman propone el siguiente ejemplo: El primero es un residente de cuello blanco de treinta años de Manhattan. Ella participa en la vida moderna en todas las formas típicas de su demografía: teléfono inteligente, Google, Gmail, Netflix, Spotify, Whatsup. Ella usa Facebook, con su configuración de privacidad predeterminada, para mantenerse en contacto con amigos. Ella utiliza aplicaciones de contactos. Ella viaja con frecuencia, twitteando y publicando fotos etiquetadas geográficamente en Instagram. Su billetera tiene una tarjeta de débito, tarjetas de crédito y tarjetas de transportes, así como tarjetas de "recompensas al cliente" de su supermercado y de otras tiendas. En su automóvil, tiene GPS y pago virtual de autopistas y parkings. Los datos que genera todos los días, y que los gobiernos y las empresas tienen, sobre ella son casi incalculables. Además de la información recopilada por las compañías sobre sus gastos, comunicaciones, actividades en línea y movimiento, es ingente.

Lo compara con una segunda persona. Vive dos horas al suroeste de Manhattan, en Camden, Nueva Jersey, la ciudad más pobre de Estados Unidos. Está subempleado, trabaja a tiempo parcial en un restaurante y cobra parte del salario en efectivo. No tiene ordenador ni televisión por cable. Rara vez viaja y no tiene pasaporte, automóvil o GPS. Utiliza Internet, pero solo en la biblioteca local en los terminales públicos. Cuando toma el autobús, paga la tarifa en efectivo.

Pues bien, hoy en día, muchas de las herramientas de Big Data están calibradas para gente de Manhattan, o para gente de cualquier ciudad europea o asiática, que habitualmente generan grandes cantidades de datos electrónicamente.

La ciudad, en este caso del ejemplo de Lerman, Manhattan, también puede rastrear sus movimientos a través de las tarjetas de transporte, datos útiles no solo para la aplicación de la ley, sino también para determinar nuevos horarios de tránsito, planear carreteras y establecer peajes. Para procesar estos datos, la ciudad cuenta con funcionarios dedicados a analizar temas que van desde los hábitos de viaje hasta el uso de electricidad, desde las notas de las pruebas de los alumnos hasta la más ignota de las cosas medibles[86].

Un mundo donde las decisiones se toman por Big Data tendrá en cuenta los hábitos de la gente que pueda medir y sus preferencias. Pero el Big Data actualmente pasa por alto el ejemplo propuesto por Lerman en referencia a personas como la de New Jersey, por no hablar de otros sitios donde la penetración de internet o celular es mucho menor.

Entiendo, junto con Lerman, que en un futuro, ya presente, en que el Big Data, y las predicciones que posibilita su tratamiento, reordenará fundamentalmente las decisiones de los gobiernos y el mercado, la exclusión de determinadas personas marginadas por el Big Data tiene implicaciones preocupantes para las oportunidades económicas, la movilidad social y la participación democrática.

[86] FEUER, A "*The Geek Squad de la Alcaldía*," NY TIMES, 23 de marzo de 2013.

Tal y como Lerman expone, estas tecnologías pueden crear un nuevo tipo de ausencia de voz, donde las preferencias y comportamientos de ciertos grupos reciben poca o ninguna consideración cuando los actores poderosos deciden cómo distribuir bienes y servicios y cómo reformar las instituciones públicas y privadas. Y así lo están demostrando recientes estudios.[87]

Se presentan dos tipos de problemas que deberían ser abordados por el legislador:

En primer lugar, aquellos que quedan fuera de la revolución del Big Data pueden sufrir daños económicos tangibles. Las empresas pueden ignorar o subestimar las preferencias y comportamientos de los consumidores que no compran de manera que las herramientas de Big Data puedan capturar, agregar y analizar fácilmente. Es posible que las tiendas no abran en sus vecindarios, negándoles no solo las opciones de compra, sino también las oportunidades de empleo; ciertas promociones no pueden ser ofrecidas a ellos; es posible que los nuevos productos no estén diseñados para satisfacer sus necesidades o que su precio no se ajuste a sus presupuestos. Por supuesto, las personas pobres y los grupos minoritarios ya están marginados en muchos aspectos en el mercado. Pero los grandes datos podrían reforzar y exacerbar los problemas existentes.

En segundo lugar, los políticos y los gobiernos pueden llegar a confiar en los grandes datos hasta el punto de que la exclusión de los flujos de datos conduce a la exclusión de la vida cívica y política, una barrera para la plena ciudadanía. Las campañas políticas ya explotan el Big Data para recaudar

[87] https://www.lavanguardia.com/lacontra/20190315/461031608874/es-mas-facil-saber-por-que-amamos-que-por-que-odiamos.html

dinero, planificar los esfuerzos de participación de los votantes y dar forma a sus mensajes[88].

La exclusión o representación insuficiente en los conjuntos de datos del gobierno, entonces, podría significar perder servicios sociales o sanitarios importantes y bienes públicos. La revolución del Big Data puede crear nuevas formas de desigualdad y subordinación, según la definición de Lerman, y por lo tanto aumenta el sentido de que no son tratados de manera justa por los diferentes gobiernos e incluso puede llegar a afectar a la misma esencia de la democracia.

Desde este punto de vista, el Big Data tiene el potencial de consolidar las desigualdades y estratificaciones existentes y crear otras nuevas. Podría reestructurar las sociedades de modo que las únicas personas que importan, literalmente las únicas que cuentan, sean las que regularmente contribuyen a los flujos de datos correctos.

Desde mi punto de vista, esto también debiera ser tenido en cuenta por el legislador y la doctrina sobre el tema. El Big Data no es sólo una cuestión de privacidad. También podría poner en peligro la igualdad política y social al relegar a las personas vulnerables a un estatus inferior.

III

Comparto con Lerman el hecho de que la doctrina está severamente limitada en su capacidad para abordar desventajas que no pueden atribuirse fácilmente

[88] RUTENBERG, J, Datos en los que puede creer, NY TIMES, 23 de junio de 2013,

al diseño oficial o que afectan a una clase "difusa y amorfa"[89].Además, es difícil imaginar qué igualdad formal o "anticlasificación" igualaría.

Comparto, igualmente, la reflexión de que una definición del Big Data que tuviese en cuenta la igualdad sería algo forzado ya que obligaría a públicos y privados, todo el ecosistema relacionado con el Big Data, a recopilar la información de todos, todo el tiempo, en nombre de la igualdad, o a recopilar información proporcionalmente de diferentes grupos raciales y socioeconómicos, teniendo en cuenta que, después de todo, dos de las supuestas garantías de privacidad incorporadas al Big Data son la anonimización y la aleatorización de los datos.

Pero debería conjugarse una posibilidad legal que lo permitiese.

Quizá el problema radica en el consentimiento de los datos y en el uso indiscriminado que se realiza en su obtención y tratamiento y en los que el RGPD define como el propósito del tratamiento de los datos.

El enfoque, lo que Owen Fiss llamó el "principio de desventaja de grupo"[90], puede necesitar una revisión, dado el potencial de Big Data para imponer nuevas formas de estratificación y reforzar el estado de los grupos ya desfavorecidos por no tener datos de ellos para ser tratados.

Es cierto, como expone Lerman y que no ha sido puesto en duda por ningún investigadores, sino todo lo contrario[91], - aunque él lo expone de diferente

[89] GOODWIN L, "Educación, Igualdad y Ciudadanía Nacional". 116 YALE LJ 330, 334 (2006).

[90] OWEN FISS M, "Grupos y la cláusula de igual protección", 5 PHIL. & PUB. AFF. 107, 147-56 (1976).

[91] Por citar un ejemplo, DEVINS, FELIN, KAUFFMAN Y KOPPL "The law and big data", disponible en https://www.lawschool.cornell.edu/research/JLPP/upload/Devins-et-al-final.pdf

manera y se refiere a las minorías sociales de estados Unidos-, que el ecosistema del tratamiento de datos debiera tener en cuenta, y sobre todo los Gobiernos, que existen grupos desfavorecidos sobre los que existe poca o nula "huella digital" y que para la adopción de políticas u otro tipo de acciones se les debiera tener en cuenta - ya que tienen todo el Derecho- para la adopción de éstas mediante un coeficiente corrector en los algoritmos o técnicas de tratamiento del Big Data para que su sesgo poblacional no sea un factor que desencadene desprotección en cualquier factor. Pero tal y como exponemos, los actores privados son muy importantes dentro del ecosistema del Big Data y ejercen una influencia en las sociedades y un poder sobre la agregación y el flujo de información, que en generaciones anteriores ni siquiera los gobiernos disfrutaban; y más aún con el Internet de las Cosas. Por lo tanto, la definición legal del Big Data y su concepción como Derecho estaría incompleta a menos que se extendiera, al sector privado.

IV

Podemos, a la vista de todo lo anterior, y a la vista del informe FTC de enero de 2016[92], exponer que las externalidades negativas del Big Data serán las siguientes:

a) Errores en atribuir comportamientos a personas que se han visto excluidas del proceso de obtención de datos.

b) Crear o reforzar las disparidades existentes debido al tratamiento de datos que no tiene en cuenta a los excluídos.

[92] Íb. Supra

c) Exponer información confidencial o que se tengan en cuenta en el tratamiento datos que las personas puedan considerar sensibles.

Sobre este aspecto, la Free Trade Commission pone como ejemplo un estudio, que combinó datos en Facebook "Me gusta" e información limitada de la encuesta, que concluyó que los investigadores podrían predecir con precisión la orientación sexual de un usuario masculino, el origen étnico, o su posicionamiento político o religioso entre otros[93] .

d) Fraude por parte de ciertas compañías al poder detectar consumidores más vulnerables.

e) Crear nuevas justificaciones para la exclusión. El análisis de Big Data puede brindar a las empresas nuevas formas de intentar justificar su exclusión de ciertas poblaciones de oportunidades particulares.

f) Prácticas que afecten a la libre competencia, segmentando mercados o imponiendo políticas de dumping o subiendo precios u ofreciendo menos servicios donde no hay competencia.

e) Debilitar la efectividad de la manera de actuar o elección libre de las personas. Incluso se puede utilizar big data para hacer inferencias sobre las personas que optan por restringir la recopilación de sus datos.

[93] Ver KOSINSKIN, M ET AL., Private Traits and Attributes Are Predictable From Digital Records of Human Behavior, 110 Proceedings of the Nat'l Acad. of Scis. 5802, 5803–04 (2013), http://www.pnas.org/content/110/15/5802.abstract. Ver también Jon Green, Facebook Knows You're Gay Before You Do, Am. Blog (Mar. 20, 2013), http://americablog.com/2013/03/facebook-might-know-youre-gay-before-you-do.html

10. Diferentes aproximaciones legales a la protección de los derechos de los datos personales.

10.1. Estados Unidos: The Algorithmic Accountability Act of 2019.

Mención en un aparte merece la propuesta de ley Federal de Estados Unidos, presentada en el Congreso Federal el 4 de octubre de 2019[94], por los demócratas denominada The Algorithmic Accountability Act of 2019 (AAA en adelante) , que busca mejorar la privacidad de los datos y la inteligencia artificial.

Si se aprueba, la AAA ordenaría a la Comisión Federal de Comercio (FTC en adelante) "exigir a las entidades que usan, almacenan o comparten información personal" que realicen evaluaciones de impacto de cualquier sistema de decisión automatizado o cualquier depósito de información del consumidor que se considere de "alto riesgo"[95].

"Según sus promotores, el proyecto de ley es consecuencia de las numerosas noticias conocidas en los últimos tiempos sobre algoritmos informáticos que provocan resultados sesgados y discriminatorios. Por ejemplo, a principios de abril, el Departamento de Vivienda y Desarrollo Urbano de los EEUU (Department of Housing and Urban Development) acusó a Facebook de violar la Ley de Vivienda Equitativa (Fair Housing Act), al permitir a los anunciantes discriminar por motivos de raza, religión y discapacidad de los interesados. Igualmente, el año pasado, Reuters informó de que Amazon

[94]https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf
[95] BYUNGKWON L, GARY MURPHY G, POPP F AND AMLER J. "A Glimpse Into The Potential Future Of AI Regulation". (2019).

había cerrado una herramienta de reclutamiento automatizado que estaba sesgada en contra de las mujeres".[96]

De esta manera, la AAA crea un marco regulatorio diseñado para reducir el riesgo de que, en primer lugar, los sistemas de AI conduzcan a resultados imprecisos, desleales, sesgados o discriminatorios para los consumidores, o, en segundo lugar, que los datos personales de los consumidores se difundan de manera incorrecta.

Estas protecciones propuestas en la AAA en algunos aspectos son protecciones ya implementadas en Europa bajo el RGPD. Aunque la AAA enfrenta perspectivas inciertas de convertirse en ley dadas las realidades políticas actuales, ofrece una visión de la posible regulación futura de EE. UU. de inteligencia artificial en el ámbito federal o estatal.

En resumen, tal y como manifiesta el estudio de Byungkwon y otros, ya citado[97], la proposición de ley de AAA, es un intento de implementar una supervisión más estricta de cómo los datos personales se almacenan, utilizan y analizan las empresas y otras entidades que tienen acceso a grandes volúmenes de datos del consumidor.

Aunque la AAA no prevé expresamente un derecho de acción privado, ni una jurisdicción extraterritorial, la FTC estaría obligada a implementar regulaciones que requieran que las entidades cubiertas realicen evaluaciones de impacto periódicas de los sistemas existentes de inteligencia artificial o sistemas de datos de consumidores considerados, ya sea por violaciones de

[96] http://www.worldcomplianceassociation.com/2336/noticia-se-presenta-en-los-estados-unidos-un-proyecto-de-ley-de-responsabilidad-algoritmica-algorithmic-accountability-act.html
[97] Ver nota 95

datos o por el uso de determinaciones algorítmicas que son potencialmente injustas o sesgadas[98].

En definitiva, los nuevos sistemas de inteligencia artificial o los sistemas de información considerados de "alto riesgo" requerirían una evaluación de impacto, en determinadas empresas que determina la ley[99]- y donde se incluye a los "data dealers" o a las empresas que posean datos de más de un millón de usuarios o de aparatos-, antes de su implementación para evitar posibles sesgos en su definición.

El senador Wyden, uno de los impulsores de la ley, indicó que los algoritmos están cada vez con mayor frecuencia involucrados en las decisiones más relevantes para la vida de las personas como comprar una casa, conseguir un trabajo o incluso ir a la cárcel. Pero con demasiada frecuencia estos algoritmos dependen de suposiciones o datos sesgados que en realidad pueden reforzar la discriminación contra las mujeres y las personas de color.

Y esta discriminación según otro de los impulsores de la ley, el senador Booker, puede ser hoy significativamente difícil de detectar, dando lugar a casas que nunca se sabe que están a la venta, a oportunidades de trabajo que nunca se presentan o a ofertas de financiación de las que nunca se tiene conocimiento, todo debido a algoritmos sesgados.

Por ello, según el senador Booker, la AAA exige que las empresas que utilizan software para tomar decisiones que pueden cambiar la vida de las personas, evalúen regularmente sus herramientas en cuanto a precisión,

[98] La AAA establece que "(C) an assessment of the risks posed by the automated decision system to the privacy or security of personal information of consumers and the risks that the automated decision sy tem may result in or contribute to inaccurate, unfair, biased, or discriminatory decisions impacting consumers"
[99] Artículo 5 de la AAA "Covered entity".

imparcialidad, parcialidad y discriminación, identifiquen los sesgos en estos sistemas y arreglen cualquier discriminación o sesgo que encuentren “Es un paso clave para asegurar una mayor responsabilidad por parte de estas entidades”.

Según la congresista Clarke, los algoritmos planteados seguramente no estarán exentos de leyes antidiscriminatorias americanas. La AAA reconoce que los algoritmos tienen autores, y sin una supervisión diligente, pueden reflejar los sesgos de los que están detrás del teclado. Al exigir a las grandes empresas que no hagan la vista gorda ante los impactos no deseados de sus sistemas automatizados, la AAA garantiza que las tecnologías del siglo XXI son herramientas de empoderamiento, en lugar de marginación, al tiempo que refuerzan la seguridad y la privacidad de todos los consumidores[100].

La AAA especifica que las evaluaciones de impacto deben realizarse, cuando sea posible, "en consulta con terceros externos, incluidos auditores independientes y expertos en tecnología independientes". Una vez que haya completado la evaluación de impacto del sistema de inteligencia artificial o del sistema de información, se requeriría a la empresa que “aborde razonablemente y de manera oportuna los resultados de las evaluaciones de impacto”.

La AAA inicialmente proyecta una amplia red de actividades dentro de su alcance. Define, en su artículo 1, al sistema de decisión automatizado como “a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that

[100] Información extraída de http://www.worldcomplianceassociation.com/2336/noticia-se-presenta-en-los-estados-unidos-un-proyecto-de-ley-de-responsabilidad-algoritmica-algorithmic-accountability-act.html

makes a decision or facilitates human decision making, that impacts consumers".

Esta definición incluiría una amplia gama de sistemas utilizados para procesar la información del consumidor, o para proporcionar servicios a los consumidores, o de cualquier otra forma que "afecte" a los consumidores. El proyecto de ley parece apuntar a casi cualquier tecnología computacional automatizada, no solo a aquellas en las que la inteligencia artificial en realidad toma una determinación, sino incluso a la llamada "inteligencia aumentada", donde un proceso informático sirve para ayudar y mejorar las determinaciones humanas[101].

Solo aquellos sistemas de decisión automatizados considerados de "alto riesgo" estarán sujetos a la evaluación de impacto requerida. La AAA define "sistema de decisión automatizado de alto riesgo" como uno que justifica un mejor control, ya sea porque los tipos de entradas de datos son particularmente sensibles o porque las salidas del sistema son especialmente importantes para los consumidores. Un sistema de decisión automatizado podría designarse como de alto riesgo en función de cualquiera de los siguientes criterios establecidos en el artículo 7 de la AAA:

"(A) taking into account the novelty of the technology used and the nature, scope, context, and purpose of the automated decision system, poses a significant risk—

(i) to the privacy or security of personal information of consumers; or

[101] BYUNGKWON Y OTROS. Supra

(ii) of resulting in or contributing to inaccurate, unfair, biased, or discriminatory decisions impacting consumers;

(B) makes decisions, or facilitates human decision making, based on systematic and extensive evaluations of consumers, including attempts to analyze or predict sensitive aspects of their lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements, that—

(i) alter legal rights of consumers; or

(ii) otherwise significantly impact consumers;

(C) involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;

(D) systematically monitors a large, publicly accessible physical place; or

(E) meets any other criteria established by the Commission in regulations."

Cualquier sistema de decisión automatizado de alto riesgo requeriría una evaluación de impacto para evaluar el proceso de desarrollo, el diseño y los datos de capacitación del sistema para "impactos en la precisión, imparcialidad, sesgo, discriminación, privacidad y seguridad"[102].

La AAA especifica, en su artículo 2, que la evaluación de impacto debe incluir:

[102] BYUNGKWON Y OTROS. Supra

- Una descripción detallada de la funcionalidad, el diseño, los datos de capacitación y el propósito del sistema;

- Una evaluación de costo / beneficio del sistema a la luz de, entre otros, su propósito prácticas de minimización de su transparencia para los consumidores y las oportunidades para que los consumidores corrijan u objeten sus resultados;

- Una evaluación de los riesgos de privacidad de datos;

- Una evaluación de los riesgos planteados por el sistema de decisión automatizado para la privacidad o seguridad de la información personal de los consumidores y los riesgos que el sistema de decisión automatizado puede resultar o contribuir a decisiones imprecisas, desleales, sesgadas o discriminatorias que afectan a los consumidores; y

- Un plan de seguridad tecnológica y física para minimizar los riesgos para la privacidad de los datos o los resultados automatizados dañinos.

Bajo la AAA, se requiere una "evaluación de impacto de protección de datos" para evaluar si un sistema de información de alto riesgo protege la privacidad y seguridad de la información personal almacenada o procesada por el sistema.

Aunque las evaluaciones solo se requerirán para los sistemas de información de alto riesgo, la AAA define "sistema de información" de manera muy amplia para incluir cualquier proceso, que no sea un sistema de decisión automatizado, que involucre información personal, incluyendo "recopilación, registro, organización, estructuración, almacenamiento, alteración,

recuperación, consulta, uso, intercambio, divulgación, difusión, combinación, restricción, borrado o destrucción de información personal."

10.2. El Reglamento General de Protección de Datos europeo.

La evaluación de impacto para la normativa europea es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos. Las evaluaciones de impacto, según la guía[103], son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento. En otras palabras, una evaluacón de impacto es un proceso utilizado para reforzar y demostrar el cumplimiento.[104]

Así, el considerando 84 del reglamento Europeo establece que "A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la

[103] Íbidem. Supra
[104] Información extraída de Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.".

El RGPD, tal y como expone la guía[105], requiere que los responsables del tratamiento apliquen medidas adecuadas para garantizar y poder demostrar el cumplimiento de dicho reglamento, teniendo en cuenta entre otros «los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas» (artículo 24.1 RGPD). La obligación de los responsables del tratamiento de llevar a cabo una evaluación de impacto en determinadas circunstancias debe entenderse en el contexto de su obligación general de gestionar adecuadamente los riesgos derivados del tratamiento de datos personales.

Un "riesgo" es un escenario que describe un acontecimiento y sus consecuencias, estimado en términos de gravedad y probabilidad. Por otra parte, la "gestión de riesgos" puede definirse como las actividades coordinadas para dirigir y controlar una organización respecto al riesgo.

El Article 29 working Party[106] indica en su guia de protección de datos[107], sobre la función de un enfoque basado en el riesgo de los marcos jurídicos

[105] Íb. Supra
[106] Article 29 Working Party es un grupo de Trabajo de la Comisión Europea, que trabaja independientemente, sobre todo lo relativo a privacidad y protección de datos. Todos los documentos, guías y opiniones de A29WP, sepueden encontrar en https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

sobre protección de datos, que la referencia a "los derechos y libertades" de los interesados atañe principalmente a los derechos a la protección de datos y a la intimidad, pero también puede implicar otros derechos fundamentales como la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión.

En consonancia con el enfoque basado en el riesgo introducido por el RGPD, no resulta obligatorio realizar una evaluación de impacto en todas las operaciones de tratamiento. Por el contrario, solo se requiere "cuando sea probable que un tipo de tratamiento [...] entrañe un alto riesgo para los derechos y libertades de las personas físicas" (artículo 35 RGPD, apartado 1). No obstante, el mero hecho de que las condiciones que dan lugar a la obligación de llevar a cabo una evaluación no se hayan cumplido no disminuye la obligación general de los responsables del tratamiento de aplicar medidas para gestionar adecuadamente los riesgos para los derechos y libertades de los interesados. En la práctica, esto significa que los responsables deben evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuando es probable que un tipo de tratamiento entrañe "un alto riesgo para los derechos y libertades de las personas físicas"[108]

[107] Disponible de manera traducida al español en https://www.aepd.es/media/criterios/wp248rev01-es.pdf (último acceso 1 de septiembre de 2019) aunque en la tesis se trabaja y se traduce por el autor siempre de la versión inglesa o francesa de todos los documentos.

[108] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Supra

11. Conclusiones.

I

Como mantengo en esta tesis, Internet, la conectividad móvil y su consecuencia, el Big Data es un fenómeno internacional, y así como Internet ha borrado las fronteras, también lo hace el Big Data y sus efectos en todo el mundo. Por tanto, la definición legal y doctrinal del Big Data debiera conceptualizarse como Universal –aunque reconozco que es utópico por el momento.

El concepto de Big Data y el tratamiento de datos (entendido como iguales) considero que no está correctamente planteado, al existir serias limitaciones en el planteamiento legal ya que se necesita una redefinición de los términos y un estudio riguroso ya que, el uso de Big Data, puede generar un uso irracional de la letra y el espíritu de las diferentes legislaciones aplicables al efecto, como el cambio de valores y los nuevos usos que requiera la sociedad.

Según Devins[109], que cita a otros autores[110], lo que ofrece el Big Data es, en muchos sentidos, opuesto a las tradiciones del Estado de Derecho.

[109] DEVINS Y OTROS. Law and Big Data. Ud supra

[110] ver GOODRICH, P "Rhetoric and Modern Law", in "The Oxford handbook of rhetorical studies" 613, 617–18 (Michael MacDonald ed., 2014) (exploring the limits of empirical data in the law); Ver HALE, SANDRA B."The discourse of court interpreting: discourse practices of the law, the witness and the interpreter" 4–8, 31–32 (2004), ASIM ZIA ET AL.,"The Prospects and Limits of Algorithms in Simulating Creative Decision Making"14 Emergence 89, 97 (2012) (discussing the limits of algorithms in interpreting affordances).

II

En mi opinión, el concepto que se establece en lo relativo al tratamiento de datos y sus finalidades es defectuoso por la misma razón que los esfuerzos para "diseñar" instituciones para cumplir objetivos predefinidos son defectuosos. Las finalidades son fundamentalmente creativas y evolutivas y, por lo tanto, evolucionarán inevitablemente de manera imprevisible, más allá de sus propósitos iniciales. Es lo que yo denomino la "viralización del Big Data" que comprende el uso indiscriminado de los datos para otras finalidades imprevisibles cuando inicialmente se establecieron o la reutilización de los datos.

Las partes involucradas en el tratamiento de datos, los interpretan y utilizan de formas novedosas para lograr sus propios objetivos y finalidades. Es necesario tener un "marco" o paradigma para interpretar estas posibilidades y determinar cuáles son relevantes o útiles en un contexto dado y si realmente el consentimiento efectuado -si es que realmente se dio- sirve para los propósitos de esas nuevas finalidades, objetivos, o su reutilización.

Esta problemática expuesta puede parecer muy alejada de la práctica del Big Data, particularmente en lo que se refiere a la ley, pero son muy pertinentes, ya que plantean preguntas sobre qué se puede establecer exactamente con los datos y el rol legislativo para orientar la observación y la recopilación y análisis de datos.

En mi opinión, tal y como se concibe el tratamiento de datos del Big Data, puede dar lugar a "monopolios sociales" donde determinados individuos sean los factores necesarios y desencadenantes de las decisiones que se tomen tanto por las administraciones como por el sector privado. Y los monopolios

no es algo que convenga a la sociedad en su conjunto ya que llevan a ineficiencias en el "mercado".

El análisis de lo expuesto en esta tesis lleva a concluir que, debido a la falta de regulación y a la falta de conceptualización del tratamiento del Big Data, se puede producir una falta de pérdida de igualdad social en determinados aspectos sociales y de mercado ya que para la toma de decisiones no se tienen en cuenta todas las variables reales que afectan a la decisión que se tomará en base a esos datos. Datos que, además, serán reutilizados creando aún más desigualdad por la desviación acumulada.

Y las personas tienen que tener derecho a saber cómo las partes del ecosistema -Gobierno, empresas- han utilizado sus datos -y cuales son estos- para tomar determinadas medidas. Es más, no sólo cómo se han utilizado sino de quién se han obtenido para saber que el tratamiento de datos ha sido justo y lleva a conclusiones y a políticas socialmente equitativas.

En mi opinión, el Big Data y el tratamiento de datos debieran formar parte de una misma definición. Los datos debieran ir asociados a su tratamiento. No cabe distinguir entre datos y su tratamiento ya que aquellos, sin el tratamiento, no son más que meros datos en bruto ajenos al control legal. La definición del Big Data debe ir unida a recopilación de datos y tratamiento; Un concepto que abarque las dos unidades legales.

III

El análisis del Big Data puede ser visto desde diferentes puntos de vista. En primer lugar hay quienes piensan que todo análisis de Big Data nos va a llevar al conocimiento de un mundo mejor; en segundo lugar hay quienes piensan de otra manera: que el análisis del Big Data plantea unos graves

problemas técnicos ya que la enorme cantidad de datos que existen hace muy difícil su tratatamiento y correcta utilización[111].

Pero lo que parece claro es que el Big Data puede llegar a transformar mediante el análisis de datos a la sociedad o a las personas y eso plantea unos dilemas éticos y morales muy importantes que no son objeto de esta tesis pero que deben ser tenidos en consideración ya que mediante el análisis de los datos se pueden llegar a percibir los comportamientos de las personas ya no son en el pasado sino en el futuro mediante algoritmos[112].

El Big Data puede traer importantes beneficios a la sociedad y a los particulares, pero también puede tener un impacto potencial en los derechos individuales y de libertad.

Las empresas que se dedican a la recolección masiva de datos, su transmisión instantánea y el uso de estos datos para propósitos que no están previstos en la normativa, han puesto a los principios de la protección de datos bajo unos nuevos parámetros. Hay que tener en cuenta estos nuevos contornos empresariales para fijar reglas éticas y morales relacionadas con el tratamiento de datos no solo el de transparencia, proporcionalidad y limitación en el propósito de tratamiento de datos, sino en los que se han venido conociendo como nuevos derechos como son la rendición de cuentas y la privacidad por diseño.

Las empresas tienen que ser mucho más transparentes en la forma en la que tratan la información personal; tiene que haber un mayor control sobre cómo

[111] PAGALLO, U. "The Legal Challenges of Big Data". (2017).

[112] Ver PAGALLO, U AND DURANTE,M. "The Pros and Cons of Legal Automation and its Governance" (2016) 7(2) European Journal of Risk Regulation 323-334.

se usan los datos; tiene que haber un buen diseño para proporcionar el derecho a la cancelación de los datos. En definitiva, una mayor transparencia en el uso de los datos y los algoritmos que rigen su tratamiento. Y más si tenemos en cuenta que ese tratamiento de los datos nos va a llevar a una predicción del comportamiento humano.

El Big Data, en su concepción legal, tiene que ser concebido siempre, por defecto, como una técnica que recoge y trata información personal privada o confidencial, aunque se hayan aplicado técnicas de anonimización[113].

El uso de Internet de las Cosas nos va a llevar a que cada vez haya una mayor información personal y confidencial sobre nosotros que esté disponible en el mercado para ser tratada por empresas y a poder predecir nuestro comportamiento sin que el consumidor sepa que sus datos personales están siendo tratados. Incluso podemos estar hablando de información sensible y confidencial cómo pueden ser datos de salud[114].

Consciente de ello la nueva directiva de protección de datos trata de regular todo el ciclo de la vida de los datos desde su recogida hasta su análisis y transformación o venta, pero lo hace de manera diferenciada.

La ley, en su concepción general de Teoría del Derecho, sirve para regular el comportamiento humano mediante unas técnicas. Sin embargo, en el Big Data, la ley no regula el comportamiento humano sino que regula una técnica que nada tiene que ver con el comportamiento humano sino con la innovación tecnológica y como esta innovación tecnológica puede llegar a afectar al

[113] EUROPEAN DATA PROTECTION SUPERVISOR. Meeting the challenges of Big Data .(2015)

[114] EUROPEAN DATA PROTECTION SUPERVISOR. Íb. Supra en 112

comportamiento humano y las diferentes relaciones humanas. Será pues una regulación por diseño[115] donde la ley tiene que tener muy claro el cómo y por qué se regulan estos comportamientos humanos[116] y la privacidad.

Las primeras tesis sobre la "privacidad por diseño" se expresaron en la década de 1970 y se incorporaron en la década de 1990 a la Directiva de protección de datos 95/46/EC. De acuerdo con el considerando 46 de esta Directiva, las medidas técnicas y organizativas deben tomarse ya al momento de planificar un sistema de procesamiento para proteger la seguridad de los datos.

El término "Privacidad por diseño" no significa nada más que "protección de datos a través del diseño de tecnología". Detrás de esto está el pensamiento de que la protección de datos, en los procedimientos de procesamiento de datos, se adhiere mejor cuando ya está integrada en la tecnología cuando se crea. Sin embargo, todavía hay incertidumbre acerca de lo que significa "Privacidad por diseño" y cómo se puede implementar. Esto se debe, por un lado, a la implementación incompleta de la Directiva en algunos Estados miembros y, por otro lado, a que el principio de "Privacidad por diseño" que se encuentra en el Reglamento general de protección de datos, que el enfoque actual en los datos pautas de protección, que requieren que las personas responsables ya incluyan definiciones de los medios para procesar los datos en el momento en

[115] PAGALLO,U. "On the Principle of Privacy by Design and its Limits: Technology, Ethics, and the Rule of Law" in Serge Gutwirth et al (eds), European Data Protection: In Good Health? (2012) 331-346; PAGALLO U, "Cracking down on Autonomy: Three Challenges to Design in IT Law'"(2012) 14(4) Ethics and Information Technology 319-328; y PAGALLO U, "Designing Data Protection Safeguards Ethically" (2011) 2(2) Information 247-265.

[116] PAGALLO, U. Íbidem supra en 114.

que se definan para cumplir con los principios y los requisitos de "Privacidad por diseño".

La legislación deja completamente abierta qué medidas de protección exactas deben tomarse. No se dan más detalles en el considerando 78 RGPD (que interpreta el artículo 25 RGPD) el cual establece que "La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos

desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

Además de los criterios nombrados, se debe considerar el tipo, el alcance, las circunstancias y el propósito del procesamiento. Esto debe contrastarse con las diversas probabilidades de ocurrencia y la gravedad de los riesgos relacionados con el procesamiento. El texto de la ley lleva a uno a concluir que a menudo se deben usar varias medidas de protección a la vez para satisfacer los requisitos legales, de conformidad con el artículo 25 RGPD. En la práctica, esta consideración ya se realiza en una fase temprana de desarrollo al establecer decisiones tecnológicas. La certificación reconocida puede servir como un indicador para las autoridades de que las personas responsables han cumplido con los requisitos legales de "Privacidad por diseño". Así, al seleccionar precauciones, se pueden usar otras normas, como las normas ISO. Al seleccionar en casos individuales, uno debe asegurarse de que se incluyen el estado de la técnica y los costos de implementación razonables.

IV

El Big Data tiene que ser un nuevo concepto legal. Tiene que ver con el Derecho a la privacidad y el Derecho a la protección de datos, pero no es lo mismo. Así, el Tribunal Constitucional alemán, el Tribunal Constitucional español, entre otros, han ido desarrollado la noción de lo que en derecho comparado se conoce como "autodeterminación informativa" que es derivada del principio constitucional de dignidad en Alemania y de intimidad en España, mientras que, en Francia, los tribunales han comenzado a aplicar los

derechos de protección de datos como un componente del derecho a la libertad[117].

Sin embargo, esta concepción legal está lejos de ser universal en todos los sistemas legales europeos, y está siendo expresado en términos bastante diferentes.

Yvonne McDermott[118] apunta que esta concepción legal se puede criticar, que nada aportaría al substrato legal ya que nos encontramos ante algo de naturaleza procesal, en la medida en que no representa directamente ningún valor o interés per se, ya que simplemente es para lograr el respeto de los valores incorporados en otros Derechos[119]. De lo expuesto hasta aquí se observa como la concepción jurídica del Big Data sí que importa.

V

El Big Data va de recolección y tratamiento de datos. De datos dispares entre si, pero que se tratan y se conectan para sacar unos resultados, predicciones, tendencias, rasgos, identidades o identificaciones.

Mientras que desde el punto de vista empresarial se ha visto como un elemento de "business inteligence", parece claro que, desde el punto de vista jurídico, en la medida que pueden afectar a derechos de las personas, no pueden ser tratados de igual manera que los datos empresariales.

[117] DE HERT Y GUTWIRTH, 2009, "Reinventing Data Protection?" Autoeditado.
[118] MCDERMOTT. Y, "Conceptualising the right to data protection in an era of Big Data". Disponible en https://journals.sagepub.com/doi/full/10.1177/2053951716686994.
[119] DE ANDRADE, N. (2012) Oblivion: The right to be different … from oneself. Reproposing the right to be forgotten. Revista de los Estudios de Derecho y Ciencia Política de la UOC 13: 122–137.

Para que el Big Data goce de entidad legal se tienen que dar dos elementos: Que sean individualizables en relación a una persona y que de los datos tratados, ya sea a través de ellos mismos o a través de agregación de otros, puedan ser interrelacionados para así inferir alguna caracterísitica que ataña a la personalidad, identidad, imagen o indentificación del sujeto para así, mediante diferentes técnicas, segmentarlo o individualizarlo y, mediante cualquier acción, intentar sugerir o modificar cualesquiera de los elementos configurativos de su personalidad, imagen o creencias, o de averiguar su indentificación única.

Esta definición tiene la ventaja de que el uso de Big Data para políticas públicas – dejando a un lado el debate de la posible marginación- quedaría al margen y sería posible, pero a la vez prevendría, contra posibles abusos de la Administración Pública.

En definitiva, a la definición de las 5 "V" del Big Data (que serviría desde el punto de vista empresarial) se debieran añadir las 3 "I": Individualizables, Interrelacionados y que tengan el propósito de Inferir.

CAPÍTULO III. DERECHO AL OLVIDO Y SU APLICACIÓN AL BIG DATA

I

El artículo 8 CEDF, un documento que constituye el derecho primario de la UE y tiene un valor fundamental en el orden jurídico de la UE, establece que:

"1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*

2. Estos datos se tratarán 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

(...)."

El derecho secundario de la UE, en particular el RGPD, en su artículo 17, ha establecido un marco legal que faculta a los interesados el otorgarles derechos con respecto a los controladores de datos. Además de los derechos de acceso y rectificación, el GDPR reconoce una serie de otros derechos, y entre ellos lo que el Reglamento llama "derecho de supresión", que no es otra cosa que el Derecho al Olvido.

El citado artículo 17 del RGPD establece que:

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

(...)"

II

El punto de partida, se da a partir de la legislación vigente. Pero el desarrollo tecnológico es tan rápido y discurre por unos caminos tan complicados que es

imposible abordar el asunto desde la perspectiva de una única legislación nacional, pues el mundo "virtual" no entiende de fronteras.

Proporcionar a los interesados el derecho a que se borren sus propios datos es particularmente importante para la aplicación efectiva de los principios de protección de datos que afectan a la personalidad, a la propia imagen, a la identificación y a la identidad y, en particular, el principio de minimización de datos (los datos personales deben limitarse a qué es necesario para los fines para los que se procesan esos datos).

1. Definición del Derecho al Olvido en Internet.

El Derecho al Olvido en Internet puede ser definido como aquel derecho, fundamental dicen algunos[120], que tienen las personas a que los enlaces que existen sobre ellas en los buscadores, que les perjudiquen y no sean pertinentes puedan ser retirados de Internet. Así mismo, habrá que entender que el Derecho al Olvido puede ser entendido de igual manera en relación a los datos individuales sobre los que trabaja el Big Data.

Hay que tener en cuenta que es posible encontrar resoluciones jurisdiccionales en diversos países sobre el «Derecho al Olvido», sobre todo

[120] GONZALEZ FUSTER, G."El nuevo derecho, por lo tanto, a pesar de ser reconocido formalmente como 'fundamental' por la Carta, no correspondía exactamente a la categoría clásica de derechos fundamentales entendida como afín a los derechos humanos, sino que subyacía ya en el mismo una especie de naturaleza híbrida, a medio camino entre los derechos humanos, por un lado, y los imperativos de libre comercio, por otro." "¿Un debate cada vez más fundamental o cada vez menos?". Revista Taleo número 97. Telefónica

en lo atinente a cuestiones penales[121], por lo que el Derecho al Olvido no se conceptúa como algo solo que ataña a Internet.

A la vista de esta definición, tenemos que tener en cuenta varias cosas:

a) Se trata siempre de enlaces, no de la información original.
b) Si hablamos de enlaces, la manera de encontrarlos es a través de buscadores de internet.
c) Que perjudiquen y no sean pertinentes, son dos conceptos subjetivos y ambiguos.

2. Los antecedentes del Derecho al Olvido.

Siguiendo a Orza Linares y Ruiz Tarrías[122], como antecedente más remoto, podemos encontrar que, ya en 1931, en el Tribunal de California se resolvió el caso denominado *Melvin v. Reid.* Se trataba de un asunto en el que la víctima, tras un pasado como prostituta y haber sido acusada de homicidio, había conseguido rehacer su vida, hasta que una película, realizada y exhibida por el demandado bajo el título «*The Red Kimono*» desveló su pasado, con su nombre real y le arruinó la vida. El Tribunal consideró que se había producido una lesión en su privacidad al traer de nuevo a la actualidad aspectos de la vida de la demandante que ya habían quedado olvidados[123].

[121] PACE, A. (1998) «El derecho a la propia imagen en la sociedad de los mass media» Revista Española de Derecho Constitucional, núm. 52, pags. 33-52.

[122] ORZA LINARES, RM, y RUIZ TARRÍAS, S .“Neutralidad de la red y otros retos para el futuro de Internet”.Conference.2011, Huygens Editorial. ISBN: 978-84-694-7037-4. Páginas 371 a 378.” El Derecho al Olvido en Internet”

[123] CORRAL TALCIANI, H. «Configuración jurídica del derecho a la privacidad II: Concepto y delimitación». Revista Chilena de Derecho, vol. 27 núm. 2, págs. 331-355.(2000)

Más recientemente, según los mismos autores, una primera respuesta legal a esta persistencia de los datos, con la aparición de los primeros ordenadores, fue la regulación de los derechos de acceso, rectificación y cancelación de los datos personales que pudieran constar en las bases de datos públicas o privadas[124].

De este modo, estos mismos autores consideran que el Derecho al Olvido era un simple derecho de cancelación de los datos[125], que presentaba muchas dificultades especialmente en lo que se refería a determinadas bases de datos que recogían datos de solvencia de los ciudadanos, como el caso del famoso RELI en España. Y siempre teniendo en cuenta que las bases de datos oficiales, en España[126], normalmente están excluidas de la regulación general y suelen presentar numerosas dificultades a la hora de cancelar o, simplemente, de rectificar los datos recogidos, aunque no siempre es así[127].

Observamos, por tanto, como el Derecho al Olvido se configura, por muchos operadores jurídicos, como una protección de los datos personales y lo que, en el mundo físico, puede que sea así, no lo es en el mundo de Internet; un mundo con sus propias reglas.

[124]Especialmente en lo que se refiere a las bases de datos de solvencia patrimonial, las primeras que fueronobjeto de una regulación específica. Cfr., entre otros, FERRANDO VILLALBA, Mª L. (2.000) "*La información de las Entidades de Crédito. Estudio especial de los informes comerciales bancarios" Valencia,Ed. Tirant lo Blanch; DUBIÉ, P. (2003) «Protección de datos y Derecho al Olvido», Derecho de los negocios, Año nº 14, Nº 154-155, págs. 1-16*

[125] GARRIGA DOMÍNGUEZ, A. (2004) Tratamiento de datos personales y derechos fundamentales. Madrid, Dykinson, pág. 40

[126] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. «BOE» núm. 298, de 14 de diciembre de 1999, páginas 43088 a 43099.

[127] El Tribunal Catalán de Contratos del Sector Público, por ejemplo, admite que con un correo electrónico del interesado se puedan modificar y cancelar determinados datos, de acuerdo con la Ley.

Sin embargo, hay que tenir en cuenta que uno de los rasgos estructurales del Derecho al Olvido en internet es que "no es una derivación de las garantías de privacidad/intimidad, sino que es una consecuencia de la idea de autodeterminación informativa (art. 18.4 CE y art. 8 de la carta de derechos de la UE) con perfiles por ello diferentes, concretados normativamente en las reglas en materia de protección de datos, a los habituales al resto de derechos de la personalidad del art. 18 CE: de ello se derivan consecuencias respecto del modo en que se relacionarán estas garantías con las libertades informativas"[128]

Google es el rey de las búsquedas (65,2% a nivel mundial en 2012 y del 95% en 2018). Cuando nos refiramos en el estudio a buscadores o a compañías de internet haremos referencia únicamente a Google, pero puede hacerse extensivo al resto de buscadores y compañías salvo que se diga otra cosa.

3. Conceptos asociados al Derecho al Olvido.

El problema con el Derecho al Olvido es que se mezclan diferentes figuras jurídicas haciendo, aún más difícil, la compresión global de la figura y la búsqueda de posibles soluciones; además hay que intentar definir estos conceptos, aunque sea de manera somera, para el correcto discernimiento del Derecho al Olvido digital.

[128] BOIX PALOP, A., «El equilibrio entre los derechos del artículo 18 de la Constitución, el "Derecho al Olvido" y las libertades informativas tras la sentencia Google», Revista General de Derecho Administrativo, 38, (2015)

3.1. La protección de datos.

En primer lugar tenemos el concepto de "protección de datos", un concepto desarrollado hace más de 4 décadas para favorecer la protección de las personas contra el uso inapropiado de la información tecnológica por el hecho de procesar información que les concierne.

La "protección de datos" pues, no fue diseñada para prevenir o limitar el uso de la tecnología informática, sino que se diseñó con la convicción de que la tecnología informática cada vez funcionaría de manera más extensiva y que ese funcionamiento tendría efectos sobre los derechos e intereses de las personas. En otras palabras, la protección de datos se refiere a los derechos e intereses de las personas y no a los datos concretos sobre dichas personas.[129]

3.2. La privacidad.

La privacidad es otro concepto que, relacionado con la protección de datos, tiene un impacto directo sobre el Derecho al Olvido. La privacidad es el respeto por la vida privada de cada uno y ese respeto conlleva la privacidad de los datos personales.

La privacidad de las personas tiene que ser entendida, debido a la fuerte carga ética que emana del concepto, como aquella figura jurídica que trata de evitar interferencias indebidas en asuntos privados así como de asegurar que

[129] HUSTINX. P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation"https://secure.edps.europa.eu/EDPSWEB/weBigDataav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf (última visita 28 de septiembre de 2018)

terceras personas no puedan efectuar un control sobre materias que pueden afectar a la persona y que menoscaban su dignidad y autonomía.

Hay que recordar, en este punto, la amplia diferencia del concepto de "privacidad" que existe entre Estados Unidos de América y Europa, ya que no existe una concepcón unitaria.

Mientras que en Europa, la jurisprudencia entiende la privacidad como una expresión de la dignidad que tiene todo ser humano por el hecho de existir – y por lo tanto se configura como un derecho sustantivo- la jurisprudencia de Estados Unidos de América entiende la privacidad como un mero control de la información personal y como una simple autonomía de decidir con quién compartes tu información personal.

La privacidad en Estados Unidos ha sido definida como "the right to be let alone"[130]. La privacidad es un derecho ante toda intromisión que no sea consentida.

La Cuarta Enmienda de la Constitución de Estados Unidos[131] tiene un alcance mucho más limitado que el derecho al respeto de la vida privada, tal como se

[130] SALDAÑA, M.N "The right to privacy. la génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de warren y brandeis". UNED. Revista de Derecho Político N.º 85, septiembre-diciembre 2012, págs. 195-240. A su vez, cita "De la extensa literatura estudiosa del célebre artículo, vid. BRATMAN, B. E. (2002). «Brandeis and Warren's "The Right to Privacy" and The Birth of The Right to Privacy», Tennessee Law Review, vol. 69, págs. 623-651; DREYFUSS, R.C. (1999). «Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore», Stanford Technology Law Review, Paper núm. 8, págs. 1-32; KRAMER, I. R. (1990). «The Birth of Privacy Law: A Century Since Warren and Brandeis», Catholic University Law Review, vol. 39, págs. 703-724; BARRON, J. H. (1979). «Warren and Brandeis, The Right to Privacy», 4 Harvard Law Review, 193 (1890): Demystifying a Landmark Citation», Suffolk University Law Review, vol. 13, págs. 875 y ss., GLANCY, D. J. (1979). «The Invention of the Right to Privacy», Arizona Law Review, vol. 21, núm. 1, págs. 1-39.

[131] El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosimil, estén corroborados mediante juramento

establece en el artículo 7 de la Carta de la de Derechos Fundamentales de la Unión Europea[132]. "Como resultado, la Cuarta Enmienda solo se aplica al contenido y no a otros datos en las comunicaciones -como la persona que llama, la hora y la ubicación-; y en principio, solo protege a los ciudadanos estadounidenses. Además, la información confiada a un proveedor de servicios ya no cuenta con su protección, mientras que el punto de partida en la legislación de la UE sigue residiendo en la confidencialidad de las comunicaciones."[133].

Según Bennet[134] "Estados Unidos ahora es la única democracia industrial avanzada que no ha aprobado un estatuto de protección de datos generalizado equivalente al modelo europeo y que se aplique a todo el sector privado, aunque el Estado de California ha legislado al respecto. El enfoque estadounidense ha sido gradual, inconexo, reactivo y totalmente consistente con un estilo de política pluralista y un marco constitucional fragmentado. El sistema político estadounidense tiende a no hacer muy bien regulaciones generales y anticipadas y quizás nunca lo pretendiera." Para continuar diciendo que "el panorama incompleto y fragmentado de la privacidad en EEUU es menos una cuestión de valores culturales o de imperativos constitucionales que la presión de los intereses comerciales sobre un Congreso fragmentado y el uso de un sistema de financiación política permisivo. Este sistema ha permitido un importante mercado de datos

o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargada

[132] Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

[133] HUSTINGS, P. "Restaurar la confianza al otro lado del Atlántico". Revista Taleo número 97. Telefónica.

[134] BENNETCOLLIN J. "Distintos intentos por camuflar las ineptitudes de la protección de la privacidad estadounidense". Revista Taleo número 97. Telefónica.

personales, no tolerado en ninguna otra parte y un conjunto de actores corporativos que no quieren ceder su ventaja económica en aras de la privacidad.

La profesora Saldaña[135] expresa que "Warren y Brandeis citan diferentes casos ingleses previos para demostrar que el common law había venido ofreciendo ya alguna protección frente a la publicación no consentida de diversos aspectos de la vida privada a través de la aplicación inadecuada del Derecho de propiedad intelectual y de la quiebra de confianza o de la buena fe de la teoría de los contratos, de ahí que el llamado «right to privacy» no fuese más que una aplicación de una regla ya existente" .

3.3. El Derecho a no ser encontrado.

El "derecho a no ser encontrado", a pesar de no ser ningún concepto jurídico es una definición que debería ser tenida en cuenta por el legislador.

Este derecho a no ser encontrado se enmarca dentro del derecho a la privacidad y, en concreto al derecho a la autodeterminación informativa personal.

Desde mi punto de vista, el derecho a no ser encontrado se confunde, con frecuencia, con el Derecho al Olvido y es utilizado, forzando la legalidad y la realidad de las cosas, por determinadas personas para forzar a los buscadores de internet a borrar sus datos.

[135] SALDAÑA, M.N. Íbidem. Supra

No es que se tenga que negar que exista apriorísticamente un derecho a no ser encontrado, todo lo contrario. Pero muchas veces la información que se intenta ocultar poco tiene que ver con las garantías que intenta establecer la legalidad en relación con el derecho de privacidad que todo ser humano, por el mero hecho de existir, debería de disfrutar.

3.4. *El Derecho a la información*.

El derecho a la información, corolario de la libertad de expresión, y que es tratado en diferentes partes de esta tesis, es algo que no puede ser soslayado en este estudio. Las administraciones púbicas de los países democráticos deben velar para que la información fluya de una manera efectiva, veraz y transparente ya que cumple un servicio de "watchdog"[136]. El derecho a la información es, pues, de interés público. Hay que concluir, en este aspecto, que se deberán ponderar cautelosamente los derechos en juego de las partes interesadas. Unos derechos que son muy difíciles de ponderar en el caso de las nuevas tecnologías ligadas a Internet ya que la legislación fluye de manera independiente a fronteras y legislaciones.

3.5. El derecho de cancelación y al bloqueo de datos personales.

El derecho de cancelación es uno de los derechos reconocidos a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que

[136] Véase por ejemplo, la sentencia del Tribunal Internacional de Derechos Humanos de Estrasbrugo asunto Sunday Times (n° 2) v. Reino Unido de 1991.

éstos se supriman cuando resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo.

Mientras en Europa es un Derecho reconocido, no siempre ocurre así en todas las diferentes jurisdicciones como la estadounidense donde solo la California Consumer Privacy Act (CCPA)[137], en el titulo 1.81.5, que entra en vigor el 1 de enero de 2020, parece reconocer específicamente este derecho (La CCPA lo definió como un derecho de "opt-out" fuertemente unido al derecho de bloqueo de datos).

El bloqueo de datos, consiste en su identificación y reserva con el fin de impedir su tratamiento, excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante su plazo de prescripción. Por tanto, no procede admitir un derecho de acceso durante el bloqueo de datos, ya que equivale a su cancelación.

En junio de 2010 la Unión Europea y los Estados Unidos de América firmaron un acuerdo relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo, comúnmente conocido como Acuerdo TFTP, que entró en vigor en agosto de ese mismo año. El objetivo principal de dicho acuerdo es ofrecer un marco legal para habilitar el intercambio de información entre Europa y los Estados Unidos en el contexto de la lucha contra el terrorismo.

[137] Disponible en https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Considerando el derecho que asiste a los ciudadanos en lo tocante a la posibilidad de acceder a sus datos personales y a rectificarlos en caso de que estos no sean corrector, los artículos 15 y 16 del acuerdo establecen un procedimiento para facilitar tanto el ejercicio del derecho de acceso como el de rectificación, además de la posibilidad de que estos sean eliminados o bloqueados para impedir el acceso a los mismos.

3.6. El Derecho de oposición.

El derecho de oposición reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

4. La autodeterminación informativa.

La RAE lo define como “poder de disposición y control que el titular de los datos personales ejerce sobre los mismos, consintiendo su tratamiento”; o no, podríamos añadir. Estamos, por tanto, ante derechos personalísimos que solo el titular, o tercero por delegación, pueden ejercitar.

Es un bien jurídico consistente en asegurar a las personas el control de la información y de los datos que en su caso les es propia para permitirles protegerse de los perjuicios derivados del uso por terceros, públicos o privados, de esa información o de esos datos. Las ilimitadas posibilidades que ofrece la tecnología han hecho imprescindible garantizar a los individuos instrumentos jurídicos que hagan posible ese control.[138]

El Magistrado del Tribunal Supremo Pablo Lucas Murillo[139] expone sobre la autodeterminación informativa que "Hablar del derecho a la autodeterminación informativa es hablar de la protección de los datos de carácter personal, del mismo modo que tratar de la protección de datos de carácter personal es tratar del derecho a la autodeterminación informativa. Hay, pues, plena coincidencia y la diferencia de denominaciones obedece a que una, la primera, acuñada por Alemania y utilizada por su Tribunal Constitucional Federal en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo, se fija en la principal facultad que encierra este derecho: la de que su sujeto, su titular, es decir, cualquier persona, decida, consienta de forma informada y libre el uso por terceros de datos que le conciernen. En cambio, la segunda denominación que, como veremos, es la acogida por la LOPD, por nuestro Tribunal Constitucional y por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, utiliza una expresión que pretende denominar el conjunto de medios jurídicos a través de los cuales se satisface aquella facultad. Personalmente, he preferido hablar de

[138]MURILLO DE LA CUEVA, L. "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad". Conferencia disponible en http://www.fcjuridicoeuropeo.org/wp-content/uploads/file/jornada15/1_LUCAS_1.pdf (último acceso 27 de agosto de 2019)

[139]MURILLO DE LA CUEVA, L. "El derecho a la autodeterminación informativa y la protección de datos personales" Bibid [1138-8552 (2008), 20; 43-58].

autodeterminación informativa porque, si bien se trata de una fórmula poco estética, es, sin embargo, más precisa pues apunta al núcleo del derecho, a su aspecto sustantivo, mientras que la protección de los datos personales es su manifestación instrumental y, por eso, tiene un carácter técnico que le priva de capacidad significativa. No obstante, como lo que realmente importa es el alcance efectivo de este derecho fundamental y, visto que no hay contradicción entre estas denominaciones, lo que procede es examinar los términos en los que se ha configurado efectivamente, dejando al margen las consideraciones nominales".

No puedo dejar estar en desacuerdo con lo expuesto por Lucas Murillo por lo que luego explicaremos. El concepto que autodeterminación informativa no es el medio instrumental para la protección de datos personales sino que es –tan solo mencionarlo en este momento- la expresión genuina de lo que yo concibo como el derecho a la configuración de la personalidad. No se trata tan solo de poder gestionar lo que la ley configura como datos personales.

4.1 La configuración del Derecho de autodeterminación informativa en diferentes legislaciones y tratados internacionales.

I

El derecho a la autodeterminación informativa es fruto de varios factores y antecedentes:

En el caso de las legislaciones internacionales, en 1974 se aprobó *The Privacy Act* de los Estados Unidos, y se fueron poniendo las bases de los principios esenciales configuradores del núcleo esencial del derecho a la

autodertminación informativa. En 1976 la Constitución de Portugal lo incorporó el derecho en el artículo 35. En 1978, al igual que a España con su Contitución, le tocó el turno a Francia con la publicación de la Ley de Informática, Ficheros y Libertades, a Dinamarca con las leyes sobre ficheros públicos y privados y a Austria con la Ley de Protección de Datos. Finalmente, en 1979 el Parlamento Europeo aprobó una resolución sobre la tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática[140].

Este derecho no se fundamenta en el derecho a la vida privada, sino, principalmente, "en los valores de libertad y dignidad humana en relación con el desarrollo de la personalidad"[141]

Los antecedentes, en Derecho Internacional comparado, del derecho a la autodeterminación informativa los podemos ubicar en diferentes instrumentos internacionales:

- La Declaración Universal de los Derechos del Hombre señala el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques.

- El Pacto Internacional de Derechos Civiles y Politicos señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su

[140] ORREGO, C.A "Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano" Anuario de derecho constitucional latinoamericano año XIX, Bogotá, 2013, PP. 311 a 330,

[141] AZURMENDI, A. "Por un «Derecho al Olvido» para los europeos: aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014". UNED. Revista de Derecho Político N.º 92, enero-abril 2015, págs. 273-310

domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

- La Convención Americana sobre derechos humanos señala que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

II

Sin embargo, a pesar de todos los antecedentes y factores acabados de exponer, es la Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, la que concibe el derecho de autodeterminación informativa al declarar que el libre desarrollo a la personalidad abarca "la facultad del individuo de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida". Aunque reconoció que tal "autodeterminación informativa" es limitable "en aras del interés preponderante de la colectividad, tuvo en cuenta la necesidad de protección especial cuando se trata de datos acumulados automáticamente, en los que lo decisivo no es tanto la clase de datos como "la posibilidad de utilización de los mismos".

Salvo en el caso de Portugal, ha entrado en el ordenamiento jurídico de la mano del legislador ordinario y de pronunciamientos judiciales y sólo recientemente ha recibido el estatuto de derecho fundamental.

En España el rango de derecho fundamental se lo ha dado el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, prácticamente al mismo tiempo que se aprobaba la Carta de los Derechos Fundamentales de la Unión Europea y que el Tribunal Europeo de Derechos Humanos dictaba

sus Sentencias más significativas al respecto -casos Amann contra Suiza y Rotaru contra Rumania- en el año 2000[142].

4.2. La configuración de la autodeterminación informativa en España

I

Sin embargo, en el ámbito español, el derecho a la autodeterminación informativa es algo que ha venido gestándose con el tiempo, desde la Sentencia del Tribunal Constitucional de 1985. Así tenemos que los antecedentes del derecho a la autodeterminación informativa en España son los siguientes:

II

a) Sentencia del Tribunal Constitucional 53/1985, de 11 de abril, donde se establece que:

"La doctrina ha puesto de manifiesto -en coherencia con los contenidos y estructuras de los ordenamientos positivos- que los derechos fundamentales no incluyen solamente derechos subjetivos de defensa de los individuos frente al Estado, y garantías institucionales, sino también deberes positivos por parte de éste (…)

(…)Por consiguiente, de la obligación del sometimiento de todos los poderes a la Constitución, no solamente se deduce la obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales, sino también la obligación positiva de contribuir a la

[142] MURILLO DE LA CUEVA, L. "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad". Conferencia disponible en http://www.fcjuridicoeuropeo.org/wp-content/uploads/file/jornada15/1_LUCAS_1.pdf (último acceso 27 de agosto de 2019)

efectividad de tales derechos, y de los valores que representa, aun cuando no exista una pretensión subjetiva por parte del ciudadano. Ello obliga especialmente al legislador, quien recibe de los derechos fundamentales "los impulsos y líneas directivas", obligación que adquiere especial relevancia allí donde un derecho o valor fundamental quedaría vacío de no establecerse los supuestos para su defensa"

En definitiva, el respeto a los derechos fundamentales de la persona (y en concreto, el derecho a la intimidad) no puede ser llevado a cabo por parte del Estado manteniendo una actitud pasiva o simplemente negativa, de no vulneración, sino que el Estado ha de desarrollar positivamente esos derechos, más aún cuando hay un mandato legal expreso, (el artículo 18.4 CE).

III

b) Auto del Tribunal Constitucional 642/1986, de 23 de julio,

Es la primera vez que se pronuncia sobre la relación entre la informática y la intimidad. Así el FJ 3 establece que:

"*El derecho a la intimidad, que ha tenido acogida explícita en la Constitución con el carácer de fundamental, parte de la idea originaria del respeto a la vida privada personal y familiar, la cual debe quedar excluida del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. En tal sentido, la Sentencia de este Tribunal 110/1984, tras aludir a las manifestaciones tradicionales de este derecho, en particular a la inviolabilidad del domicilio y de la correspondencia, se refiere a la extensión que ha experimentado la protección que de este derecho se deriva, como consecuencia de los avances de la técnica y del*

desarrollo de los medios de comunicación de masas, lo que obliga al «reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida".

Para continuar manifestando que en prinicipio, los datos relativos a la situación económica de una persona, y, entre ellas, los que tienen su reflejo en las distintas operaciones bancarias en las que figura como titular, entran dentro de la intimidad constitucionalmente protegida, no puede haberla tampoco en que la Administración está habilitada y que su uso más allá de lo legalmente autorizado podría constituir un grave atentado a los derechos fundamentales de las personas.

Tal y como manifiesta el Doctor Cuervo Álvarez[143] "En efecto, parece excesivamente restrictivo hablar del uso "legalmente autorizado" como criterio de medida de las violaciones del artículo 18.4 CE, pues en tanto esa ley no se dicte la protección no existiría. Sería más correcto hablar de uso "constitucionalmente autorizado", lo que permitiría el adecuado amparo de este derecho. Por otra parte, pese a la parquedad de las palabras, parece que el Tribunal Constitucional no identifica el artículo 18.4 con el artículo 18.1, aunque tampoco lo considera un derecho fundamental autónomo, nuevo."

IV

c) Sentencia Tribunal Constitucional 254/1993, de 20 de julio.

La sentencia 254/1993 del Tribunal Constitucional empezó a concretar el derecho a la autodeterminación informativa, al albur de una demanda contra

[143] CUERVO ÁLVAREZ, J.Blog de informàtica Jurídica. Disponible en http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/ (último acceso junio de 2019)

la petición denegada por la administración sobre la existencia, contenido y finalidad de ficheros automatizados de titularidad pública en los que constaban datos personales y sobre sendas decisiones judiciales que avalaban la actuación administrativa.

La sentencia resuelve favorablemente una demanda de amparo contra la denegación presunta por parte de la Administración Pública de información acerca de la existencia, contenido y finalidad de ficheros automatizados de titularidad pública en los que consten datos personales del actor y contra las dos decisiones judiciales que confirmaron aquella denegación. A juicio del actor, las resoluciones impugnadas vulneraron el derecho a la intimidad y la "libertad informática", garantizadas en los apartados 1 y 4 del artículo 18 de la Constitución respectivamente, al no dar satisfacción adecuada a su derecho a ser informado sobre esos ficheros automatizados que contienen datos personales que a él le conciernen. Este derecho, alega el actor, está recogido en el artículo 8, letras a) y b), del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Tal y como explica el Doctor Cuervo[144] el demandante pretende elevar este poder jurídico individual a derecho constitucional merecedor de amparo,

"En último término, el actor hace uso de la remisión del apartado 4 del artículo 18 CE como si ésta estableciera una reserva legal de desarrollo del derecho a la intimidad del artículo 18.1 CE, que se llena con el Convenio. Sin embargo, el TC en un primer momento concibe el artículo 18.4 CE como la sede de un derecho fundamental de configuración legal, lo que él llama la

[144] CUERVO ÁLVAREZ, J. Ud Supra

libertad informática, para acabar argumentando que esa libertad forma parte del contenido esencial de los derechos fundamentales del artículo 18.1 CE.

Los diversos planteamientos realizados sobre la STC 254/1993 suscitan tres cuestiones:

a) Alcance normativo del Convenio 108.

b) Aplicabilidad directa de los Derechos Fundamentales

c) El derecho a la intimidad y el derecho a la Autodeterminación Informativa."

A los efectos que interesan, es en el fundamento jurídico sexto donde se recoge como nuevo derecho la autodeterminación informativa al establecer que "*con independencia de esto, sin embargo, es lo cierto que los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en el Constitución, como hemos mantenido, en virtud del art. 10.2 CE, desde nuestra STC 38/1981, fundamentos jurídicos 3º y 4º. Es desde esta segunda perspectiva desde la que hay que examinar la presente demanda de amparo.*

Dispone el art. 18.4 C.E. 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". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos

fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

"Los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos. Este principio general de aplicabilidad inmediata no sufre más excepciones que las que imponga la propia Constitución, expresamente o bien por la naturaleza misma de la norma (STC 15/1982, fundamento jurídico 8º).

"no puede deducirse sin más (como hace el Abogado del Estado), que los derechos a obtener información ejercitados por el demandante de amparo no forman parte del contenido mínimo que consagra el art. 18 C.E. con eficacia directa, y que debe ser protegido por todos los poderes públicos y, en último término, por este Tribunal a través del recurso de amparo (art. 53 C.E.)."

"A partir de aquí se plantea el problema de cuál deba ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo.

"El uso de la informática encuentra un límite en el respeto al honor y la intimidad de la personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio

interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data).

En este sentido, las pautas interpretativas que nacen del Convenio de protección de datos personales de 1981 conducen a una respuesta inequívocamente favorable a las tesis del demandante de amparo. La realidad de los problemas a los que se enfrentó la elaboración y la ratificación de dicho tratado internacional, así como la experiencia de los países del Consejo de Europa que ha sido condensada en su articulado, llevan a la conclusión de que la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades."

"Toda la información que las Administraciones públicas recogen y archivan ha de ser necesaria para el ejercicio de las potestades que les atribuye la Ley, y ha de ser adecuada para las legítimas finalidades previstas por ella, como indicamos en la STC 110/1984, especialmente fundamentos jurídicos 3º y 8º, pues las instituciones públicas, a diferencia de los ciudadanos, no gozan del derecho fundamental a la libertad de expresión que proclama el art. 20 C.E. (STC 185/1989, fundamento jurídico 4º.4, y ATC 19/1993. Los datos que conservan las Administraciones son utilizados luego por sus distintas autoridades y organismos en el desempeño de sus funciones, desde el

reconocimiento del derecho a prestaciones sanitarias o económicas de la Seguridad Social hasta la represión de las conductas ilícitas, incluyendo cualquiera de la variopinta multitud de decisiones con que los poderes públicos afectan la vida de los particulares.

Esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios, impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente (STC 11/1981, fundamento jurídico 8º, y 101/1991, fundamento jurídico 2º).”

V

Para algunos autores, aunque yo no comparta esa opinión al igual que Villaverde Menéndez[145], se crea la “libertad informática” como un derecho fundamental autónomo[146].

[145] VILLAVERDE MENÉNDEZ, “Protección de datos personales, derecho a ser informado y autodeterminación informática a propósito de la STC 254/1993”, Revista de Derecho Constitucional, mayo-agosto 1994, pp. 189 a 223

[146] Ver GONZÁLEZ MURÚA, “Comentarios a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al art. 18.4 de la Constitución y la protección de datos personales”, Revista

Cuervo[147] afirma que "También podría entenderse que efectivamente el derecho a controlar los datos personales se deduce del apartado 4 del artículo 18 CE, pero que se trata de un derecho vinculado a la intimidad del artículo 18.1 CE en el que se integra como contenido positivo; o sea, el derecho a controlar los datos personales no tiene autonomía propia, pero se trata de un derecho que no cabe deducir de forma inmediata del artículo 18.1 CE, sino a través de una interpretación conjunta con el artículo 18.4 CE."

Desde mi punto de vista, el Tribunal Constitucional, con esta sentencia no está estableciendo el derecho fundamental de autodeterminación informativa, sino que habla de "libertad informática" – sin llegar muy bien a entender lo que eso signifcaba ya que por ejemplo, Internet no estaba disponible para fines comerciales y para hacer una captación masiva de datos- en el sentido del derecho a la privacidad y a la intimidad influenciados, y coincido con el Doctor Cuervo, en el sentido que le da la introducción de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[148], que expone que "La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática.

Vasca de Administración Pública, núm. 37; MURILLO DE LA CUEVA, L. "Informática y protección de datos personales", Madrid, 1993, p. 36).

[147] CUERVO ÁLVAREZ, J. Ud Supra en 142.

[148] BOE núm. 262, de 31 de octubre de 1992, páginas 37037 a 37045

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos."

Es cierto, y hay que decirlo, que esta exposición de motivos coincide con el sentido que el Tribunal Constitucional Alemán[149] señala como derecho de autodeterminación informativa, pero no es menos cierto que el Tribunal Constitucional, en aquellos años, no podía ser consciente de lo que significaría la "libertad informática" – ya que nadie lo sabía- y seguramente pensaba más en el uso de la informática por parte de las Administraciones Públicas para un fin determinado y sin tener en cuenta para nada el tratamiento masivo de datos.

VI

d) Sentencia del Tribunal Constitucional 143/1994, de 9 de mayo, en recurso de amparo interpuesto contra la Sentencia del Tribunal Supremo, que declaró la inadmisibilidad del recurso contencioso-administrativo formulado contra el Real Decreto 358/1990, de 9 de marzo, y contra la Orden de 14 de marzo de 1990, que regularon la composición y forma del NIF y la tarjeta acreditativa del mismo.

La demanda cuestionaba la legitimidad constitucional de una norma que, a través de un instrumento de recopilación de información, podía permitir un uso desviado de dicha información y, en consecuencia, la efectiva invasión de la esfera privada de los ciudadanos afectados.

[149] Sentencia de 5 de diciembre de 1983, citada anteriormente.

El Tribunal establece que "*es un hecho […] admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho".*

A su vez el Tribunal vuelve a reiterar en su fundamento jurídico séptimo que "*el derecho fundamental a la intimidad no agota su contenido en facultades puramente negativas, de exclusión*" señalando, en este mismo fundamento que "*un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta"*

Y continuaba estableciendo: En este marco destaca, en desarrollo del art. 18.4 C.E., la Ley Orgánica de 29 de octubre de 1992, de regulación del tratamiento automatizado de los datos de carácter personal, que aparte, de las reglas generales sobre tratamiento de datos que no vienen ahora al caso, establece normas específicas para restringir el defecto que la parte imputa a la norma reglamentaria impugnada. En concreto, garantizándose la seguridad de los archivos (art. 9), imponiéndose un deber específico de secreto profesional, incluso después de finalizadas sus tareas al respecto, al "responsable del fichero automatizado y (a) quienes intervengan en cualquier fase del

tratamiento de los datos de carácter personal" (art. 10) e impidiendo la transmisión de datos de carácter personal almacenados, con la excepción de que concurra el consentimiento del interesado, la autorización legal específica o la conexión y reconocida necesidad de la transmisión de datos para el logro de finalidades constitucionalmente relevantes (art. 11) en las condiciones dispuestas en la norma. Todas ellas como garantías para determinar el carácter proporcionado y razonable de la obligación de transmitir información fiscal puesto de manifiesto en la doctrina de este Tribunal (STC 110/1984, fundamento jurídico 4º).

VII

A mi entender, el Tribunal Constitucional sigue fundamentando en relación con el uso de la informática que hace la Administración Pública, sin ir más allá, tal y como se ha expuesto anteriormente.

VIII

e) Sentencia 11/1998 Tribunal Constitucional, de 13 de Enero.

En esta sentencia ya que se puede ver una perfilación de la doctrina del Tribunal Constitucional con un uso de la Informática, Internet y del uso del Big Data, tal y como lo entendemos hoy en día.

La sentencia fundamenta en relación a un uso indebido por la empresa de datos informáticos relativos a la afiliación sindical.

El Tribunal Constitucional viene a "1.o Reconocer al recurrente su derecho a la libertad sindical, art. 28.1 C.E en conexión con el art. 18.4 de la misma. 2.o Declarar la nulidad de la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid de 30 de junio de 1995, recaída en el recurso

de suplicación núm. 786/95. 3.o Declarar la firmeza de la Sentencia dictada por el Juzgado de lo Social núm. 25 de Madrid, de 7 de noviembre de 1994, en autos núm. 757/94."

En su Fundamento Jurídico 4ª expone que "*En lo que atañe a la queja constitucional relativa a la quiebra del derecho a la libertad sindical (art. 28.1 C.E.), debe indicarse, como ya se afirmó desde la STC 70/1982, que «el derecho a la libertad sindical que reconoce el art. 28 C.E. incluye como ``contenido esencial'' el derecho a que las organizaciones sindicales libremente creadas desempeñen el papel y las funciones que les reconoce el art. 7 C.E., de manera que participen en la defensa y protección de los intereses de los trabajadores», afirmándose en la STC 23/1983 que «por muy detallado y concreto que parezca el enunciado del art. 28.1 C.E. a propósito del contenido de la libertad sindical, no puede considerársele como exhaustivo o limitativo, sino meramente ejemplificativo, con la consecuencia de que la enumeración expresa de los derechos concretos que integran el genérico de libertad sindical no agota, en absoluto, el contenido global de dicha libertad».*

Por su parte, la STC 254/1993 declaró con relación al art. 18.4 C.E., que dicho precepto incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos (fundamento jurídico 6.o). La garantía de la intimidad, latu sensu, adopta

hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (fundamento jurídico 7.o).

Partiendo de estas premisas, en este caso debe tenerse en consideración que la afiliación del trabajador recurrente a determinado Sindicato, se facilitó con la única y exclusiva finalidad lícita de que la Empresa descontara de la retribución la cuota sindical y la transfiriera al Sindicato, de acuerdo con lo establecido en el art. 11.2 L.O.L.S. Sin embargo, el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al período de huelga."

Y en fundamento jurídico sexto expone que:

"*Establecidas estas consideraciones con relación a la libertad sindical (art. 28.1 C.E.), y a la protección de los datos informáticos (art. 18.4 C.E.), es procedente desde la perspectiva constitucional, situar correctamente la relación de los citados arts. 18.4 y 28.1, respecto de la libertad sindical.*

En efecto, el art. 18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en supuestos como el presente, el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical,

entendida ésta en el sentido que ha sido establecido por la doctrina de este Tribunal, porque es, en definitiva, el derecho que aquí se ha vulnerado como consecuencia de la detracción de salarios, decidida por la empresa al trabajador recurrente por su incorporación a determinado Sindicato.

En suma, ha de concluirse que tuvo lugar una lesión del art. 28.1 en conexión con el art. 18.4 C.E. Éste no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona --a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal-- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical."

Para añadir más tarde, en el Fundamento Jurídico sexto que

"*En este caso la vulneración de derechos fundamentales no queda supeditada a la concurrencia de dolo o culpa en la conducta del sujeto activo, a la indagación de factores psicológicos y subjetivos de arduo control.*

Este elemento intencional es irrelevante y basta constatar la presencia de un nexo de causalidad adecuado entre el comportamiento antijurídico y el resultado lesivo prohibido por la norma."

IX

Interesa resaltar en esta Sentencia que se establece una garantía de la dignidad frente a la libertad informática proveniente de un uso no legal de datos, ya que esa libertad informática comporta que el ciudadano se pueda oponer a que determinados datos personales sean utilizados para fines distintos del legítimo que justificó su obtención, tratando de evitar que la informatización de los datos personales propicie comportamientos discriminatorios

La segunda cosa que destaca en esta sentencia, es la coincidencia del término privacidad con el término de autodeterminación informativa, cosa que yo no comparto pues ésta tiene muchos más matices que aquella y se fundamenta en diferentes valores tal y como observa – y yo comparto- la profesora Azurmendi[150], como se ha visto anteriormente.

X

f) Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre.

Para la expresidenta del Tribunal Constitucional, Dña. María Emilia Casas[151] especial interés ofrece la STC 202/1999, de 8 de noviembre, que otorgó el amparo solicitado por el trabajador frente a otras sentencias que le habían denegado la cancelación de sus datos médicos contenidos en un fichero informatizado sobre bajas por incapacidad temporal de su empresa

La expresidenta del TC expone que "Es la primera Sentencia del Tribunal sobre el "Derecho al Olvido", que, sin denominarlo así, apreció la

[150] AZURMENDI, A. Íbidem. Supra en 140
[151] CASAS BAAMONDE, M. E. "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional" Conferencia en XXI Congreso Nacional de Derecho Sanitario.

vulneración del derecho a la intimidad del trabajador causado por el almacenamiento en soporte informático de sus diagnósticos médicos del trabajador, sin mediar su consentimiento expreso y sin apoyo legal".

La Sentencia expone en su Fundamento Jurídico Segundo que "*la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC* 254/1993, fundamento jurídico 7º; 11/1998, fundamento jurídico 4º, y 94/1998, fundamento jurídico 4º)*"*

En su Fundamento Jurídico Cuarto, la sentencia refiere que el fichero informatizado, cuya cancelación en lo concerniente a sus datos sobre baja con diagnóstico médico solicitaba el trabajador, no era un compendio de historiales clínico-sanitarios, sino una relación de partes de baja con anotación de las correspondientes fechas de baja y alta laboral, el motivo de la baja, los días durante los cuales se prolongó la situación de baja y el diagnóstico médico. Su mantenimiento no se dirigía a la preservación de la salud de los trabajadores, sino al control del absentismo laboral, por lo que no encontraba apoyo en "*la existencia de un interés general (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados*

arrojados por la vigilancia periódica --y consentida por los afectados-- del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral, sino tan sólo la relación de períodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador".

La Sentencia del Tribunal Constitucional fundamenta que las facultades del poder de dirección empresarial no comprenden el almacenamiento en soporte informático de los datos de salud de los empleados y en concreto del diagnóstico médico, sin su consentimiento, concluyendo en su Fundamento Jurídico quinto que "*tal medida no tenía "la consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral […], pues no se trata de medida de suyo ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad*"

Así mismo, la sentencia expone que "*interesa recordar que, en desarrollo de lo previsto en el art. 18.4 C.E., en la L.O.R.T.A.D. se enuncian, entre otros principios generales de la protección de datos, la congruencia y racionalidad de su utilización, "en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y, en consecuencia, prohíbe tajantemente el uso de los datos para finalidades distintas de las que motivaron su recogida (aps. 1 y 2 del art. 4)" (STC 94/1998*, f*undamento jurídico 4º), así como su exactitud y puesta al día (art. 4.3). Esta regulación es sustancialmente coincidente con lo dispuesto en los arts. 5 y 7 del Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de personas con respecto*

al tratamiento automatizado de datos de carácter personal, ratificado por España mediante Instrumento de 27 de enero de 1984, y en los arts. 6 y ss. de la Directiva 95/46/CE, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Pues bien, en este caso debemos afirmar que el expresado tratamiento informático --con vistas a su conservación-- de los datos referidos a la salud de los trabajadores de que tenga conocimiento la empresa quiebra la aludida exigencia de nítida conexión entre la información personal que se recaba y el legítimo objetivo para el que fue solicitada"

(…) "*el tratamiento y conservación del diagnóstico médico en la mencionada base de datos sin mediar consentimiento expreso del afectado incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 C.E." (FJ 5).*

En el punto tercero del fallo, la Sentencia restablece al recurrente en el derecho vulnerado, ordenó la inmediata supresión de las referencias existentes a los diagnósticos médicos contenidas en la citada base de datos

(…) "*el tratamiento y conservación del diagnóstico médico en la mencionada base de datos sin mediar consentimiento expreso del afectado incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 C.E." (FJ 5).*

En el punto tercero del fallo, la Sentencia restablece al recurrente en el derecho vulnerado, ordenó la inmediata supresión de las referencias existentes a los diagnósticos médicos contenidas en la citada base de datos.

En ejecución de la STC 202/1999, la posterior STC 153/2004, de 20 de septiembre, volvería a amparar al recurrente, en este caso ulterior por

vulneración de su derecho fundamental a la tutela judicial efectiva, al haberle sido denegada la prueba pericial solicitada para comprobar la supresión de la referencia a los diagnósticos médicos del mismo en fichero informatizado o base de datos de la empresa.

XI

g) Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre

La STC 290/2000 resolvió cuatro recursos de inconstitucionalidad, acumulados, planteados contra determinados artículos de la, hoy derogada, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[152].

El recurso de inconstitucionalidad del Consejo Ejecutivo de la Generalitat de Cataluña oponía, en esencia, que la ley recurrida vulneraba el orden constitucional de competencias al atribuir al Estado competencias exclusivas en la ejecución de dicha Ley Orgánica sobre todos los ficheros de datos de titularidad privada y aquellos otros creados por la Administración Local, reservando a las Comunidades Autónomas únicamente competencias respecto de los ficheros creados por sus propias Administraciones y desconociendo las competencias autonómicas sobre las materias o actividades a que servían los ficheros de datos. Consideraba inconstitucional la reserva de competencias ejecutivas a la Agencia de Protección de Datos, frente al tratamiento informático de sus datos de carácter personal, reivindicando sus competencias ejecutivas y de tutela administrativa sobre los ficheros de datos de carácter personal privados y de las Administraciones Locales en Cataluña.

[152] BOE núm. 262, de 31 de octubre de 1992, páginas 37037 a 37045

La sentencia del Tribunal Constitucional reconoce que el derecho a la protección de datos de carácter personal es un nuevo derecho fundamental, declarandando su contenido esencial, No es sólo una primigenia garantía del derecho a la intimidad, sino un derecho fundamental autónomo a la protección de datos de carácter personal.

El art. 18.4 CE, "*como ya ha declarado este Tribunal, contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que es, además, en sí mismo, "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama 'la informática'" (STC 254/1993, de 20 de julio, FJ 6, doctrina que se reitera en las SSTC 143/1994, de 9 de mayo, FJ 7; 11/1998, de 13 de enero, FJ 4; 94/1998, de 4 de mayo, FJ 6, y 202/1999, de 8 de noviembre, FJ 2) (FJ 7).*

Ese derecho fundamental a la protección de datos personales frente a la informática o, si se quiere, a la "libertad informática" según la expresión utilizada por la citada STC 254/1993, garantiza a la persona un poder de control y disposición sobre sus datos personales, que se descompone en un haz de facultades, como elementos esenciales del derecho, "integrado por los derechos que corresponden al afectado a 1) consentir la recogida y el uso de sus datos personales y a conocer los mismos. 2) ser informado de quién posee sus datos personales y con qué finalidad; y 3) a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos".

En su Fundamento Jurídico Séptimo expone que "*En suma, 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 del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes"* .

En efecto, al dar cumplimiento al mandato contenido en el art. 18.4 CE, el legislador, no se había limitado a residenciar la protección de datos personales frente al uso de la informática exclusivamente en la vía judicial, cuando ya se ha producido la lesión del derecho fundamental, sino que había configurado esa protección con carácter preventivo mediante el ejercicio por la Agencia de Protección de Datos de sus funciones de control y atención de reclamaciones de los afectados. De suerte que, según explicaba el Tribunal Constitucional, precisamente ese carácter tuitivo o preventivo justificaba en su Fundamento Jurídico Noveno "*la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada*"

Interesante es, a los efectos, el Fundamento Jurídico decimo primero que fundamenta que (…) "*El bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales*

de los ciudadanos o afectar al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional" es establecer un régimen legal para "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de datos de carácter personal" "*la Ley que ha desarrollado un derecho fundamental específico, el derecho a la protección de los datos personales frente al uso de la informática […]. De lo que se desprende, en definitiva, que el objeto de la Ley cuyos preceptos se han impugnado no es el uso de la informática, sino la protección de los datos personales. De suerte que esta protección mal puede estar al servicio de otros fines que los constitucionales en relación con la salvaguardia de los derechos fundamentales, ni tampoco puede ser medio o instrumento de actividad alguna".*

XII

Casa Baamonde[153] expone que, las conclusiones alcanzadas por el Tribunal en este orden de consideraciones de tipo competencial fueron éstas:

1ª) Los límites establecidos por el legislador al uso de la informática en cumplimiento del mandato del art. 18.4 CE han de ser los mismos en todo el territorio nacional en virtud del art. 81 CE:, Tal y como indica el fundamento jurídico decimo cuarto, "sólo mediante esa proyección general es posible garantizar la protección de los derechos a que se refiere el art. 18.4 CE, con independencia de que tales límites a la informática también contribuyen a la salvaguardia del específico derecho fundamental a la protección de datos personales"

[153] Íb. Supra

2) Tal y como dice el fundamento jurídico decimo quinto de la Sentencia, "es la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute" la que justifica el ejercicio de las funciones y potestades de la Agencia de Protección de Datos y del Registro Central de Protección de Datos, que quieren evitar que se vulneres derechos fundamentales, en cualquier lugar del territorio nacional sin importar quiénes son los responsables de los ficheros que contengan datos de carácter personal.

XIII

Continúa Casas Baamonde[154] exponiendo que la STC 292/2000 ha introducido ciertos matices nuevos que definen el contenido del derecho y su reconocimiento como tal en el art. 18 CE. Así:

- El derecho fundamental a la intimidad, los derechos fundamentales mencionados en el art. 18.1 de la Constitución, no están adaptados a la realidad tecnológica actual o futura, por más que el legislador fuese consciente de que la tecnología iba a comportar ciertos riesgos para las personas en cuanto a sus derechos, disminuyéndolos en su intensidad, tal y como muestra el fundamento jurídico cuarto.

- El fundamento jurídico quinto de la sentencia expone como, los derechos fundamentales a la intimidad y a la protección de datos de carácter personal, que comparten "el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar" se diferencian por su función, por su objeto y por su contenido: "el derecho a la intimidad garantiza "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los

[154] Íb. Supra en 150

demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 209/1988, fundamento jurídico 3º); el derecho a la protección de datos personales no garantiza el poder de resguardar la propia vida, sino un poder de disposición sobre los datos personales, "sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", que "impone a los poderes públicos la prohibición de que se conviertan en fuentes de […] información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información" (FJ 6). Por lo demás, los datos personales no son solo los relativos a la intimidad, sino a los bienes de la personalidad que pertenecen al ámbito de la vida privada y están indisolublemente unidos a la dignidad personal. "

Y continúa diciendo que "Así, el objeto de protección de este derecho fundamental son los datos personales, sean o no íntimos. "El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado" (FJ 6) También alcanza a los datos personales públicos: "los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo" (FJ 6)."

- De conformidad con el fundamento jurídico sexto, el derecho fundamental a la protección de datos atribuye a su titular "diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos" de hacer: "el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos". Así, "en definitiva, el poder de disposición sobre los datos personales faculta a la persona para decidir qué datos personales proporciona a un tercero, sea el Estado o un particular, qué datos personales puede ese tercero recabar, permitiéndole saber quién posee esos datos personales y para qué y oponerse a esa posesión o uso: "Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos" ".

- Para acabar, la sentencia del TC declara la inconstitucionalidad y nulidad de la expresión "interés público", del art. 24.2 LOPD, "como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de

intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE".

5. Una nueva forma de conceptuar jurídicamente la privacidad.

I

Tal y como expresa la profesora Azurmendi [155] "una de las primeras consecuencias del ejercicio del derecho de autodeterminación informativa es una protección más efectiva frente al riesgo que supone para la libertad de los individuos el enorme poder de información acumulado por las empresas de Internet. Un poder que básicamente consiste, por un lado, en su capacidad de predecir los comportamientos de millones de personas —previo conocimiento, durante años, de sus intereses, de sus comunicaciones personales, de sus intercambios de opiniones, sus sites favoritos, sus acciones profesionales, sus compras online, sus fotografías, las que de otros han publicado de ellas, y miles de cuestiones más-. Y, por otro lado, en la generación de unas identidades digitales que acompañen de por vida a los ciudadanos, determinando en muchos casos decisiones de su entorno profesional, personal, etc. Éste es el horizonte protegible de las nuevas versiones del derecho a la privacidad"

Realmente el concepto de privacidad tiene que ser redefinido a la luz del Big Data que viene a dar un vuelco jurídico a dicho concepto a la luz de lo aquí estudiado y de la conceptualización de lo que tiene que ser el Derecho al Olvido a la vista de la autodeteminación informativa.

[155] Íbidem. Supra en 140.

La privacidad a la luz de los tratamientos algorítmicos e interrelaciones y extrapolaciones que es capaz del realizar el Big Data, necesita ser redefinida jurídicamente.

El concepto de privacidad parece estar concebido sin tener en cuenta la realidad – paralela o no- que impone el mundo de Internet y la conexión de datos en el sentido tanto de su acaparamiento masivo e inconsciente como de su mismo tratamiento masivo.

Hoy en día es imposible desligar la identidad digital de la física. No estamos hablando de una realidad paralela o ficticia creada por en una red social (aunque quién sabe si esa realidad paralela o ficticia es la personalidad real, mostrada o latente, de la persona) sino que hablamos de los datos que emitimos como personas- sea en forma de palabras, localizaciones, interacciones, etc- y que muestran y demuestran nuestra verdadera personalidad entendida como la forma de pensar, actuar y vivir.

La privacidad, entendida desde el punto de vista tradicional, se basa en el derecho al respeto a la vida privada de las personas a partir de la obtención y análisis de un dato o unos pocos datos.

En nuestra opinión, dos elementos nuevos surgen a la hora de concebir un nuevo derecho a la privacidad que tenga en cuenta el derecho a la propia imagen, a la identidad y que no menoscabe el derecho a la libre manifestación de la personalidad.

En primer lugar, debe tener en cuenta la obtención y tratamiento masivo de datos y la posible interrelación entre los diferentes tipos de datos que conlleva el Big Data.

Unos datos, en bruto o en sí mismos -de manera semiestructurada-, puede que no revelen nada sobre la privacidad de una persona. Pero estos mismos datos, por su interrelación, anexión o correlación a otros, puede que sí que revelen la identidad o aspectos de la personalidad de una persona. Y eso, el responsable del tratamiento tiene que saberlo y debería advertirlo al emisor primigenio de los datos para que lo sepa.

En definitiva, en la categoría de datos personales no debe observarse sólo si estos lo son netamente, sino que debe observarse si unos datos no personales o privados, debidos al uso del Big Data, se convierten o pueden convertir en personales o privados.

En segundo lugar, la privacidad en concepto clásico se relaciona siempre con la persona. Pues bien, la nueva privacidad tiene que ser entendida no solo con la persona, sino también con la personalidad, concepto éste íntimamente unido al concepto de persona – y de su dignidad por tanto- pues manifiesta el modo de vivir, pensar o actuar.

En tercer lugar, con las dificultades que esto entraña, la privacidad debe tener una concepción global como elemento más íntimo de la persona; de su manera de ser. No se puede entender la privacidad en unas jurisdicciones de una manera diferente que en otras, o de maneras diferentes. La persona, por el simple hecho de serlo, tiene el derecho inalienable a la privacidad.

En cuarto lugar, y consecuencia de todo lo anterior, el titular del derecho debiera disponer de la posibilidad de ejercitar convenientemente el Derecho al Olvido sobre sus datos personales. Puede ser que el titular, dadas determinadas circunstancias de la vida, desee que sus datos personales -originarios o aquellos que se han convertido en personales- desaparezcan o no

sean tratados. Y tiene derecho a ellos pues son manifestación directa de su personalidad.

La privacidad, entendida de manera clásica, observa este derecho como algo de, más o menos, fácil ejecución por la razón expuesta al principio de que tiene en cuenta que son pocos datos o de fácil localización o que son pocos los que tratan los datos.

Pues bien, hoy en día, eso no es así. Son ingentes cantidades de datos, de la más diversa naturaleza y están desperdigados por muchas partes.

El legislador, al menos el internacional, debiera tener en cuenta ésta y todas las consideraciones anteriores.

6. El tratamiento sobre datos personales en los tratados y convenios internacionales.

6.1 Declaración Internacional de Derechos Humanos.

El artículo 12 de la Declaración Internacional de Derechos Humanos[156] establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

[156] Asamblea General de las Naciones Unidas, París 1948.

Lo más importante de este artículo 12 es que pone el foco en la "vida privada" y en la privacidad, ya que el "domicilio" y la "correspondencia" se encontraban ya en las construcciones jurídicas de muchos países.

6.2. La Convención Europea de Derechos Humanos

El artículo 8 de la Convención Europea de Derechos Humanos[157] establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

6.3. Comentarios a los Tratados anteriores.

Aunque estos dos Tratados fueron muy novedosos y necesarios, se han quedado anticuados.

No se preveía de ninguna manera el tratamiento masivo de los datos, ni la irrupción de internet.

Pero lo más significativo es que el concepto de "vida privada" que es un concepto indeterminado y más o menos amplio según la normativa de cada

[157] Council of Europe, Roma 1950.

país. Pero es de fundamental importancia y el Tribunal Europeo de Derecho Humanos se inclina a entender la "vida privada" en consonancia con el art 8 de la CEDH.[158]

Tampoco se podía prever la hiperactividad que desarrollan las autoridades públicas en el tratamiento de datos. Datos que muchas veces se publican en Internet, los buscadores recogen y ciertos particulares quieren borrar.

Pero la culpa de esa hiperactividad no la tienen solo las autoridades públicas, que en sociedades democráticas y libres tienen todo el derecho a tratar los datos de la manera que estimen pertinente en aras de la consecución de las actividades que la administración pública tiene encomendada.

La principal culpa es de algunas empresas privadas que hacen un mal uso de la información de que disponen y que quieren explotar económicamente. Información, por otro lado, que muchas veces el propio particular ha cedido como fotos o comentarios en determinadas redes sociales o al aceptar aplicaciones del teléfono móvil que muestran nuestra geolocalización, las tiendas a las que vamos o nuestras preferencias.

De hecho, el Consejo de Europa ya se dio cuenta de que el artículo 8 de la Convención Europea de Derechos Humanos se encontraba desfasado pues "el poder de la información", y los datos que se manejan, es enorme[159].

[158] Ver , por ejeplo, las sentencias Klass vs Germany, ECHR (1978), A-28; Malone vs United Kingdom, ECHR (1984), A-82; Leander vs Sweden, ECHR (1987), A-116; Gaskin vs United Kingdom, ECHR (1989), A-160; Niemietz vs Germany, ECHR (1992), A-251-B; Halford vs United Kingdom, ECHR 1997-IV; Amann vs Switzerland, ECHR 2000-II, y Rotaru vs Romania, ECHR 2000-V.

[159] Explanatory report to Convention 108. http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm (última visita 30 de septiembre de 2018)

De la misma manera, el Consejo de Europa certifica que no hay una normativa clara en los países para proteger los derechos de las personas en este campo y en particular "*on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others.*"[160].

Hay que resaltar el hecho de que el Consejo de Europa es consciente de que siempre se debe aplicar la misma ley para todos los ciudadanos, con independencia de donde se produzca el tráfico de datos. El CdE entiende que no puede ser que haya una protección diferente para las personas en función del país donde vivan.[161]

Y, en un paso más allá, los tribunales franceses han entendido que la protección de datos personales, y en especial el Derecho al Olvido, se tiene que aplicar a una persona en todo el mundo[162] y no sólo en el territorio de su jurisdicción. De esta manera, los límites de lo que se considera "vida privada" aumentan su alcance tanto en su aspecto nominativo como de localización.

Así, el concepto de vida privada ya no se limita a situaciones íntimas, sino a situaciones de la vida profesional o de comportamiento, con independencia de cuando se produjeron[163].

Y creemos que hay que de insistir en una idea. No sólo estamos hablando de "datos sensibles" como datos médicos o cuentas bancarias. Estamos hablando de fotos colgadas en redes sociales, comentarios en blogs, noticias sobre nuestra vida profesional, datos de localización, preferencias, etc; en

[160] Supra. Council of Europe, Roma 1950.Párrafo tercero.
[161] Supra. Council of Europe, Roma 1950.Párrafo noveno.
[162] http://www.elconfidencial.com/tecnologia/2014-09-30/primera-sancion-a-google-por-no-aplicar-el-derecho-al-olvido-en-todo-el-mundo_218178/ (última visita 1 de octubre de 2018)
[163] Ver nota 9.

definitiva, datos que nosotros libremente hemos consentido su cesión u obtención.

A la vista de lo anterior hay que entender que se le está imponiendo a los buscadores, y en este caso a Google, una obligación desmesurada al ser considerado responsable del tratamiento en virtud del RGPD. Una obligación que seguramente no se habría impuesto a otras empresas con otro tipo de productos. No creemos que Google debiera ser responsable sobre una foto que nosotros colgamos en una fiesta o sobre una insolvencia que tuvo nuestra empresa en un determinado momento.

Los buscadores, no son los poseedores de esa información. Solo indexan lo que otros cuelgan. No se inventan nada. Solo procesan. Quizás el problema radique en la manera en cómo procesan, pero eso es un secreto comercial, al igual que la fórmula de la Coca Cola.

Pero efectivamente, es que Internet, es un ente global y no local. Y las cuestiones que le afectan, necesitan ser abordadas de una manera que hasta ahora no se ha hecho.

6.4 El Convenio 108 del Consejo de Europa para la Protección de Datos Personales.

El Convenio 108 del Consejo de Europa[164] tiene por objeto limitar de manera estricta la posibilidad de desligarse de la aplicación de las normas de protección de datos, de conformidad con los principios enunciados en el Convenio Europeo de Derechos Humanos, ya que la privacidad de cada

[164] Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de caràcter personal, Estraburgo,28 de enero de 1981,ETS 108.

individuo, y en especial el procesamiento de datos que le conciernen, debe mantener con independencia de las fronteras[165]

Desde nuestro punto de vista, es muy importante el hecho de que está abierto a países de fuera de la Unión Europea. Hasta el momento, lo han ratificado 46 estados[166].

En Convenio 108 recuerda que el derecho a la protección de los datos personales constituye también una condición previa para el ejercicio de otros derechos fundamentales, tales como la libertad de expresión y la libertad de conciencia.

En definitiva, la Convención 108 establece que[167]:

a) Los datos deberán obtenerse y utilizarse con una finalidad determinada y no deberán volver a utilizarse con un objetivo no relacionado;
b) Sólo deberán ser almacenados y tratados los datos estrictamente necesarios para esta finalidad;
c) Los datos tratados deberán ser exactos y estar actualizados;
d) Los datos deberán conservarse únicamente por el tiempo necesario para cumplir la finalidad para la cual se hayan registrado;

De igual manera, la Convención, en su art. 8 establece que las personas tendrán derecho a:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia

[165]Supra. Convenio 108. Art. 26
[166] Uruguay fue el primer estado "no miembro" en ratificarlo en abril de 2013.
[167] Supra . Convenio 108. Art 5.

habitual o el establecimiento principal de la autoridad controladora del fichero.

b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) Obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos que emanan del Convenio;
d) Disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) anteriores.
e) Un recurso que debería llevar a cabo una "autoridad independiente" que no aparece mencionada en el Convenio 108 pero que se añadió al Convenio a través de Protocolo en 2001,[168] tal vez al albur de lo que establecía la Directiva 95/46/CE.

6.5 El Convenio 108 Plus Del Consejo De Europa para la Protección de Datos Personales. La modificación del Convenio 108.

El 10 de octubre de 2018, se abrió a la firma de los países miembros del Consejo de Europa y de otros que, aunqueno lo sean, se quieran adherir, la

[168] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001

modificación del convenio 108, que se ha denominado Convenio 108+[169]. Interesa destacar el hecho de que, ahora, los organismos y organizaciones internacionales también se podrán adherir al convenio.

Con esta modificación, los principios originales que rigen la Convención 108 se han reafirmado, algunos se han fortalecido y se han establecido algunas nuevas salvaguardas ya que existe la nueva realidad del mundo en línea, que hace que se tengan que reconocer. De esta manera, los principios de transparencia, proporcionalidad, responsabilidad, minimización de datos, privacidad por diseño, etc. se reconocen ahora como elementos clave del mecanismo de protección y se han integrado en el instrumento modernizado.

Las principales novedades de la Convención modernizada[170] pueden presentarse de la siguiente manera:

Artículo 1. Objeto y finalidad de la Convención.

El artículo 1 establece que "The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy"

En virtud del artículo 1, el objetivo de la Convención está claramente subrayado, es decir, garantizar a todas las personas que se encuentren bajo la jurisdicción de una de las Partes (independientemente de su nacionalidad o lugar de residencia) la protección de sus datos personales durante el

[169] Texto final disponible en https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[170] Ver https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

procesamiento, contribuyendo así al respeto de sus derechos y libertades fundamentales, y en particular su derecho a la privacidad. Con esta redacción, la Convención destaca el hecho de que el procesamiento de datos personales puede permitir positivamente el ejercicio de otros derechos y libertades fundamentales, lo que puede facilitarse garantizando el derecho a la protección de datos.

En cuanto a lo expuesto por los artículos 2 y 3 -definiciones y ámbito de aplicación- si bien las nociones esenciales, como la definición de datos personales y la de los interesados, no se modifican en absoluto en comparación con el anterior convenio, se proponen otros cambios en las definiciones: se abandona el concepto de "archivo". “Controlador de un archivo de datos” se reemplaza por “controlador de datos”, además de lo cual se usan los términos “procesador” y “destinatario”.

La Convención se conserva, y el alcance naturalmente continúa cubriendo el procesamiento en los sectores público y privado indistintamente, ya que esta es una de las grandes fortalezas de la Convención.

Por otro lado, la Convención ya no se aplica al procesamiento de datos realizado por una persona física para el ejercicio de actividades puramente personales de nuestro hogar. Además, las Partes ya no tienen la posibilidad de hacer declaraciones destinadas a eximir de la aplicación de la Convención ciertos tipos de procesamiento de datos (por ejemplo, con fines de seguridad y defensa nacional).

El artículo 4, obligaciones de las partes, establece que cada parte debe adoptar en su legislación interna las medidas necesarias para dar efecto a las disposiciones de la Convención. Además, cada Parte debe demostrar que tales

medidas realmente se han tomado y son efectivas y aceptar que el Comité de la Convención pueda verificar que se hayan cumplido estos requisitos. Este proceso de evaluación de las Partes ("mecanismo de seguimiento") es necesario para garantizar que el nivel de protección establecido por la Convención sea realmente otorgado por las Partes. Es importante señalar, como se ha dicho anteriormente, que las organizaciones internacionales ahora tienen la posibilidad de adherirse a la Convención (artículo 27), al igual que la Unión Europea (artículo 26).

El artículo 5, legitimidad del procesamiento de datos y calidad de los datos, establece que:

"1 Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2 Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

3 Personal data undergoing processing shall be processed lawfully.

4 Personal data undergoing processing shall be: a processed fairly and in a transparent manner; b collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; c adequate, relevant and not excessive in relation to the purposes for which they are processed; d accurate and, where

necessary, kept up to date; e preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed."

El artículo 5 aclara la aplicación del principio de proporcionalidad para subrayar que debe aplicarse durante todo el procesamiento, y en particular con respecto a los medios y métodos utilizados en el procesamiento. Además, se ve reforzado por el principio de minimización de datos. Se introduce una nueva disposición para establecer claramente la base legal del procesamiento: el consentimiento (que debe ser válido debe satisfacer varios criterios) del interesado o alguna otra base legítima establecida por la ley (contrato, interés vital de los datos) sujeto, obligación legal del controlador, etc.).

El artículo 6, datos confidenciales, establece que el catálogo de datos confidenciales se ha ampliado para incluir datos genéticos y biométricos, así como datos procesados para la información que revelan en relación con la afiliación sindical u origen étnico (esas dos últimas categorías se están agregando a la prohibición existente sobre el procesamiento de datos personales que revelen el origen racial, opiniones políticas o creencias religiosas u otras, salud o vida sexual y datos personales relacionados con delitos, procedimientos penales y condenas).

En términos de seguridad de datos, el art. 7 introduce el requisito de notificar, sin demora, cualquier violación de seguridad. Este requisito se limita a los casos que pueden interferir seriamente con los derechos y libertades fundamentales de los interesados, que deben notificarse, al menos, a las autoridades supervisoras.

Según lo expuesto en al art.8, los controladores tendrán la obligación de garantizar la transparencia del procesamiento de datos y para ese fin deberán proporcionar un conjunto de información requerida, en particular en relación con su identidad y lugar habitual de residencia o establecimiento, sobre la ley base y los propósitos del procesamiento, los destinatarios de los datos y las categorías de datos personales procesados. Además, deben proporcionar cualquier información adicional necesaria para garantizar un procesamiento justo y transparente. El Controlador está exento de proporcionar dicha información cuando el procesamiento esté expresamente prescrito por la ley o esto resulte imposible o implique esfuerzos desproporcionados.

A los interesados se les otorgan nuevos derechos, en virtud del art. 9, para que tengan un mayor control sobre sus datos en la era digital. La Convención modernizada amplía el catálogo de información que se transmitirá a los interesados cuando ejerzan su derecho de acceso. Además, los interesados tienen derecho a obtener conocimiento del razonamiento subyacente al procesamiento de datos, cuyos resultados le incumben. Subraya el Consejo de Europa que este nuevo derecho es particularmente importante en términos de perfiles de individuos.

Este último derecho debe asociarse con otra novedad, a saber, el derecho a no estar sujeto a una decisión que afecte al interesado que se basa únicamente en un procesamiento automatizado, sin que el interesado tenga en cuenta sus opiniones. Los interesados tienen derecho a oponerse en cualquier momento al procesamiento de sus datos personales, a menos que el controlador demuestre motivos legítimos convincentes para el procesamiento que anulen sus intereses o derechos y libertades fundamentales.

La Convención modernizada impone, en su art. 10, obligaciones más amplias a quienes procesan o procesan datos en su nombre. Sobre este tema, el Consejo de Europa deriva a la Recomendación de 2010 sobre la protección de las personas con respecto al procesamiento automático de datos personales en el contexto de la elaboración de perfiles y su memorándum explicativo.

La responsabilidad se convierte en una parte integral del esquema de protección, con la obligación de que los controladores puedan demostrar el cumplimiento de las normas de protección de datos. Los controladores deben tomar todas las medidas apropiadas, incluso cuando se subcontrata el procesamiento, para garantizar que se garantice el derecho a la protección de datos (privacidad por diseño, examen del impacto probable del procesamiento de datos previsto en los derechos y libertades fundamentales de los interesados (" evaluación de impacto de privacidad ") y privacidad por defecto).

Artículo 11. Excepciones y restricciones.

Los derechos establecidos en la Convención no son absolutos y pueden estar limitados cuando así lo establece la ley y constituye una medida necesaria en una sociedad democrática sobre la base de motivos específicos y limitados. Entre esos motivos limitados se incluyen ahora "objetivos esenciales de interés público", así como una referencia al derecho a la libertad de expresión. La lista de disposiciones de la Convención que pueden restringirse se ha ampliado ligeramente (véanse art. 7.1; 8.1; y 11.1) y en un nuevo párrafo se añade específicamente las actividades de procesamiento para fines de seguridad y defensa nacional, para lo cual los poderes de "supervisión" del Comité, así como algunas misiones de las autoridades de supervisión pueden

ser limitados. El requisito de que las actividades de procesamiento para fines de seguridad y defensa nacional estén sujetas a una revisión y supervisión independiente y efectiva, está claramente establecido.

El Consejo de Europa subraya que es importante recordar que, contrariamente a las disposiciones anteriores del Convenio 108, las Partes en el Convenio modernizado ya no podrán excluir del ámbito de aplicación del Convenio ciertos tipos de procesamiento. .

El objetivo de esta disposición, de conformidad con el art.14, es facilitar, cuando corresponda, el libre flujo de información independientemente de las fronteras, al tiempo que garantiza una protección adecuada de las personas con respecto al procesamiento de datos personales. El propósito del régimen de flujo transfronterizo es asegurar que la información procesada originalmente dentro de la jurisdicción de una Parte siempre permanezca protegida por los principios apropiados de protección de datos. Los flujos de datos entre las Partes no pueden prohibirse ni estar sujetos a una autorización especial ya que todos ellos, al haberse suscrito al núcleo común de las disposiciones de protección de datos establecidas en el Convenio, ofrecen un nivel de protección considerado apropiado. Existe una excepción: cuando existe un riesgo real y grave de que dicha transferencia conduzca a eludir las disposiciones de la Convención.

En ausencia de normas armonizadas de protección compartidas por los Estados pertenecientes a una organización internacional regional y que rijan los flujos de datos (véase, por ejemplo, el marco de protección de datos de la Unión Europea), los flujos de datos entre las Partes deberían funcionar libremente. Con respecto a los flujos transfronterizos de datos a un receptor

que no está sujeto a la jurisdicción de una Parte, se debe garantizar un nivel adecuado de protección en el Estado u organización del receptor. Como esto no se puede suponer dado que el destinatario no es Parte, el Convenio establece dos medios principales para garantizar que el nivel de protección de datos sea realmente apropiado; ya sea por ley, o por salvaguardas estandarizadas ad hoc o aprobadas que sean legalmente vinculantes y exigibles (en particular cláusulas contractuales o normas corporativas vinculantes), así como debidamente implementadas.

La Convención modernizada complementa, mediate su art. 15, el catálogo de poderes de las autoridades con una disposición que, además de sus poderes para intervenir, investigar, entablar procedimientos judiciales o llamar la atención de las violaciones de las disposiciones de protección de datos por parte de las autoridades judiciales, las autoridades también tienen el deber de crear conciencia, proporcionar información y educar a todos los actores involucrados (sujetos de datos, controladores, procesadores, etc.). También permite a las autoridades tomar decisiones e imponer sanciones. Además, se recuerda en este artículo que las autoridades de supervisión deben ser independientes en el ejercicio de estas tareas y poderes.

El convenio modernizado también aborda la cuestión de la cooperación (y la asistencia mutua) entre las autoridades supervisoras en su art. 17 Las autoridades supervisoras tienen que coordinar sus investigaciones, realizar acciones conjuntas y proporcionarse información y documentación sobre sus leyes y prácticas administrativas relacionadas con la protección de datos. La información intercambiada entre las autoridades de supervisión incluirá datos personales solo cuando dichos datos sean esenciales para la cooperación o cuando el interesado haya dado su consentimiento específico, libre e

informado. Finalmente, el Convenio proporciona un foro para una mayor cooperación: las autoridades supervisoras de las Partes tienen que formar una red para organizar su cooperación y cumplir con sus obligaciones según lo especificado por el Convenio.

El Comité de la Convención, según los art. 22 a 24, desempeña un papel crucial en la interpretación de la Convención, fomentando el intercambio de información entre las Partes y desarrollando normas de protección de datos. El papel y los poderes de este Comité se fortalecen con la Convención Modernizada. Ya no se limita a un rol "consultivo" sino que también tiene poderes de evaluación y monitoreo. Proporcionará una opinión sobre el nivel de protección de datos proporcionado por un estado u organización internacional antes de la adhesión a la Convención. El comité también puede evaluar el cumplimiento de la legislación interna de la Parte en cuestión y determinar la efectividad de las medidas adoptadas (existencia de una autoridad supervisora, responsabilidades, existencia de recursos legales efectivos). También puede evaluar si las normas legales que rigen las transferencias de datos ofrecen una garantía suficiente de un nivel adecuado de protección de datos.

6.6. Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.

Más desconocida entre el gran público y algunos profesionales es la Guía que publicó la OCDE, el 23 de septiembre de 1980, sobre protección de datos personales y el flujo transfronterizo de estos datos.

Sin embargo, se trata de la primera "Soft Law" que contiene los principios fundamentales en materia de protección de datos y que han sido utilizadas por la mayoría de los países para redactar la legislación sobre esta materia.

Estos principios fundamentales son:

a) Principio de limitación al almacenamiento de datos.
b) Principio de datos relevantes.
c) Principio del propósito de la recolección de datos personales.
d) Principio de salvaguarda de los datos recogidos de terceros
e) Principio de que las personas puedan acceder a sus datos, borrarlos y modificarlos.
f) Principio de trasparencia.

6.7. Resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990

El punto 9 de dicha resolución establece que "cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, sino solamente en la medida en que así lo exija la protección de la vida privada".

7. El Derecho al Olvido en Estados Unidos. Análisis jurisprudencial.

No se puede entender este estudio, como veremos, sin una mención a la legislación de norteamérica ni a su manera de abordar el problema, muy diferente a la europea. El problema del Derecho al Olvido es global y, sin duda, Estados Unidos es una pieza muy importante del fichero.

Entendemos que la solución del problema tiene que venir por "casar" el mayor número de legislaciones, pues el Derecho al Olvido ha de aplicarse tanto si la búsqueda en Google se hace en Madrid o Washington. O si el tratamiento de datos –en referencia al Big Data- está siendo realizado en Ruanda con una base de datos Suiza por una empresa Australiana.

Mientras que la mayoría de los países amparan en su Constitución el derecho a la privacidad de la información, la Constitución de los Estados Unidos no contempla explícitamente este Derecho. Por el contrario, en Estados Unidos, con su jurisprudencia, se entiende que el derecho a la privacidad hay que apreciarlo en cada situación atendiendo al tipo de industria, uso e información.[171]

Hay que atender a la idiosincrasia del país – un país construido bajo la premisa de que todo el mundo tiene derecho a una segunda oportunidad y a reinventarse- para comprender cómo se entiende el Derecho al Olvido en la legislación americana y en su interesante intersección de leyes.

Para la jurisprudencia de los Estados Unidos, todo el mundo tiene derecho a que su pasado sea olvidado siempre y cuando lleve en el momento una vida honorable. La reputación actual está estrictamente protegida.

[171] REINDERG, JR "Resolving Conflicting International Data Privacy Rules in Cyberspace", Stanford Law review 52 (2000)

La diseminación de los hechos privados puede dar lugar a causas penales, aunque estos hechos sean ciertos.[172]

Pero el principal problema con la aplicación del Derecho al Olvido en Estados Unidos se produce con el hecho de que cada información que se cuelga en la Red está considerada como "speech", incluida la información compilada por los motores de búsqueda[173], y el deseo de borrar información contenida en los Buscadores atenta contra la "Fredom of Speech".

La primera enmienda de la constitución de EEUU protege de manera muy extrema la libertad de comunicación, que prácticamente no tiene límites ni excepciones[174].

Además, la Communnications Decency Act[175], en su sección 230, inmuniza a los proveedores de Internet de la responsabilidad sobre la libertad de expresión en los sitios web de dos maneras:

En primer lugar, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".

Y en segundo lugar al afirmar que "no cause of action may be brought and no liability may be imposed under any State or local rule that is inconsitent with this section".

[172] Ver Florida Star v. BJF (Corte Suprema de Estados Unidos, 1989)
[173] Nos referimos a información colgada por terceres personas, no a la que una persona haya colgado voluntariamente
[174] Por ejemplo, ver la recinte Sentencia de la Corte Suprema, Town of Greece, New York v. Galloway et al.
[175] http://www.law.cornell.edu/uscode/text/47/230

Por tanto, en Estados Unidos, los resultados de búsqueda de Google están protegidos por la Primera Enmienda de la Constitución, y únicamente tendrán responsabilidad sobre los resultados publicados por información que viole la propiedad intelectual o por publicaciones de "obscenidad, difamación, fraude, o que inciten al crimen"[176].

La Sección 230 de la Communnications Decency Act tiene como objetivo el impedir pleitos contra servicios interactivos de computación por el "exercise of editorial discretion over internet content and editorial decisions regarding screening and deletion of content from their services"[177].

La Sección 230 hace que Google, Yahoo y Microsoft, entre otros, tengan inmunidad sobre sus decisiones editoriales en relación a la selección y borrado de sus datos.[178]

Numerosa jurisprudencia sigue la misma línea. Google está protegida por la "libertad de expresión" de la Primera Enmienda de la Constitución y por la sección 230[179].

Pero es que la jurisprudencia aún ha ido más lejos. Ha habido casos donde se ha intentado litigar contra Google por las "sugerencias" que éste ofrece en la búsqueda de resultados[180].

[176] United States vs Stevens, 130 S. Ct. 1577,1580 (2010).
[177] Langdond vs Google,Inc. 474 F. Supp.2d 622,630 (D.Del.2007)
[178] Caso Langdond. Íbidem at Supra. Traducción propia.
[179] Supplementmarket.com Inc v s Google. Tribunal de Pensilvania. 26 de julio de 2010. Mmubango vs Google,Inc 2013 WL 664231 (E.D. Pa. February 22, 2013).
[180] Stayart vs Google Inc. 2013 WL 811793 (7th Cir. March 6, 2013).

Lo mismo puede decirse de las infructuosas demandas contra Google basadas en la privacidad o en la propiedad intelectual del programa de anuncios de Google[181] o de Google Street View[182].

En conclusión, no hay que olvidar que la libertad de Internet y la neutralidad en la red es un movimiento muy poderoso en Estados Unidos[183][184].

Como conclusión, el Derecho al Olvido en estados Unidos no se ajusta al concepto de Derecho al Olvido en Europa, tal y como veremos, por la diferente preponderancia que se le da a determinados derechos.

Sin duda, entendemos que en un mundo global no cabe tratar al Derecho al Olvido en referencia a una única legislación o un único territorio, sin relación alguna con las demás partes. El mundo online, un mundo global, exige un enfoque global y, en consecuencia, hay que concluir que la solución deberá venir dada también de manera global.

8. EL Derecho al Olvido en la jurisprudencia internacional.

8.1. Jurisprudencia del Derecho al Olvido en Italia.

I

A) Sentencia de la Sala segunda, del 9 de marzo de 2017, En el asunto C/398/15, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Corte suprema di cassazione

[181] KinderStart.com LLC v. Google, Inc., No. C 06-2057 RS (N.D. Cal. complaint filed March 17, 2006)

[182] Boring v. Google, Inc., 598 F.Supp.2d 695 (W.D. Pa. 2009)
[183] www.internetdeclaration.og. Ver preámbulo
[184] http://www.whitehouse.gov/net-neutrality (última visita 3 de diciembre de 2018)

(Tribunal Supremo de Casación, Italia), mediante resolución de 21 de mayo de 2015.

El Sr. Salvatore Manni fue el único director de Immobiliare Salentina, una empresa que se declaró insolvente en 1992 y fue liquidada en 2005. Su relación con Immobiliare Salentina se reflejó en el registro de empresas, que fue administrado por la Cámara de Comercio de Lecce. Este registro de empresas cumplió con la Primera Directiva 68/151/CEE del Consejo, de 9 de marzo de 1968, tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el artículo 58, párrafo 2 del Tratado, para proteger los intereses de socios y terceros [185], que requería que los Estados miembros adoptaran medidas para garantizar la divulgación obligatoria de cierta información relacionada con las empresas. Así, el artículo 2.1[186] de la Directiva citada exigía la divulgación por parte de las empresas de las personas autorizadas para representar a las empresas en los tratos con terceros, los que controlan las empresas y los liquidadores designados de las empresas.

En 2007, el Sr. Manni no pudo vender sus propiedades y culpó al hecho de que el registro de las empresas reflejó su participación en Immobiliare

[185] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al26003

[186] 1 .” Los Estados miembros tomarán las medidas necesarias para que la publicidad obligatoria relativa a las sociedades se refiera al menos a los actos e indicaciones siguientes :
a) la escritura de constitución y los estatutos , si fueran objeto de un acto separado ;
b) las modificaciones de los actos mencionados en la letra a) , comprendida la prórroga de la sociedad ;
c) después de cada modificación de la escritura de constitución o de los estatutos , el texto íntegro del acto modificado , en su redacción actualizada ;
d) el nombramiento , el cese de funciones , así como la identidad de las personas que , como órgano legalmente previsto , o como miembros de tal órgano ;
i) tengan el poder de obligar a la sociedad con respecto a terceros y representarla en juicio ,
ii) participen en la administración , la vigilancia o el control de la sociedad .
Las medidas de publicidad deberán precisar si las personas que tengan poder de obligar a la sociedad pueden hacerlo por sí o deben hacerlo conjuntamente” (...)

Salentina. Argumentó que la información del registro fue utilizada para determinar su calificación de riesgo por una compañía especializada en la recolección y procesamiento de información de mercado y en la evaluación de riesgos.

Posteriormente, el Sr. Manni solicitó que sus datos personales que lo vincularan a la liquidación de Immobiliare Salentina fueran borrados, anonimizados o bloqueados del registro de empresas. En agosto de 2011, el Tribunal de Lecce accedió a su solicitud, ordenando que la Cámara de Comercio de Lecce anonimizara los datos que lo vinculaban a la liquidación de Immobiliare Salentina y que pagaran 2.000 euros por daños ocasionados. El Tribunal de Lecce dictaminó que no era permisible que las entradas en el registro que vinculaban el nombre de un individuo a una fase crítica en la vida de una empresa fueran permanentes, a menos que hubiera un interés general específico en su retención y divulgación. El Tribunal de Lecce razonó que "después de un período apropiado" desde la conclusión de la liquidación de una empresa, y después de que esa empresa había sido eliminada del registro, indicando el nombre de la persona que era el único director de esa empresa en el momento de la liquidación dejó de ser "necesaria" y "útil".

Continuó diciendo que, en tales casos, el interés público en una "memoria histórica" de la existencia de la empresa y las dificultades que experimentó, también podrían lograrse mediante datos anónimos.

La Cámara de Comercio de Lecce apeló ante el Tribunal de Casación, que luego suspendió el procedimiento y formuló una cuestión prejudicial al TJUE sobre si " el artículo 3 de la Directiva 68/151[187] y el artículo 6, apartado 1,

[187] "1 . En cada Estado miembro se abrirá un expediente, en un registro central o bien en un registro mercantil o registro de sociedades , por cada una de las sociedades inscritas .

letra e)[188], de la Directiva 95/46[189] deben interpretarse en el sentido de que los Estados miembros pueden, o deben, permitir a las personas físicas mencionadas en el artículo 2, apartado 1, letras d) y j), de la Directiva 68/151 solicitar a la autoridad responsable del registro de sociedades que limite, al expirar un plazo determinado tras la liquidación de la sociedad de que se trate y sobre la base de una apreciación caso por caso, el acceso a los datos personales que les conciernen inscritos en dicho registro".

II

El Tribunal de Justicia de la Unión Europea (TJUE) comenzó reconociendo que la autoridad responsable de mantener el registro de un Estado miembro en virtud de la Directiva 68/151[190] equivalía a un "controlador de datos" en virtud de la 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[191].

---

2 . Todos los actos y todas las indicaciones que se sometan a la publicidad en virtud del artículo 2 se incluirán en el expediente o se transcribirán en el registro ; el objeto de las transcripciones al registro deberá aparecer en todo caso en el expediente .
3 . Deberá poderse obtener copia íntegra o parcial de todo acto o toda indicación de las mencionadas en el artículo 2, por correspondencia y sin que el costo de esta copia pueda ser superior al costo administrativo" .

[188] "e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos."

[189] 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

[190] Íb.Supra

[191] Íb.Supra

Además, la divulgación de datos personales contenidos en esos registros equivalía a "procesamiento de datos". El TJUE se refirió al caso de Google España, explicando que la Directiva 95/46 “busca garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas, en particular su derecho a la privacidad, con respecto al procesamiento de datos personales. "

El Tribunal añadió que el procesamiento de datos en virtud de la Directiva 95/46, particularmente cuando infringe el derecho al respeto de la vida privada, debe evaluarse en relación con la Carta de los Derechos Fundamentales de la Unión Europea.

El TJUE señaló que el artículo 6, apartado 1, letra e), de la Directiva 95/46 exigía que los Estados miembros se aseguraran de que “los Estados miembros dispondrán que los datos personales sean conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente”

El TJUE recordó que un interesado posee " el derecho de obtener del responsable del tratamiento, en su caso, la supresión o el bloqueo de los datos (véase, en este sentido, la sentencia de 13 de mayo de 2014, Google Spain y Google, C:131/12, EU:C:2014:317”

El TJUE también señaló que “los Estados miembros reconocerán al interesado, concretamente, en los supuestos contemplados en las letras e) y f) del artículo 7 de ésta, el derecho a oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional

disponga otra cosa. La ponderación que ha de efectuarse en el marco de dicho artículo 14, párrafo primero, letra a), permite así tener en cuenta de modo más específico todas las circunstancias que rodean a la situación concreta del interesado. En caso de que exista una oposición justificada, el tratamiento llevado a cabo por su responsable ya no puede versar sobre estos datos (véase la sentencia de 13 de mayo de 2014, Google Spain y Google, C:131/12, EU:C:2014:317, apartado 76).”

El TJUE consideró el propósito de la divulgación pertinente como primer paso para determinar si una persona tenía derecho a borrar, bloquear o restringir el acceso a los datos en el registro de las empresas después de un cierto período de tiempo. En este caso, la publicidad se realizó de conformidad con la Directiva 68/151, que tenía como objetivo proteger " en particular, los intereses de terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada, ya que, como garantía respecto a terceros, sólo ofrecen su patrimonio social. A tal fin, la publicidad debe permitir a los terceros conocer los actos esenciales de la sociedad y ciertas indicaciones relativas a ella, concretamente la identidad de las personas que tienen el poder de obligarla.”

III

Además, al estandarizar el procedimiento de divulgación adoptado en todos los Estados miembros, la Directiva 68/151 pretendía "garantizar la seguridad jurídica en las relaciones entre las sociedades y los terceros en la perspectiva de una intensificación del tráfico mercantil entre los Estados miembros como consecuencia de la creación del mercado interior y que, desde esta perspectiva, es importante que toda persona deseosa de establecer y mantener

relaciones comerciales con sociedades radicadas en otros Estados miembros pueda fácilmente tomar conocimiento de los datos esenciales relativos a la constitución de las sociedades mercantiles y a los poderes de las personas encargadas de representarlas, lo que requiere que todos los datos pertinentes figuren de manera explícita en el registro (véase, en este sentido, la sentencia de 12 de noviembre de 1974, Haaga, 32/74, EU:C:1974:116, apartado 6)."

El TJUE señaló que la información en el registro de empresas puede ser necesaria para un tercero mucho después de que una empresa haya dejado de existir[192].

El TJUE también señaló que la Directiva 68/151 no estableció un límite de tiempo máximo para las divulgaciones en los registros de la empresa. El TJUE concluyó que, a la luz de la gama de posibles escenarios en los que la información podría ser necesaria, le era imposible identificar un límite único para cuándo se debería eliminar la información de los registros.

El TJUE fundamenta que los Estados miembros no pueden garantizar a las personas físicas a las que se refiere el artículo 2, apartado 1, letras d) y j), de la Directiva 68/151 el derecho a obtener tras un determinado plazo a contar desde la liquidación de la sociedad de que se trate que se supriman los datos personales que les conciernen, inscritos en el registro con arreglo a esta última disposición, o que el público tenga bloqueado el acceso a ellos.

Por otra parte, esta interpretación de los artículos 6, apartado 1, letra e), y 12, letra b), de la Directiva 95/46 no conduce a una injerencia desproporcionada en los derechos fundamentales de los interesados, concretamente en su

[192] Véanse la sentencia de 4 de diciembre de 1997, Daihatsu Deutschland, C‑97/96, EU:C:1997:581, apartados 19, 20 y 22, y el auto de 23 de septiembre de 2004, Springer, C‑435/02 y C‑103/03, EU:C:2004:552, apartados 29 y 33).

derecho al respeto de la vida privada y su derecho a la protección de datos personales, garantizados por los artículos 7 y 8 de la Carta Carta de los Derechos Fundamentales de la Unión Europea[193] porque, en primer lugar, la divulgación se refería a categorías muy limitadas de información y, en segundo lugar, las personas que estaban involucradas en sociedades anónimas o de responsabilidad limitada sabían que estaban obligadas a revelar datos relacionados con su identidad y funciones.

Sin embargo, el TJUE señaló que "puedan existir situaciones particulares en las que razones preponderantes y legítimas propias de la situación concreta del interesado justifiquen excepcionalmente que el acceso a los datos personales que les conciernen, inscritos en el registro, se limite, al expirar un plazo suficientemente largo tras la liquidación de la sociedad de que se trate, a los terceros que justifiquen un interés específico en su consulta".

El TJUE acordó la decisión final sobre si un individuo puede hacer una solicitud para tal limitación es un asunto de las legislaciones nacionales.

IV

Por último, el TJUE opinó, con respecto a la solicitud de la parte actora que "incumbirá al tribunal remitente apreciar, a la luz del conjunto de circunstancias pertinentes y teniendo en cuenta el plazo transcurrido desde la liquidación de la sociedad de que se trate, la posible existencia de razones preponderantes y legítimas que, en su caso, puedan justificar excepcionalmente la limitación del acceso de terceros a los datos que conciernen al Sr. Manni contenidos en el registro de sociedades, de los que se desprende que fue administrador único y liquidador de Immobiliare Salentina.

[193] Íbidem Supra

Sobre este particular, debe señalarse que el mero hecho de que, supuestamente, los inmuebles de un complejo turístico construido por Italiana Costruzioni, cuyo administrador único es actualmente el Sr. Manni, no se vendan debido a que los potenciales adquirentes de estos inmuebles tienen acceso a estos datos en el registro de sociedades no constituye una razón de este tipo, habida cuenta, en particular, del interés legítimo de éstos a disponer de esa información.

El TJUE devolvió el caso a los tribunales nacionales italianos para su determinación definitiva.

La decisión amplía la libertad de expresión al proporcionar una protección sólida a la divulgación de información en registros de empresas disponibles al público, incluida información sobre los directores y liquidadores de empresas después de que hayan dejado de existir.

V

El TJUE se negó a aceptar que cierta información en el registro de empresas podría estar sujeta a una divulgación limitada porque perjudicaba la reputación de un hombre de negocios, reconociendo que el interés público en la seguridad jurídica y el comercio justo superaban el derecho del hombre de negocios a una reputación y una vida privada.

Este caso reconoce una excepción significativa al "Derecho al Olvido", y define de manera limitada las circunstancias bajo las cuales las personas pueden obtener el borrado, bloqueo o anonimato de sus datos personales en

los registros mantenidos de conformidad con la Directiva 68/151, que debe ser examinada caso a caso.

De Verda[194] explica como antecedentes que "En la jurisprudencia italiana es muy conocido el caso resuelto por la Ordenanza del Juzgado Roma de 6 de mayo 1983 (FI 1984, I, 299), que prohibió cautelarmente la difusión en televisión de una película-documental, sobre la muerte, una tarde de 1977, del famoso jugador de fútbol del "Lazio", Lucciano Re Cecconi. El deportista, queriendo gastar una broma a un amigo joyero, al que habían atracado varias veces, en compañía de otras personas, fue a su tienda y, cuando estaba de espaldas, le gritó: "Esto es un atraco", a lo que este respondió, volviéndose y disparándole un tiro que acabó con su vida, sin tener tiempo de reconocerlo. El joyero fue acusado por el Ministerio Fiscal, que pidió tres años de prisión, siendo absuelto en el juicio penal, celebrado un mes después, al apreciarse la eximente de actuación en legítima defensa".

Contúna explicando De Verda[195] que "la Sentencia de la Corte de Casación, de 9 de abril de 1998 (FI 1998, I, 1834), ha admitido, explícitamente, el Derecho al Olvido. Más recientemente, la sentencia de la misma Corte, de 5 de abril de 2012 (NGCC 2012, I, 836), afirma que, si el interés público a la libertad de información limita el derecho a la intimidad, no obstante, al sujeto concernido, en aras al libre desarrollo de su personalidad, se le reconoce un Derecho al Olvido, esto es, a que no sean posteriormente divulgadas noticias que, por el transcurso del tiempo, resulten ya olvidadas o ignoradas para la generalidad de las personas. Ello, siempre que no exista un interés público a su actual consentimiento, por razones de carácter histórico, didáctico o

[194] DE VERDA, J. R. (2014). "Breves reflexiones sobre el llamado Derecho al Olvido". Revista Actualidad Jurídica Iberoamericana, 1.
[195] Íbidem

cultural, o, más en general, porque persista un interés social en dicho conocimiento".

VI

B) Otro de los antecedentes italianos lo situa De Verda[196] en que "[…] el Tribunal de Roma, el 15 de mayo de 1995 ("Dir. Informática"" 1996, 422) […] afirmó que la nueva publicación, después de treinta años, de un hecho delictivo, con fines promocionales, constituye una difamación y obliga a la sociedad editora del periódico a resarcir el daño moral ocasionado, al tratarse de una información carente de interés público. En el caso litigioso, un periódico había reproducido una antigua página del 6 de diciembre de 1961, en la que se encontraba una noticia relacionada con un concurso semanal. Sin embargo, en dicha página aparecía, además, otra antigua noticia, relativa a una confesión de homicidio con el nombre y la fotografía del reo, el cual, tras haberse beneficiado de una reducción de condena y de una medida de gracia del Presidente de la República, se había reinsertado plenamente en la sociedad, tanto, desde el punto de vista personal y afectivo, como profesional. Al volverse a publicar la antigua noticia, su protagonista perdió su trabajo y la confianza de las personas que lo rodeaban."

VII

C) Interesante es la Sentencia del Tribunal Supremo Italiano en el caso Vendetti contra la RAI, ya que la sentencia del Tribunal Supremo Italiano se produce despúes de la Sentencia del TJUE sobre Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González[197]

[196] Íbidem
[197] Íb. Supra.

Resulta que el 12 de diciembre de 2000, los periodistas del programa de televisión italiano "La vita in diretta" sorprendieron al famoso compositor italiano Antonello Venditti, afuera de un restaurante, para entrevistarlo. Venditti se negó clara y perentoriamente y posteriormente se transmitió un video de la escena en el principal canal de televisión italiano, "RAI 1", junto con un comentario que preguntaba irónicamente por qué Venditti estaba tan nervioso, especialmente desde que se acercaba la Navidad y la gente debería estar de buen humor.

Cinco años después, el 27 de abril de 2005, el video se transmitió nuevamente en el mismo programa de televisión que la segunda entrada en una lista de los personajes más desagradables y malhumorados del mundo del espectáculo. El video comentó sobre el hecho de que Venditti se negó a ser entrevistado porque no estaba acostumbrado a ser el centro de atención. Como resultado, demandó a la emisora, alegando daños por el uso ilegal y con fines comerciales de su imagen, la violación de su derecho a ser olvidado y la naturaleza difamatoria del comentario incluido en el video transmitido.

En 2007, el Tribunal de Primera Instancia de Roma[198] rechazó la afirmación de Venditti sobre la base de que la celebridad del compositor y el interés del público en conocer el evento justificaron la excepción al requisito de consentimiento para el uso de la imagen de una persona. El Tribunal también determinó que no existía una violación del Derecho al Olvido; que la transmisión era legal y que cumplía con el derecho a la privacidad y, en cualquier caso, era justificable como sátira.

[198] Disponible en http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20180320/snciv@s10@a2018@n06919@tO.clean.pdf (último acceso julio 2019)

En 2014, el Tribunal de Apelación confirmó la decisión del Tribunal de Roma y Venditti apeló ante el Tribunal Supremo italiano.

El Tribunal Supremo italiano señaló que el caso involucraba un conflicto entre los derechos fundamentales, a saber, el derecho a informar sobre lo que es de interés público y el derecho de un individuo a no ser tergiversado por la publicación de información que no es relevante para el interés público.

El Tribunal también señaló que una persona tiene derecho a obtener la eliminación de las listas, archivos o registros de su nombre con respecto a hechos o eventos que no son de interés público. En este sentido, se refirió en particular a la decisión del TJUE en Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González[199], que estableció que los europeos que sentían que estaban siendo tergiversados por información que era inexactos, inadecuados, irrelevantes o excesivos para el procesamiento de datos podrían pedir a los motores de búsqueda como Google que desvinculen el material. Si se aprueba la solicitud, la información permanecerá en línea en el sitio original, pero ya no aparecerá en las consultas de los motores de búsqueda. El TJUE declaró que, por regla general, este "derecho a ser olvidado" para los interesados no solo anularía el interés económico del motor de búsqueda sino también el interés del público en general en tener acceso a la información. Las excepciones a esto, por ejemplo, el papel del interesado en la vida pública, podrían justificar la interferencia con el derecho fundamental de privacidad del interesado.

[199] ÍbidemSupra

Con base en la jurisprudencia del TJUE y los tribunales nacionales italianos, el Tribunal Supremo italiano enumeró los factores a considerar para determinar si el Derecho al Olvido prevalece sobre el derecho a informar:

a) el beneficio de la imagen o las noticias para el debate público;

b) la efectividad de su difusión en el momento actual, por ejemplo, por razones de justicia, policía o protección de derechos o libertades de terceros, o con fines científicos, educativos o culturales, pero no cuando el interés es meramente económico;

c) si el tema es bien conocido y especialmente cuando es público y se trata de un funcionario público;

d) los métodos utilizados para obtener la información o imagen que debe estar de acuerdo con el periodismo responsable y las formas en que se difunde, que no deben exceder el derecho a informar al ser tratados de manera sensacionalista o utilizados para expresar opiniones personales;

e) si el tema recibió notificación previa y la oportunidad de responder antes de la publicación.

El Tribunal Supremo determinó que los tribunales inferiores se habían basado exclusivamente en la celebridad de Venditti para justificar la retransmisión, y no habían tenido debidamente en cuenta el contenido del video y cómo se difundió.

Destacó la clara diferencia entre el caso y los eventos de Venditti con respecto a la protección del orden público o la seguridad personal, donde el interés del público en saber, puede existir durante mucho tiempo después del evento real o volver a ser relevante en el caso de un evento posterior.

En el presente caso, el Tribunal Supremo italiano consideró que la conducta de Venditti retransmitida por televisión cinco años después de que tuvo lugar el evento no era relevante para el debate público ni justificada por razones de justicia, seguridad pública o de interés científico o educativo. De hecho, dijo el Tribunal, el único interés servido por la transmisión de una clasificación irónica de celebridades fue el interés comercial y los objetivos de audiencia de la emisora.

La Sentencia del Tribunal Supremo Italiano hace prevaler el Derecho al Olvido al Derecho a la Información.

8.2. El Derecho al Olvido en Francia.

I

A) De Verda[200] expone que como antecedentes en Francia tenemos en primer lugar "[…] la STGI de París, de 18 de diciembre de 1991 ('Legipresse', 1992, n. 8, III-1), […] apreció la ilicitud de un artículo aparecido en "Paris Match" con el título "Los ángeles del mal" […] en el artículo se desvelaba el nombre y paradero actual de una mujer, que, después de haber cumplido su pena, se había alejado de su ciudad, trasladándose a Marruecos, donde dedicaba sus energías a cuidar a personas en un hospital. La mujer, en cuestión, después de la aparición del artículo se suicidó, para no decir la verdad sobre su vida anterior a su prometido. El Tribunal, con toda razón, consideró que se habían suministrado informaciones adicionales concernientes a su vida privada actual, las cuales no eran necesarias para la información del público."

[200] Ibidem

II

B) En segundo lugar, tenemos "la sentencia del TPI de Namur, de 24 de noviembre de 1997 ("Legipresse", 1998, n. 154, III-123), afirma […] que una persona condenada judicialmente tiene un real Derecho al Olvido, que se desprende del art. 8 CEDH y del art. 19 del Pacto Internacional de Derechos Civiles o Políticos de Nueva York, el cual debe ser considerado como aquel que permite a la persona no dedicada a una actividad pública exigir el secreto y la tranquilidad, sin los cuales el libre desarrollo de su personalidad quedaría coartado. Observa que el principio general ha de ser el del respeto del "Derecho al Olvido" de la persona rehabilitada, a no ser que se trate de "redivulgar" hechos ya conocidos en la época en que tuvo lugar el proceso y de que exista un interés contemporáneo a esa "redivulgación""

III

C) Y por último destaca "la Sentencia de la Corte de Apelación de Montpellier, de 8 de abril de 1997[201] que observa que el Derecho al Olvido no puede ser reconocido de manera absoluta, siendo el juez quien, en atención a las circunstancias del caso, debe determinar su alcance, teniendo en cuenta la gravedad de los hechos, el tiempo pasado desde su comisión y el esfuerzo de las personas condenadas, desde el momento en que, al haber purgado su pena, pueden oponerse legítimamente al recuerdo de su pasado, si dicho recuerdo no responde a ninguna necesidad de orden ético, histórico o científico."

[201] "Legipresse", 1997.

8.3. El Derecho al Olvido en la India.

I

Hay dos sentencias interesantes: Dharamraj Bhanushankar Dave vs. State of Gujarat and Ors. [SCA No. 1854 of 2015] Sri Vasunathan vs The Registrar General [W.P. No. 62038/2016]. Sentencia del 17 de junio de 2017[202]

A) En el primer caso, (ante el Tribunal Superior de Gujarat), el peticionario presentó una petición de "restricción permanente [en] la exhibición pública gratuita de la sentencia y la orden". El peticionario pedía que no se publicase una sentencia, en la que fue absuelto, sobre una imputación por homicio. El argumento principal del peticionario fue que, a pesar de que la sentencia se clasificó como "no publicable", fue publicada por un repositorio en línea de sentencias y también fue indexada por la búsqueda de Google.

El Tribunal Superior India rechaza la petición del demadante ya que no encuentra legislación sobre protección de datos en India, o alguna amenaza al derecho constitucional a la vida y la libertad y concluye que la publicación en un sitio web no equivale a "informar"", ya que informar solo se refiere a eso por o mediante informes legales.

Obviando la consideración sobre "informar", el primer punto es de relevancia. La falta de disposiciones legales disponibles apunta a la ausencia de legislación de protección de datos en la India. En ausencia de dicha ley, el único recurso que tiene un individuo es buscar protección constitucional bajo uno de los derechos fundamentales, en particular el Artículo 21[203] de la

[202] Ver KHERA, K. "case commentary: right to be forgotten"en Jamia Law Jornal . Vol 3.pag 219-228 y https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments.

[203]http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsgA84bcFRy75ulvS2cmS%2F%2BjkA3PZOKwiEGbqxBy6k1YqUAPtR49CgNDuaJy%2BjX2lD

Constitución india sobre el respeto a la vida privada y a la dignidad del individuo, que a lo largo de los años, se ha convertido en el depósito infinito de derechos no enumerados. Sin embargo, típicamente los derechos bajo el Artículo 21 son de naturaleza vertical, es decir, disponibles solo contra el estado. Su aplicación, en los casos en que una parte privada está involucrada sólo, ha sido admitida desde agosto de 2017[204].

II

B) En el segundo caso, el Tribunal Superior de Karnataka, en enero de 2017, falló a favor del peticionario. El peticionario había expresado su preocupación por la aparición del nombre de su hija en Internet asociado a una causa penal. El tribunal, al tiempo que hace vagas referencias al Derecho al Olvido, razonando que es una tendencia en los países occidentales donde siguen esto como una cuestión legal en casos delicados que involucran a mujeres en general y casos altamente sensibles que involucran violación o que afectan la modestia y la reputación de la persona interesada, falló a favor del peticionario[205], y ordena que el nombre se elimine del título de la causa y el cuerpo de la orden antes de entregarlo a cualquier proveedor de servicios. Esta sentencia, "is all the more problematic for while it makes a reference to jurisprudence in other countries, yet it does not base it on the fundamental right to privacy, but to the idea of modesty and reputation of women, which has no clear legal basis on either Indian or comparative jurisprudence[206].

eIjqsjqRoFXGcSal%2FheGIITazRU%2FDF%2F0xgxIyzqCusk5hI8O6RJACZdkdJwpH2%2BaQ%3D%3D

[204] https://www.elheraldo.co/mundo/declaran-constitucional-el-derecho-la-vida-privada-en-india-395871

[205] Cis India. Íbidem Supra

[206] Íbidem.

8.4. El Derecho al Olvido en China.

I

A) Ren Jiayu, un ciudadano chino demandó al motor de búsqueda chino Baidu, creado en 1999, por los resultados de búsqueda que lo asociaron con un empleador anterior.

En mayo de 2016, la justicia China determinó que los ciudadanos no tienen Derecho al Olvido cuando un Tribunal de Pekín falló a favor de Baidu en una demanda por eliminar los resultados de búsqueda[207].

Que se tenga noticia, ha sido el primero de estos casos en ser juzgado en un tribunal chino.

El demandante argumentó que al publicar los resultados de la búsqueda, Baidu había infringido su derecho de nombre y de reputación, ambos protegidos por la ley china. Debido a estas protecciones, el demandante creyó que era titular del derecho a ser olvidado y peticionó eliminar estos resultados de búsqueda. El tribunal falló en contra de Ren Jiayu, alegando, a mi entender de manera muy original, que su nombre es una colección de caracteres comunes y, como resultado de introducir esos caracteres, los resultados de la búsqueda se derivaron de la introducción de esos caracteres.

De conformidad con el informe de la Dirección General de Políticas Internas de la Comisión Europea[208], dado que no existe una autoridad de protección de datos ni ninguna otra agencia estatal para supervisar la protección de datos

[207] http://www.sixthtone.com/news/814/chinese-have-no-right-be-forgotten-court-rules
[208] EUROPEAN PARLIAMENT "The data protection regime in China in-depth analysis" . Disponible en http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf

personales, los tribunales aparentemente son el único remedio viable para la protección de las personas a este respecto. Sin embargo, el papel de los tribunales como mecanismo de aplicación sigue siendo cuestionable.

Al evaluar el enfoque chino para la protección de datos, según este informe, debe tenerse en cuenta que:

(a) Los derechos humanos, al menos como se conocen en los países occidentales, no están protegidos en China,

(b) El sector público, y todos los objetivos y propósitos estatales definidos dinámicamente por China generalmente deben ser percibidos como exentos de toda legislación.

(c) Las decisiones de los Tribunales no conducen a la seguridad jurídica.

La legislación china sobre la protección del procesamiento de datos personales, se limita a las siguientes obligaciones de los controladores de datos "[adherirse a] Los principios de legalidad, legitimidad y necesidad, indicar claramente el objetivo, los métodos y el alcance de la recopilación y el uso de la información, y obtener la conformidad de la persona cuyos datos se recopilan, [...] no violar las disposiciones de las leyes y reglamentos, y el acuerdo entre ambas partes, en la recopilación o el uso de información ".

Entre las principales deficiencias del sistema de protección de datos chino se pueden enumerar la falta de definiciones comunes, la falta de la noción de consentimiento individual, la falta de mención a los derechos de información, acceso y rectificación, así como la falta de autoridad estatal supervisora (no necesariamente una protección de datos al estilo de la autoridad de la UE, sino incluso una comisión comercial federal similar a EE. UU).

II

B) Sin embargo, en agosto de 2019[209], el buscador chino Baidu ha sido declarado responsable del contenido alojado en su web.

Debido a que los usuarios de Baidu violaron la reputación del difunto padre del señor Zhao[210], en un espacio llamado Enciclopedia de Baidu, éste demandó a Baidu ante el Tribunal de Internet de Pekín y le pidió a Baidu que proporcionara información del infractor, y que cambiara o revocara su acuerdo de usuario, términos de uso, restauración del estado original de la información, eliminación del contenido publicado considerado difamatorio, disculpa y compensación por daños mentales de 6 yuanes.

Durante el juicio, el tribunal determinó que Baidu Encyclopedia fue liberada oficialmente por Baidu en abril de 2008. Según su acuerdo de usuario, Baidu Encyclopedia es el espacio de almacenamiento de información proporcionado por Baidu a los usuarios. Los usuarios pueden acceder libremente y participar por escrito.

El padre de Zhao fue un dramaturgo y escribió el guión de la ópera "Red Coral". A principios de julio de 2018, Zhao descubrió que había críticas maliciosas a la obra de su padre, contrarias al derecho chino de reputación y se presentó queja ante el sitio web de la "Enciclopedia" de Biadu, solicitando eliminar las palabras anteriores y pedir disculpas, compensar la pérdida y revelar la identidad de quien había escrito el comentario malicioso.

[209] https://www.caixinglobal.com/2019-08-23/court-rules-baidu-responsible-for-defamatory-content-published-by-user-101454247.html

[210] Información disponible en https://www.chinacourt.org/article/detail/2019/08/id/4381990.shtml (último acceso 1 de septiembre de 2019)

El 16 de julio de 2018, Baidu Company eliminó los comentarios maliciosos agregados. El 24 de julio, Baidu Company respondió a Zhao por SMS, informándole que había cumplido con la obligación de "Notificación de eliminación" y no estaba de acuerdo con otras apelaciones.

Baidu Company consideraba que Zhao, como uno de los familiares de las partes involucradas en la entrada, no tiene derecho a presentar una demanda en nombre de otros familiares. Como proveedor de servicios de red, Baidu consideraba que no es el editor ni el proveedor del artículo involucrado. La ley actual, continuaba fundamentando Baidu, no tiene la obligación de revisar el proveedor de servicios de red por adelantado. Se ha cumplido la obligación de "Aviso de eliminación" y no debe considerarse responsable. Baidu también defiende que el proceso de creación y edición de entradas de Baidu es un proceso de mejora continua.

Después del juicio, el tribunal sostuvo que las interpretaciones legales y judiciales de China claramente daban a los familiares fallecidos el derecho de presentar una demanda por infracción de reputación. Una evaluación social negativa del fallecido no solo viola la reputación del fallecido, sino que también afecta la reputación general de los parientes cercanos del fallecido, así como la reputación personal. Por lo tanto, cualquier pariente cercano del fallecido, tiene derecho a solicitar a la corte que proteja el derecho al fallecido, o que asuman la responsabilidad de infringir su propia reputación basada en sus parientes cercanos. Para el Tribunal, Baidu Company no tomó las medidas necesarias cuando pudo saber que los usuarios de la red usaban sus servicios de red para infringir los derechos civiles de otros, y no cumplían con las obligaciones de gestión de los proveedores de servicios de red. Baidu Company ha sido condenada a asumir la responsabilidad por daños civiles a

Zhao, configurándose de esta manera, una suerte de Derecho al Olvido en China ya que se configura, al menos jurisprudencialmente, la obligación de eliminar contenidos que infrinjan derechos civiles.

8.5. Derecho al Olvido en Alemania.

I

A) En Alemania cabe destacar [211]"la Sentencia del Tribunal Constitucional Alemán, de 5 de junio de 1973 (BVerfGE 35, 202), afirma que, si bien, en principio, es lícito informar al público sobre ciertos hechos de la vida personal del criminal, en relación con los cuales ha sido declarado culpable, no obstante, el efecto de la irradiación de la protección constitucional de la personalidad impide que los medios de comunicación puedan extender, más allá de la información de hechos de actualidad y sin limitación de tiempo, el tratamiento de datos que conciernen a la persona de un criminal y a su esfera privada".

"En un caso como aquel, la emisión del documental afectaba de manera grave el libre desarrollo de la personalidad, al producir un efecto de estigmatización equivalente a "imponer una nueva sanción social". Una vez satisfecho el interés informativo sobre la actualidad, el derecho del afectado a ser dejado en paz gana peso y pone límites al deseo de los medios de mantener la atención pública sobre su persona. En este conflicto, como afirma el Tribunal, la frontera temporal entre reportaje actual lícito y la posterior reiteración ilícita no puede fijarse en meses o años, sino que el criterio decisivo es determinar si la nueva información

[211] MANRIQUE,T; "Elucubraciones acerca del derecho fundamental al olvido en el Perú y en el derecho comparado, a propósito de su reconocimiento y evolución" California Silicon Valley School of the Law. (2017)

en comparación con la noticia que se difundió en su día constituye un menoscabo nuevo o adicional. En las circunstancias del caso, el documental constituía una lesión adicional y distinta, porque, habiendo pasado un tiempo desde entonces, estaba en juego el interés del recurrente en reinsertarse en la sociedad tras el cumplimiento de la pena."[212].

II

B) Muy interesante es "la jurisprudencia del Tribunal Constitucional Federal alemán acerca del alcance de la protección constitucional del derecho general de la personalidad (art. 2.1 Ley Fundamental de Bonn), dentro del cual, junto a otros derechos de la personalidad, se reconoce un derecho a controlar la presentación de uno mismo ante la sociedad (Recht auf Selbstdarstellung). Según el Tribunal, este derecho no ampara la pretensión de su titular de presentarse ante el público de acuerdo con la imagen de sí mismo o de una manera favorable, sino que le protege frente a representaciones desfiguradoras o distorsionadoras o que afecten significativamente el desarrollo de la persona (sentencia de 24 de marzo de 1998, BVerfGE 97, 391, 403)"[213]. "En principio, si se trata de enunciados verdaderos, este derecho deberá ceder ante el de libertad de expresión, pero no siempre: un reportaje verdadero puede lesionar el derecho del afectado si las consecuencias para el libre desarrollo de la persona son graves y la necesidad de protección prevalece sobre el interés en la difusión de la información. Esta necesidad de protección podrá apreciarse si la información ha sido objeto de una difusión amplia y significativa, y si puede comportar para el afectado un efecto de estigmatización que suponga un riesgo de exclusión o

[212]https://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf
[213]https://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf

aislamiento social. El Tribunal, por tanto, exige una clara cualificación del interés en impedir la difusión de una información verdadera sobre la propia persona. Un ejemplo del grado de afectación del desarrollo de la personalidad que debe alcanzar la información para poder considerarse ilícita lo muestra el siguiente caso: un médico pretendía que un activista contrario al aborto cesara de distribuir panfletos delante de su clínica en los que se afirmaba que en ella se practicaban "abortos ilegales, porque el legislador alemán los permite y no los penaliza", así como que dejara de referirse a él como médico abortista en su página web. El Tribunal Constitucional alemán consideró que las expresiones controvertidas se situaban en el ámbito de la crítica moral a una determinada práctica médica y que no alcanzaban el nivel de gravedad suficiente como para poner en riesgo el respeto y consideración social del demandante: en definitiva, el mero deseo de no verse confrontado públicamente con su libre decisión de practicar abortos y ser criticado por ello no puede prevalecer frente a la libertad de expresión (BVerfG, 1 BvR 1745/06, de 8 de junio de 2010).

8.6. Derecho al Olvido en UK.

I

En Uk hay jurisprudencia sobre el mal uso de la información privada.

Como se desprende, entre otros casos, de Campbell, McKennitt vs Ash y Vidal-Hall[214], este es un agravio que surgió del error equitativo de abuso de confianza bajo la influencia de la Convención Europea de Derechos Humanos, y tiene dos ingredientes esenciales: En primer lugar si el reclamante debe disfrutar de una

[214] Véase [2006] EWCA Civ 1714 [2008] QB 73 [11].

expectativa razonable de privacidad con respecto a la información en cuestión; si eso se establece,la segunda pregunta surge en todas las circunstancias, ¿Deben los derechos del artículo 8 de la Convención Europea de Derechos Humanos del individuo ceder al derecho de libertad de expresión del artículo 10? La última consulta se conoce comúnmente en la jurisprudencia del Reino Unido como el "ejercicio de equilibrio" que se debe llevar a cabo de la manera establecida en el caso Campbell recién citado:

Primero, ninguno de los artículos de la CEDH tiene tanta prioridad sobre el otro. En segundo lugar, cuando los dos artículos están en conflicto, es necesario vislumbrar la importancia comparativa de los derechos específicos que se reclaman en cada caso individual. En tercer lugar, las justificaciones para interferir o restringir cada derecho, deben tenerse en cuenta.

Finalmente, se debe aplicar una regla de proporcionalidad que es lo que jurisprudencialmente se conoce como "la prueba de equilibrio final". Las autoridades proporcionan numerosas ilustraciones de este proceso de equilibrio, que por supuesto es muy sensible a los hechos. La relación entre el mal uso de las leyes de libertad de la información" y las de "protección de datos" se ha discutido en ocasiones. A menudo se considera que ambas leyes conducen a la misma conclusión, por las mismas razones[215]

II

En Reino Unido, los juicios penales tienen lugar en público, y los veredictos dictados y las condenas impuestas son actos públicos. Históricamente, ha sido

[215] véase, por ejemplo, el litigio Campbell v MGN Ltd, Murray v Express Newspapers plc [2007] EWHC 1908 (Ch) [2008] EMLR 22; pero esto no siempre es así: ver Mosley v Google Inc [2015] EWHC 59 (QB) [2015] EMLR 11 [8] - [9] (Mitting J).

legal informar estos asuntos en ese momento y posteriormente con el beneficio de inmunidad absoluta o calificada de responsabilidad, al menos en difamación y desacato al tribunal. La ley, ha impuesto o permitido informar con restricciones en ciertas circunstancias, ya sea para proteger los intereses de privacidad, o los de la administración de justicia, o ambas: ver, por ejemplo, s 2 de la Ley de Delitos Sexuales Enmienda de1992 y Ley de desacato al tribunal de 1981. La cuestión de si, y de ser así, cuándo la información sobre una condena puede contar como un elemento de información confidencial y / o un aspecto de la vida privada de un individuo, se ha considerado en muchísimas de ocasiones en los tribunales del Reino Unido desde 1974. No es hasta hace muy poco que se ha reconocido que información de este tipo puede caer dentro del ámbito de la vida privada de un individuo. Así por ejemplo tenemos las sentencias Elliott v Jefe de policía de Wiltshire[216] donde se sostiene que la confidencialidad no afecta las condenas ejecutadas.

III

Sin embargo, varios casos de derecho público decididos en los últimos 8 años han reconocido que una condena puede, con el paso del tiempo, retroceder tanto en el pasado como para convertirse en un aspecto de la vida privada de un individuo. Tres casos en la Corte Suprema, uno en la Corte de Apelaciones de Irlanda del Norte y uno en la Corte de Apelaciones de Inglaterra y Gales han tocado el tema.

En la Sentencia R (L) vs Comr de Policía de la Metrópolis[217], Lord Hope sugirió que el Tribunal de Estrasburgo mostró que la información sobre condenas "que se recopila y almacena en los registros centrales puede caer

[216] Vease R (Pearson) v DVLA [2002] EWHC 2482 y en el caso L vs Law Society
[217] Véase [2009] UKSC 3 [2010] 1 AC 410 ("L")

dentro del alcance de la vida privada en el sentido del artículo 8 (1), con el resultado de que interferirá con la vida privada del solicitante cuando sea puesto en libertad ". Aunque, en cierto sentido, "la información es pública porque las condenas tuvieron lugar en público" ... "A medida que retrocede en el pasado, se convierte en una parte de la vida privada de la persona que debe ser respetada".

IV

El caso R (T) v Jefe de policía de la Gran Policía de Manchester,[218] Lord Wilson argumentó que "el punto en el que una condena ... retrocede al pasado y se convierte en parte de la vida privada de una persona generalmente será el punto en el que se ha cumplido". El resto de los jueces estuvieron de acuerdo.

V

En Gaughran v Jefe de policía para el Servicio de Policía de Irlanda del Norte[219] la mayoría sostuvo que "el hecho de que una condena pueda ser cumplida es potencialmente relevante pero de ninguna manera es un factor decisivo para considerar dónde reside el equilibrio ", entre los derechos de privacidad de las personas condenadas y las justificaciones de política pública para retener sus datos biométricos.

VI

En CG v Facebook Ireland Ltd[220], se acordó que con el paso del tiempo la protección de un delincuente al prohibir la divulgación de condenas anteriores puede ser superior a los intereses de la justicia.

[218] Véase UKSC [2015] AC 49 ("T")
[219] Véase [2015] UKSC [2016] AC 345 [37],
[220] Véase [2016] NICA 54 [2017] EMLR 12 [44],

VII

En R (P) vs Secretario de Estado para el Departamento del Interior[221], el Tribunal de Apelaciones consideró la legalidad del esquema para la divulgación de condenas, en su forma revisada. El Tribunal concluyó que el vicio identificado por la Corte Suprema era que el esquema requería la divulgación indiscriminada de condenas, sin las garantías adecuadas para permitir un examen adecuado de la proporcionalidad de la interferencia con los derechos del Artículo 8 de la CEDH que involucraba. El balance que requiere la ley fue identificado por el Tribunal de Apelaciones en el "equilibrio entre los derechos de las personas a dejar atrás su pasado y lo que es necesario en una sociedad democrática". Los factores identificados como relevantes para lograr ese equilibrio incluían "la naturaleza del delito, la disposición en el caso, el tiempo transcurrido desde que se cometió el delito o la relevancia de los datos para el empleo buscado":

8.7. Derecho al Olvido en Rusia.

En enero de 2016[222], entró en vigencia la ley sobre el "Derecho al Olvido"[223].

En Rusia, el Derecho al Olvido se introdujo como un derecho especial que no tiene conexión expresa con la protección de datos ya que Ley N ° 264-FZ no modifica la legislación rusa de protección de datos[224]

[221] Véase [2017] EWCA Civ 321[2017] 2 Cr App R 12
[222] Ley Número. 264-FZ de13 de júlio de 2015.
[223] Disponible en https://wipolex.wipo.int/en/legislation/details/17041.(último acceso 28 agosto 2019)
[224] Ver wipolex. Supra.

Si bien la ley se introdujo a raíz del caso de Google España, sus disposiciones difieren en gran medida de los derechos establecidos en la ley de protección de datos de la UE y las recomendaciones hechas por el Tribunal de Justicia de la UE. "Estas divergencias lo convierten en una amenaza para los derechos humanos"[225].

La ley otorga a los ciudadanos rusos el derecho de solicitar a los motores de búsqueda que eliminen los enlaces sobre ellos que violen la ley rusa, sean inexactos, desactualizados o irrelevantes debido a eventos o acciones posteriores.

De conformidad con el artículo 10.3 de la ley[226], una persona puede solicitar la eliminación de URL para búsquedas realizadas en su nombre si dichas URL enlazan con la siguiente información sobre él:

a) información distribuida en violación de las leyes rusas.

b) información inexacta.

c) información irrelevante.

d) información que ha perdido su significado para el individuo por razones de eventos o acciones posteriores del individuo.

Según la asociación Acces Now[227], debido a que la ley no proporciona garantías para proteger el derecho a la libertad de expresión y el acceso a la información, la ley tiene un efecto escalofriante en la expresión y probablemente conducirá a la censura. La ley exige la eliminación del contenido del índice de un motor de búsqueda, en lugar de eliminarlo de la

[225] https://www.accessnow.org/cms/assets/uploads/2017/09/RTBF_Sep_2016.pdf
[226] Íbidem
[227] Íbidem

lista, y no excluye la información relacionada con una figura pública o de interés público.

La obligación de exclusión se aplica a todos los motores de búsqueda[228] que ofrecen publicidad dirigida a los consumidores que residen en Rusia. Este enfoque de exclusión recuerda al TJUE, que estableció que la incorporación de una subsidiaria local que vende publicidad o que hace de motor de búsqueda a veces puede ir en contra las leyes internas de protección de datos[229].

Sin embargo, la Directiva de protección de datos enumera otros posibles casos en los que una empresa extranjera tiene que tener en cuenta la normativa interna de protección de datos, "por ejemplo, en los casos en que una empresa extranjera no está establecida en el Estado miembro, pero para fines de procesamiento hace uso de equipos situados en el territorio de dicho Estado miembro[230]".

Por otro lado, en Rusia existe lo que se llama el derecho de "propósito general"[231]: "Los ciudadanos rusos no solo podrán solicitar la exclusión de información inexacta o irrelevante, sino también cualquier otra información sobre sí mismos que se difunda en contra de las leyes de Rusia", como puede ser terrorismo o temas de drogas.

[228] La ley rusa define lo que es un buscador de internet en el art. 10 de la ley 149-FZ, de 27 de julio de 2006 "Ob informacii, informacionnyh tehnologijah i o zashhite informacii". Ver wipolex. Íb. 205

[229] NURALLEV, R."Right to Be Forgotten in the European Union and Russia" National Research University Higher School of Economics de Moscú (2018).

[230] NURALLEV, R. Ïbidem que cita RGPD, article 4(c). Y el Article 29, Working Party, "Opinion 1/2008 on data protection issues related to search engines". Disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf

[231] NURALLEV, R. Íbidem.

Existen pues, dos instrumentos de control: El bloqueo de esa información que se quiere eliminar y que los tribunales rusos pueden ordenar a los proveedores de acceso a Internet y la eliminación de los resultados de búsqueda que permite la Ley N ° 264-FZ.

Así, el sistema ruso es diferente al sistema de los países de la UE, ya que el interés público juega un papel muy importante a la hora de decidir si se tienen que eliminar las url dodne están alojadas la información. Esta es una limitación general importante al derecho a ser olvidado. Nurallev explica que, en la práctica, esto significa que los buscadores de internet tendrán que considerar una multitud de factores al tomar una decisión sobre si excluir o no. Los operadores de internet atienden a cada situación en función de su conjunto particular de hechos[232].

Por otro lado, la Ley N ° 264-FZ, el parlamento ruso dispuso que los operadores de motores de búsqueda tendrán que eliminar las URL si la información "ha perdido el significado para el solicitante debido a eventos o acciones posteriores del solicitante". En lugar de proteger el "interés público" - como se hace en la Unión Europea de conformidad con la Jurisprudencia del TJUE-, esta disposición parece servir únicamente a los intereses del solicitante[233].

[232] NURALLEV, R, Íbidem.
[233] NURALLEV, R. Íbidem, que cita a Vladimir Zykov, "Roskomnadzor vneset srazu 136 pornosaitov v chernyi spisok" ["Roskomnadzor will add the whole 136 porn websites to the black list"]. Disponible : http://izvestia.ru/news/585309 y "Portal o bitkoinakh popal v spisok zapreshennykh v Rossii saitov" ["Portal on Bitcoins was added to the list of websites banned in Russia"]. Disponible en at: http://lenta.ru/news/2015/01/13/bitcoin/

9. El Derecho al Olvido en la legislación comunitaria europea.

9.1 La Directva 95/46/CE sobre tratamiento de datos personales.

La 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[234], ya derogada, constituyó la norma de referencia sobre la cual deben legislar los países miembros de la Unión Europea sobre la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales[235].

Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos

La Directiva "considera" que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos"[236].

[234] DO L 281de 23.11.1995

[235] Articulo 1 de la Directiva 95/46/CE
[236] Considerando segundo de la Directiva 95/46/CE

Conforme a la explicación dada por la propia Comisión Europea[237], la ya antigua Directiva 95/46/CE, y que era aplicable al caso, tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

-La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

-La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:

i) La ejecución de un contrato en el que el interesado sea parte, o

ii) El cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

iii) Proteger el interés vital del interesado, o

iv) El cumplimiento de una misión de interés público, o

v) La satisfacción del interés legítimo perseguido por el responsable del tratamiento.

- Las categorías especiales de tratamiento: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta

[237] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm (última consulta 16 de agosto de 2018)

disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.

- La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.

- El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:

i) La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;

ii) La rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

- Las excepciones y limitaciones: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

- El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de

oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

- La confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

- La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no

se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo contadas excepciones que se enumeran en el texto.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.

Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión y que en España, a nivel estatal, es la Agencia española de Protección de Datos Personales.

Una de las provisiones más importantes en referencia al Derecho al Olvido es la contenida en el artículo 12.b y en el artículo 14 de la Directiva[238].

Hay que concluir que esta Directiva nacía manifiestamente desfasada respecto a la realidad. No se había previsto, ni remotamente, el auge y el alcance de Internet y de las tecnologías asociadas.

De ahí, que la propia Comisión hubiese completado el contenido de la Directiva 95/46 con el Reglamento (CE) número 45/2001 del Parlamento

[238] Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición del articulo 14 de la Directiva

Europeo y del Consejo, de 18 de Diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de esos datos[239], con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[240].

9.2. El proceso de reforma de la Directiva 95/46/ce para adaptarla al Derecho al Olvido.

Tras quince años de entrada en vigor de la Directiva 95/46/CE, la Comisión, a través de una Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de la Regiones titulada "Un enfoque global de la protección de datos personales en la Unión Europea"[241], reconoció que con la rápida evolución de la tecnología y la globalización, se "han lanzado nuevos retos" en materia de protección de datos personales que han modificado profundamente nuestro medio.

De igual manera se reconoce que los métodos de recogida de datos son cada vez más complejos y se detectan con mayor dificultad -como vamos exponiendo en el caso del Big Data- y que ya no sólo son utilizados, esos datos personales, por entes públicos sino por empresas privadas.

Y hay que añadir que cada vez son más numerosos y se trasmiten entre más partes.

[239] DOUE L 8/1 de 12 de enero de 2001
[240] DOUE L 201 de 31 de julio de 2007, modificada por la Directiva 2009/136/CE (DOUE L 201 de 18 de diciembre de 2009)
[241] COM (2010) 609 final. 20 de julio de 2010.

La Comisión se plantea si la legislación actual puede hacer frente "plena y eficazmente" a estos nuevos retos que se plantean.

La Comisión organizó el estudio del marco jurídico actual para así poder organizar una Conferencia de alto nivel que tuvo lugar en mayo de 2009, a la que siguió una consulta pública hasta diciembre de 2009 y la reunión en Bruselas, en 2010, con todas las partes interesadas y el estudio de diversos Dictámenes, Estudios, Contribuciones y legislación comparada como la de Suecia, Reino Unido, Bélgica y Alemania.

Finalmente, la Comunicación de la Comisión propone clarificar el Derecho al Olvido que define como "el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos", es decir, cuando el interesado "retira su consentimiento al tratamiento de los datos" o de que haya expirado el plazo de conservación de los mismos.

El examen del derecho comparado aportó diferentes contrastes entre legislaciones, aunque todos los países consultados señalaron la necesidad de que la Comisión clarifique la definición del Derecho al Olvido y su separación conceptual del "derecho de cancelación".

Alemania, por ejemplo, propuso que se marcase por ley una "fecha de expiración de los datos"[242].

El Supervisor Europeo de Protección de Datos[243] propone unir el conceptualmente el Derecho al Olvido con el "derecho a la portabilidad" de datos, estableciendo así una obligación del responsable de los datos de

[242]http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/bundesregierung_en.pdf (última consulta 2 de diciembre de 2018)
[243]http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf (última consulta 2 de diciembre de 2018)

cancelar la información tan pronto como deje de cumplirse la finalidad de éstos. Propone, en general, una "nueva codificación" del Derecho al Olvido donde se invierta la carga de prueba y se instaure una "privacidad por defecto" y, lo que es más importante, "una privacidad deliberadamente obligada"

9.3. La problemática europea con el Derecho al Olvido

9.3.1. Los antecedentes del caso Google.

Según las Conclusiones del Abogado general del TJUE[244], los hechos que se produjeron fueron los siguientes:

A comienzos de 1998, un periódico español de gran tirada, La Vanguardia, publicó en su edición impresa dos anuncios relativos a una subasta de inmuebles relacionada con un embargo derivado de deudas a la Seguridad Social. Se mencionaba al interesado como propietario de éstos. En un momento posterior, la editorial puso a disposición del público una versión electrónica del periódico online.

En noviembre de 2009, el interesado contactó con la editorial del periódico afirmando que, cuando introducía su nombre y apellidos en el motor de búsqueda de Google, aparecía la referencia a varias páginas del periódico que incluían los anuncios de la mencionada subasta de inmuebles. Alegó que el embargo estaba solucionado y resuelto desde hacía años y carecía de

[244]http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=274971 (última visita 8 de octubre de 2018)

relevancia en aquel momento. La editorial le respondió que no procedía la cancelación de sus datos, dado que la publicación se había realizado por orden del Ministerio de Trabajo y Asuntos Sociales.

En febrero de 2010, el interesado remitió escrito a Google Spain solicitando que al introducir su nombre y apellidos en el motor de búsqueda en Internet de Google no aparecieran en los resultados de búsqueda enlaces a ese periódico. Google Spain le remitió a Google Inc., con domicilio social en California, Estados Unidos, por entender que ésta era la empresa que presta el servicio de búsqueda en Internet.

En consecuencia, el interesado interpuso una reclamación ante la AEPD solicitando que se exigiese a la editorial eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger sus datos personales. También solicitaba que se exigiese a Google España o a Google que eliminaran u ocultaran sus datos para que dejaran de incluirse en sus resultados de búsqueda y ofrecer los enlaces al periódico.

Mediante resolución de 30 de julio de 2010, el Director de la AEPD estimó la reclamación formulada por el interesado contra Google Spain y Google Inc., instándoles a adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos.

Pero desestimó la reclamación contra la editorial porque la publicación de los datos en la prensa tenía justificación legal. Google Spain y Google Inc. interpusieron recursos ante la Audiencia Nacional en los que solicitaban la nulidad de la resolución de la AEPD.

La AN declaró que los recursos planteaban la cuestión de cuales eran las obligaciones que tenían los gestores de motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros, que contiene sus datos personales y permite relacionarles con la misma, sea localizada, indexada y puesta a disposición de los internautas de forma indefinida. Y esta cuestión dependía de la interpretación que se le diese a la Directiva 95/46.

En conclusión, se considera que el diario La Vanguardia no tiene por qué retirar la publicación de Internet, pero Google sí que debe dejar de indexar los datos, ya que se está considerando que Google es el responsable de los datos, no ya sólo el responsable del tratamiento de los datos, dando carta de naturaleza a la presunción de que los datos "pertenecen" a Google.

9.3.2. La cuestión prejudicial ante el TJUE.

Así las cosas, la Sala de lo Contencioso-administrativo de la Audiencia Nacional plantea al Tribunal de Justicia de la UE una cuestión prejudicial de interpretación sobre la protección de datos de un particular frente a Google. Con su resolución, la AN describe jurídicamente la situación creada ante las nuevas tecnologías que traspasan fronteras y límites temporales y que se han desarrollado con posterioridad a las normativas vigentes. Es la primera vez que un tribunal planteaba esta cuestión ante el Tribunal de Justicia de la UE sobre esta cuestión.

La cuestión prejudicial de la Audiencia Nacional planteaba de fondo si un particular tiene derecho a reclamar la supresión y bloqueo de informaciones

en los buscadores de Internet relativas a su persona y que, con las nuevas tecnologías, podrán ser localizadas "a lo largo de toda su vida y la de sus descendientes".

La cuestión prejudicial contiene nueve preguntas, divididas en tres "dudas", al TJUE. La Sala de la AN entiende que el recurso plantea "el problema referido a las obligaciones que tienen los buscadores de Internet en la protección de datos personales de aquellos afectados que no desean que determinadas informaciones, publicadas en páginas web de terceros y que contienen sus datos personales y permiten relacionarles con la misma, sean localizadas, indexadas y sean puestas a disposición de los internautas de forma indefinida".

La primera duda que se plantean los jueces es si la normativa comunitaria y nacional en materia de protección de datos se puede aplicar en este caso o, si como sostiene la empresa Google Inc., los afectados deberían acudir a los tribunales de California (EEUU) donde está domiciliada la empresa matriz del grupo.

Se pregunta también la Sala si los buscadores, cuando indexan la información, están realizando un tratamiento de datos personales, si son responsables de ese tratamiento y deben atender por tanto a los derechos de cancelación y/o oposición del afectado de forma directa, aunque la información se mantenga en la fuente originaria por considerarse lícita.

Finalmente, los jueces preguntan al Tribunal de Luxemburgo si la protección de datos incluye que el afectado se niegue a que una información referida a su

persona se indexe y difunda, aun siendo lícita y exacta en su origen, pero que la considere negativa o perjudicial para su persona.[245]

9.3.3 El informe del Abogado General.

I

En las cuestiones prejudiciales ante el TJUE, el Abogado General de la Comisión emite un dictamen el cual será tenido en cuenta por el TJUE a la hora de redactar su Sentencia.[246]

Antes de proceder a entrar en el fondo de las diversas cuestiones planteadas al TJUE , el Abogado General emitió una serie de observaciones preliminares a modo de antecedentes.

Para el Abogado General, cuando la Directiva fue adoptada en 1995, se le dio una amplia gama de aplicaciones "ratione materiae" para que la Directiva pudiera ponerse al día con los desarrollos tecnológicos relacionados con el proceso de datos. En 1995 el acceso ilimitado a Internet era algo, en gran medida, muy novedoso.

Tal y como señala el abogado General "*Sin embargo, está claro que el legislador comunitario no previó la evolución de Internet hacia un almacén*

[245]http://www.poderjudicial.es/portal/site/cgpj/menuitem.0cb0942ae6fBig Dataa1c1ef62232dc432ea0/?vgnextoid=a0cca049Big Data2d5310VgnVCM1000006f48ac0aRCRD&vgnextchannel=3a20f20408619210VgnVCM100000cb34e20aRCRD&vgnextfmt=default (última consulta 30 de novembre de 2018)
[246] http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES

global y exhaustivo de información a la que se accede, o se busca, en todo el mundo.".

Y señala una no menos importante observación: "*De hecho, hoy en día cualquier persona que lea un periódico en una tableta o que siga redes sociales en un smartphone parece estar involucrado en el tratamiento automatizado de datos personales y podría estar incluido en el ámbito de aplicación de la Directiva, en la medida en que tiene lugar fuera de su ámbito meramente privado. Además, la amplia interpretación dada por el Tribunal de Justicia al derecho fundamental a la vida privada en el contexto de la protección de datos parece someter a toda comunicación humana mediante medios electrónicos a un análisis a la luz de este derecho."*

Para el abogado General, es necesario establecer un equilibrio correcto, razonable y proporcionado[247] entre la protección de datos personales, la interpretación congruente de los objetivos de la sociedad de la información y los intereses legítimos de los operadores económicos y de los usuarios de Internet en general. Aunque la Directiva no había sido modificada desde su adopción en 1995, su aplicación a nuevas situaciones fue inevitable. Es un área jurídica compleja en la que se cruzan Derecho y tecnología

Así, las definiciones amplias de "datos personales", "tratamiento de datos personales" y "responsable del tratamiento de dato " en la Directiva es probable, decía el Abogado General, que no cubran una amplia gama de nuevos situaciones de hecho debido al incremento, sofisticación y desarrollo de tecnológica.

[247] El principio de proporcionalidad nos lo encntramos en el artículo 1 del TFUE

El Abogado General observó que, si bien el TJUE había dictaminado previamente en el caso Lindqvist[248] que "*La conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento [de datos personales*]" , y que " *la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva*", sin embargo rechazó una interpretación de la Directiva que habría sido "*poco razonable*",

Eso significaba la carga por un individuo de datos sobre a una página de Internet, aunque en los datos originales se hubiesen puesto a disposición a personas de terceros países, no equivalía a una transferencia de datos en virtud del art.25[249] de la Directiva, ya que no sería racional.

El Abogado General considera importante señalar que hay que distinguir entre la responsabilidad de la editor de la fuente páginas web que contiene los datos personales -donde claramente hay que considerar que ese editor es el "responsable" en el tratamiento de los datos personales vinculado por todas las obligaciones pertinentes que la Directiva impone a los responsable de los tratamientos de datos-, y la de un proveedor de servicios de motores de

[248] http://curia.europa.eu/juris/document/document.jsf?docid=47672&doclang=ES

[249] 1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

búsqueda de Internet que proporciona acceso a los datos publicados por tercero, que el Abogado General, califica como una cuestión de "*responsabilidad subsidiaria*", muy diferente de la de los que han publicado la información. No es proporcional comparar ambas responsabilidades.

El Abogado General afirma[250] que "en mi opinión, la cuestión clave en el presente asunto es si tiene importancia que dentro de la definición de responsable del tratamiento la Directiva se refiera a éste como la persona que «determina los fines y los medios del tratamiento de datos personales»". Las partes que consideran que Google es un responsable del tratamiento basan su aserto en el hecho innegable de que el proveedor de servicio que gestiona un motor de búsqueda en Internet determina las finalidades y los medios del tratamiento de datos para sus propios fines.

"Sin embargo, dudo de que ello lleve a una interpretación veraz de la Directiva en una situación en la que el objeto del tratamiento consiste en archivos que contienen datos personales y otro tipo de datos expuestos de manera descuidada, indiscriminada y aleatoria".

Para el Abogado General, un proveedor de servicios de motor de búsqueda de Internet, como Google en el caso que nos ocupa, no tiene relación con el contenido de la fuente web de terceras personas en las que pueden aparecer los datos personales. Como motor de búsqueda funciona sobre la base de copias de las páginas web, que obtiene a través de un rastreador de código que la función de rastreador web ha recuperado y se copia, El proveedor de servicio no tiene ningún medio de poder manipular la información en el servidor. Es más, ni siquiera puede distinguir si la información se refiere a

[250] Apartados 80 y 81 del informe del Abogado General antes citado.

datos de una persona viva o a cualquier otro tipo de datos. Sobre esta base, el Abogado General concluyó que, en general, un proveedor de servicios de motor de búsqueda de Internet no puede ser considerado como un responsable de control de datos bajo la Directiva. La única excepción seria cuando el buscador no ha cumplido con los códigos de excepción de búsqueda del editor de la información o cuando una petición que emana de la página web con respecto a la actualización de la memoria caché no se ha cumplido. Sólo entonces, el buscador web podría ser considerado como responsable de la información.

Y parece que aún se puede añadir algo más. Si no hay responsabilidad para los buscadores de internet sobre datos subidos a la red por terceros, ¿Acaso la habría por los datos que nosotros hemos subido libremente? ¿Dónde queda la responsabilidad personal? ¿Por qué Google, en este caso, tiene que asumir unas obligaciones por acciones nuestras –de manera voluntaria- que ahora no queremos recordar o asumir?

Sobre el Derecho al Olvido en particular, el Abogado general considera que "No obstante, como han afirmado casi todas las partes que han presentado observaciones escritas en el presente asunto, considero que la Directiva no establece un derecho general al olvido, en el sentido de que un interesado esté facultado para restringir o poner fin a la difusión de datos personales que considera lesivos o contrarios a sus intereses. La finalidad del tratamiento y los intereses a los que sirve, al compararse con los del interesado, son los criterios que han de aplicarse cuando se procesan datos sin el consentimiento del interesado, y no las preferencias subjetivas de éste. Una preferencia subjetiva por sí sola no equivale a una razón legítima, en el sentido del artículo 14, letra a), de la Directiva.

Aunque el Tribunal de Justicia declarase que los proveedores de servicios de motor de búsqueda en Internet se responsabilizan, como responsables del tratamiento, quod non, de los datos personales contenidos en las páginas web fuente de terceros, un interesado tampoco tendría un «Derecho al Olvido» absoluto que pudiera invocar frente a los proveedores de servicios. Sin embargo, el proveedor de servicios necesitaría ponerse en la posición del editor de la página web fuente y comprobar si la difusión de los datos personales en la página web podría considerarse legal y legítima a los efectos de la Directiva. Dicho de otro modo, el proveedor de servicios necesitaría abandonar su función de intermediario entre usuario y editor y asumir la responsabilidad por el contenido de la página web fuente y, cuando resultase necesario, censurar el contenido evitando o limitando el acceso a éste."

II

En el apartado 138 de su Dictamen, el Abogado General de la Comisión concluye:

"*A la luz de las observaciones precedentes, propongo al Tribunal de Justicia que responda del siguiente modo a las cuestiones prejudiciales planteadas por la Audiencia Nacional:*

«1) Se lleva a cabo tratamiento de datos personales en el marco de las actividades de un «establecimiento» del responsable del tratamiento, en el sentido del artículo 4, apartado 1, letra a), de la 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, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, con el fin de

promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado.

2) Un proveedor de servicios de motor de búsqueda en Internet cuyo motor de búsqueda localiza información publicada o incluida en Internet por terceros, la indexa automáticamente, la almacena con carácter temporal y, por último, la pone a disposición de los usuarios de Internet, «trata» datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46 cuando esta información contiene datos personales.

Sin embargo, no se puede considerar al proveedor de servicios «responsable del tratamiento» de tales datos personales, en el sentido del artículo 2, letra d), de la Directiva 95/46, a excepción de los contenidos del índice de su motor de búsqueda, siempre que el proveedor del servicio no indexe o archive datos personales en contra de las instrucciones o las peticiones del editor de la página web.

3) Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido.»

10. La sentencia de 13 de mayo de 2014 del TJUE sobre el Derecho al Olvido.

La Sentencia del TJUE se basa en las nueve cuestiones preguntadas por la AN y que se pueden agrupar de la siguiente manera.

1. ¿La normativa Europea se le debe aplicar a Google –una empresa con sede en California-? ¿Debe entenderse que Google realiza "tratamiento de datos"? Y en caso afirmativo ¿Google es responsable de ese "tratamiento de datos"?
2. ¿Se puede imponer a Google la cancelación de los datos de terceros sin tener que acudir a la página en que se ubica la publicación?
3. ¿Cuál es el alcance del Derecho al Olvido?

Vamos a estudiar separadamente todas estas cuestiones para una mayor precisión.

I

En primer lugar cabe aquí considerar si la normativa europea es aplicable a Google.

En las cuestiones prejudiciales, la Secretaría del Tribunal de Luxemburgo envía requerimiento a los países miembros para que aleguen lo que estime conveniente en el caso en cuestión.

Italia, Alemania, Austria y Polonia, así como la Comisión, se alinean con el demandante.

El Gobierno Griego, por su parte, comparte las tesis de Google (en este caso Google Spain y Google inc).

Para Google -tanto Google Spain como Google inc-, la normativa Europea no les es de aplicación porque la empresa que presta el servicio de motor de búsqueda -Google Search- no es europea, ya que está ubicada en Estados Unidos. La información indexada por sus «arañas» o robots de indexación, es decir, programas informáticos utilizados para rastrear y realizar un barrido del contenido de páginas web de manera metódica y automatizada, se almacena temporalmente en servidores cuyo Estado de ubicación se desconoce, ya que este dato es secreto por razones competitivas.
Google Spain es sólo una entidad filial que se dedica a la venta de servicios, a clientes de dentro de España, de publicidad dentro de su buscador. Y solo eso. Y, por tanto, al no mantener ninguna relación ni ningún tipo de intervención con Google Search, no se le puede aplicar el Derecho de la Directiva.

Esa misma tesis es compartida como hemos dicho, por el Gobierno Heleno.

Las otras partes no opinan lo mismo, habida cuenta del vínculo indisociable entre la actividad del motor de búsqueda gestionado por Google Inc. y la de Google Spain, ésta debe considerarse un establecimiento de aquélla, en el marco de cuyas actividades se lleva a cabo el tratamiento de datos personales.

El TJUE aprecia, por su parte, que no se discute que Google Spain se dedique al ejercicio efectivo y real de una actividad dentro de España con una instalación estable y que además considera acreditado que es una filial de Google Inc. y, por lo tanto, un «establecimiento», en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46. Esto es importante porque sobre este particular, procede recordar, en primer lugar, que el considerando 19 de la Directiva aclara que «el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una

instalación estable», y «que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante».

A la vista de lo anterior, el TJUE da la razón al demandante y considera que sí que existe una vinculación y declara la aplicación de la Directiva de Protección de Datos y las leyes nacionales a todas aquellas multinacionales que aun no teniendo su sede en un país de la Unión Europea, cuenten con oficinas en los principales países europeos, aun cuando éstas sean sólo ″una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios″.

Es muy importante el inciso que establece el TJUE, pues para cumplir el requisito establecido en la Directiva 95/46, es necesario además que el tratamiento de datos personales por parte del responsable del tratamiento se «lleve a cabo en el marco de las actividades» de un establecimiento de dicho responsable situado en territorio de un Estado miembro, y no necesariamente "por" el establecimiento, tal y como quisieron señalar la Comisión, a través del Dictamen del Abogado General, y el gobierno español.

Como hemos visto anteriormente, Google Spain y Google Inc. niegan que éste sea el caso, dado que el tratamiento de datos personales controvertido en el litigio principal lo lleva a cabo exclusivamente Google Inc., que gestiona Google Search sin ninguna intervención por parte de Google Spain, cuya actividad se limita a prestar apoyo a la actividad publicitaria del grupo Google, que es distinta de su servicio de motor de búsqueda.

Entendemos que se pueden hacer numerosas críticas al hecho de que se obligue a estar sometido a la Directiva de protección de datos europea a una

empresa americana por el mero de hecho de tener una filial comercial en Europa. Cabe suponer, a sensu contrario, que si la filial comercial no se localiza en Europa, la Directiva no se les aplicará. Muchas de estas críticas ya han sido expuestas.[251] Tal y como exponen Botana y Ovejero[252]:

"El Tribunal no vincula la aplicación de las obligaciones derivadas del derecho europeo al estatuto de la persona perjudicada (ciudadano de uno de los países miembros de la UE y sujeto de derecho fundamental), ni tampoco a que la página de origen de los datos corresponda con una empresa europea. A pesar de que su novedosa interpretación de la Directiva está fundamentada en la mayor efectividad y eficacia del Derecho Fundamental de la Carta, lo importante no es que sea o no un ciudadano europeo el perjudicado, y por lo tanto el protegido, sino que se tenga o no sede comercial en la UE. El ámbito de protección del derecho a la intimidad reconocido en el art.8 de la Carta se extiende a todas las personas que sean o puedan ser sujetos de "búsquedas" de empresas de "motores de búsqueda", estén donde estén ubicadas, pero recordemos que la interpretación de la Directiva limita el uso de las herramientas de defensa a aquellas empresas que tienen sedes comerciales en Europa.".

El Tribunal considera que, de no aplicar a Google Search la Directiva Europea de protección de datos, se acabaría "menoscabando el efecto útil y la protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas que tienen por objeto garantizar la

[251] BOTANA, G.A y OVEJERO, A.M. "Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de Mayo de 2014 en la cuestión prejudicial planteada en el caso Google." Universidad Europea de Madrid.(2014)
[252] Íbidem,.

Directiva 95/46 y el respeto de la vida privada en lo que respecta al tratamiento de datos personales".

Como vuelven a exponer Botana y Ovejero[253]:

"El criterio territorial se amplía por aplicación de un criterio de conexión comercial, de lo que se deriva el segundo problema, pues no todas las búsquedas responden a criterios publicitarios. Sólo están "comercialmente conectadas" las búsquedas relacionadas con actividad comercial, luego no es coherente con este argumento que se exija el mismo nivel de responsabilidad sobre búsquedas sin conexión con la actividad comercial de Google, hechas solo y exclusivamente por la empresa Google Search."

II

En segundo lugar, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea la nacionalidad o residencia de la persona, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal.

[253] Ibidem en 249

El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos.

A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él.

La definición de tratamiento de datos personales incluida en el art. 4.2) del RGPD se ciñe a cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Anteriormente, el articulo 4 de la Directiva 95/46/CE definía el tratamiento como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;”

El TJUE ya tuvo ocasión de declarar que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un «tratamiento» de esta índole, en el sentido del artículo 2, letra b), de la Directiva 95/46[254]

Por consiguiente, el TJUE declara en la sentencia del Caso Google que, al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas.

Para el TJUE, ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, debían calificarse de «tratamiento» en el sentido de dicha disposición, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales.

Para el Tribunal, tampoco contradice la apreciación anterior el hecho de que estos datos hayan sido ya objeto de publicación en Internet y dicho motor de búsqueda no los modifique. De este modo, el TJUE ya ha declaró que las operaciones a las que se refiere el artículo 2, letra b), de la Directiva 95/46 deben calificarse de tal tratamiento también en el supuesto de que se refieran únicamente a información ya publicada tal cual en los medios de comunicación.

[254] véase la sentencia Lindqvist. STJUE de 6 de noviembre de 2003 en el asunto C-101/01

III

En tercer lugar, el art. 2.d) de la Directiva 95/46 definía al responsable como «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales».

Para el TJUE, el gestor del motor de búsqueda es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de ésta y, por consiguiente, debe considerarse «responsable» de dicho tratamiento en virtud del mencionado artículo 2, letra d) Por otro lado, la Sentencia declara que sería contrario, no sólo al claro tenor de la Directiva 95/46 sino también a su objetivo, consistente en garantizar, mediante una definición amplia del concepto de «responsable», una protección eficaz y completa de los interesados, excluir de esta disposición al gestor de un motor de búsqueda debido a que no ejerce control sobre los datos personales publicados en las páginas web de terceros.

El Tribunal pone de manifiesto que el tratamiento de datos personales llevado a cabo en el marco de la actividad de un motor de búsqueda se distingue del efectuado por los editores de sitios de Internet, que consiste en hacer figurar esos datos en una página en Internet, y se añade a él, considerando que es pacífico que esta actividad de los motores de búsqueda desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos.

Para el TJUE, la organización y la agregación de la información publicada en Internet efectuada por los motores de búsqueda para facilitar a sus usuarios el acceso a ella puede conducir, cuando la búsqueda de los usuarios se lleva a cabo a partir del nombre de una persona física, a que éstos obtengan mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet que les permita establecer un perfil más o menos detallado del interesado.

En consecuencia, para el TJUE, en la medida en que la actividad de un motor de búsqueda puede afectar, significativamente y de modo adicional a la de los editores de sitios de Internet, a los derechos fundamentales de respeto de la vida privada y de protección de datos personales, el gestor de este motor, como persona que determina los fines y los medios de esta actividad, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicha actividad satisface las exigencias de la Directiva 95/46 para que las garantías establecidas en ella puedan tener pleno efecto y pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada.

Considera también el TJUE que el que los editores de sitios de Internet tengan la facultad de indicar a los gestores de los motores de búsqueda, con la ayuda, concretamente, de protocolos de exclusión como «robot.txt», o de códigos como «noindex» o «noarchive», que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores, no significa que la falta de tal indicación por parte de estos editores libere al gestor de un motor de búsqueda de su responsabilidad por el tratamiento de datos personales que lleva a cabo en el marco de la actividad de dicho motor.

Considera también que esta circunstancia no modifica el hecho de que el gestor determina los fines y los medios de este tratamiento. Además, aun suponiendo que dicha facultad de los editores de sitios de Internet signifique que éstos determinen conjuntamente con dicho gestor los medios del mencionado tratamiento, tal afirmación no elimina en modo alguno la responsabilidad del gestor, ya que el artículo 2, letra d), de la Directiva 95/46 prevé expresamente que esta determinación puede realizarse «sólo o conjuntamente con otros».

Por tanto, del conjunto de las consideraciones precedentes se desprende , por un lado, que la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro lado , que el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d).

Según Google Spain y Google Inc., la actividad de los motores de búsqueda no puede considerarse tratamiento de los datos que se muestran en las páginas web de terceros que presenta la lista de resultados de la búsqueda, dado que estos motores tratan la información accesible en Internet globalmente sin seleccionar entre datos personales y el resto de información. En su opinión, además, aun suponiendo que esta actividad deba ser calificada de «tratamiento de datos», el gestor de un motor de búsqueda no puede considerarse «responsable» de ese tratamiento, ya que no conoce dichos datos y no ejerce control sobre ellos.

En cambio, los Gobiernos español, italiano austriaco y polaco y la Comisión Europea sostienen que dicha actividad implica claramente un «tratamiento de datos», en el sentido de la Directiva 95/46, que es distinto del tratamiento de datos realizado por los editores de los sitios de Internet y persigue objetivos distintos al de éste. A su juicio, el gestor de un motor de búsqueda es «responsable» del tratamiento de datos efectuado por él desde el momento en que es él quien determina la finalidad y los medios de dicho tratamiento.

En definitiva, el TJUE considera a Google como "responsable" de los datos, imponiendo una suerte de responsabilidad solidaria con la página que alberga la información. Y así, si la página que hospeda los datos no atiende los requerimientos del particular, será el buscador el que tenga que desindexarlos para que así "nadie" los pueda encontrar.

En relación a esta Sentencia, podríamos entender que los motores de búsqueda, de ninguna manera, determinan la finalidad por la cual se busca la información, pues estaríamos atribuyendo al motor de búsqueda una suerte de inteligencia artificial aunque bien es cierto que también se ha reportado sesgos sociales en algunas búsquedas en determinadas redes sociales o buscadores[255].

Cabe en este punto si no sería más acertado decir que quien marca la finalidad es quien introduce en el buscador el nombre de la persona. Sobre este punto cabría argumetar que el procesamiento de datos no significa automáticamente que la persona sea también el «responsable» de que los datos. El responsable es aquella una persona que determina los fines y medios del tratamiento de los datos personales. En cuanto a la intereses de la sociedad de la información

[255] Ver, por ejemplo, https://es.theepochtimes.com/robert-epstein-como-el-sesgo-de-los-gigantes-tecnologicos-amenaza-las-elecciones-libres-y-justas_527732.html

y el principio de proporcionalidad una persona sólo puede ser el responsable si sabe qué tipo de datos personales procesa. Bajo esta premisa, el concepto de proceso de datos está intrínsecamente ligado a que el responsable posea un dato que le sea relevante, ordenado y semánticamente reconocible y no como mero código de computación.

Por lo tanto Google –que simplemente suministra una información-, si continuamos bajo la premisa anterior, de ninguna manera tendría control sobre el contenido de los sitios web de terceros, y ni siquiera es capaz de distinguir entre los datos personales y otros datos. Google no podría, por estas razones, ni fácticamente ni legalmente, cumplir con las obligaciones que se establecían en la Directiva 95/46. Esta consideración también coincide con la Directiva de E- commerce[256] (art. 12, 13 y 14) que establece que una persona

[256] Directiva 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), DOUE 178, 17.7.2000.

Artículo 12
Mera transmisión
1. Los Estados miembros garantizarán que, en el caso de un servicio de la sociedad de la información que consista en transmitir en una red de comunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones, no se pueda considerar al prestador de servicios de este tipo responsable de los datos transmitidos, a condición de que el prestador de servicios:

a) no haya originado él mismo la transmisión;

b) no seleccione al destinatario de la transmisión; y

c) no seleccione ni modifique los datos transmitidos.

2. Las actividades de transmisión y concesión de acceso enumeradas en el apartado 1 engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.

3. El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida.

Artículo 13
Memoria tampón (Caching)
1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos, a condición de que:

a) el prestador de servicios no modifique la información;

b) el prestador de servicios cumpla las condiciones de acceso a la información;

c) el prestador de servicios cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector;

d) el prestador de servicios no interfiera en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y

e) el prestador de servicios actúe con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella será imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, de que se ha imposibilitado el acceso a dicha información o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella.

2. El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios poner fin a una infracción o impedirla.

Artículo 14
Alojamiento de datos
1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

a) el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que,

b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

2. El apartado 1 no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios.
3. El presente artículo no afectará la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de

no es responsable -en general- si no tiene ningún control sobre el contenido automático y / o almacenado.

En base a lo anterior, sería posible entender que Google no podía adoptar, a nuestro entender, medidas eficaces para que la información desaparezca, pues un mero cambio de enlace por parte del editor de la información, hará que los datos, irremediablemente, vuelvan a aparecer en los resultados de búsqueda.

Son los editores de las páginas web los que tienen el poder de que algo aparezca o no en internet, con las herramientas de exclusión de las que disponen tipo "norobot" o "noindex".

Si vamos un paso más allá y pensamos en la teoría del primer causante, tan utilizada en la jurisprudencia anglosajona, ¿No tendrían también responsabilidad las compañías telefónicas que permiten el acceso a la Red?

Además, los datos siguen ahí hospedados en la página original. Hay que entender que no por esconder los datos en los buscadores, dejan de existir.

Se forzaba a los buscadores de internet, considerando las premisas anteriormente vistas, a que interactuasen con unos datos sobre los que no tienen ningún control, forzándoles al cumplimiento de la Directiva Europea incluso si la información es lícita y veraz.

La ejecución de la Sentencia ahora analizada, puede entenderse que puede tener serios efectos colaterales: Se priva a los buscadores de los datos, que constituyen su "core business" –tanto del propio buscador como de las

servicios de poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos.

empresas asociadas- y podría llegar a producirse que los buscadores tuviesen que comprobar si la información contenida en la página de hospedaje cumple con la normativa de protección de datos del país o zona en cuestión, cosa que puede contravenir la propia jurisprudencia del TJUE[257]que afirma que cualquier sistema de filtrado que obligue a proceder a una supervisión activa del conjunto de datos sería contrario al art. 15 de la Directiva 95/46.

Apuntar también que la Sentencia analizada parece desconocer la importancia económica de los buscadores. Algunos medios de comunicación reciben el 40%[258] de sus visitas gracias a los buscadores. Esto demuestra, a nuestro entender, que si los buscadores dejan de indexarles, su negocio cae en picado por la pérdida de publicidad. Es algo ciertamente que debiera haberse tenido en cuenta a la hora de ponderar los Derechos de las partes.

III

En tercer lugar, una vez la sentencia del TJUE ha concluido que la actividad de los buscadores ha de considerarse como "tratamiento de datos" y que estos buscadores son "responsables" de la información, se declara la obligación para los Buscadores de eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en si misma lícita.

[257] Sentencia Tribunal Justicia UE caso C-70/10 Scarlet/Sabam.
[258] http://www.adamsherk.com/seo/google-news-traffic-for-news-sites/ (última visita 11 de diciembre de 2018)

Es aquí, con esta consideración, donde el TJUE viene a reconocer el "Derecho al Olvido", aunque sin citarlo expresamente. Lo entiende como una extensión de los derechos de "cancelación" y "oposición", tal y como alegaba la Agencia Española de Protección de Datos.

IV

Comentario aparte merece el apartado 83 de la STJUE.

En él se establece que "el gestor de este motor, como responsable del tratamiento, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicho tratamiento cumple los requisitos de la Directiva 95/46, para que las garantías que ella establece puedan tener pleno efecto."

Es decir, a la vista de que el TJUE establece de manera genérica la "responsabilidad" de los buscadores, sobre estos puede caer las sanciones previstas en el artículo 24 de la Directiva[259]. Lo mismo puede decirse de las "categorías especiales de datos" del artículo 8[260] de la Directiva. Si se da el caso de que una búsqueda en Google, contiene alguna de esta categoría especial de datos, el buscador podría ser considerado como ilegal al haber realizado un "tratamiento de datos" expresamente prohibido por la Directiva, y por lo tanto obligado a suspender o abandonar sus actividades.

[259] Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

[260] Artículo 8 Tratamiento de categorías especiales de datos
1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

Hay que entender que se ha establecido, pues, una suerte de responsabilidad solidaria con el editor de los datos. Esta especie de "huida hacia adelante" del TJUE ha sido calificada por algunos estudiosos como "perseguir al mensajero"[261].

De lo anterior se puede extraer que el Derecho al Olvido es mucho más que el derecho a la protección de la privacidad y de los datos personales. Tiene que ser reconocido como un Derecho independiente, que englobe las diferentes particularidades que se dan en cada legislación y que pueda ser ejercido en todo el mundo, sin importar la nacionalidad de la empresa o el lugar geográfico en dónde se encuentre el usuario. Que sea fácil de entender y que la protección del Derecho al Olvido no genere costes ni al usuario ni las empresas de Internet.

Hay que concluir, pues, que el propio TJUE establece una especie de "graduación" de Derecho al Olvido, dependiendo del papel del particular en la "vida pública". Nos tendremos que preguntar cómo se gradúa la participación en la "vida pública" y si la información contenida en un boletín oficial puede entenderse como tal.

Y tal graduación deberá hacerse en dos fases. La primera la hará Google, al que se le dirigirá la solicitud, y la segunda –si Google rechaza borrar los datos- se hará en los Tribunales de Justicia, sin duda atendiendo a otros parámetros.

[261] CEREZO,P; "No le eches la culpa al mensajero" http://sociedad.elpais.com/sociedad/2014/05/13/actualidad/1400016320_842313.html (útima visita 10 de diciembre de 2018)

11. La sentencia de 24 de septiembre de 2019 del TJUE sobre el Derecho al Olvido. Asunto c-507/17.

11.1. Antecedentes.

I

Con estos antecedentes que acabamos de exponer, y una vez establecido el Derecho al Olvido por el TJUE, al implementar las solicitudes que Google consideró apropiadas, esta compañía limitó la desindexación a los dominios donde se originaron las solicitudes, como Google.es o Google.fr, de manera que los resultados siguieran apareciendo si se realizaban búsquedas en dominios de otros países fuera Europa, como en Rusia o en Chile. Eso significa que puede acceder a Google.com en Francia y ver los resultados que se excluyeron en Google.fr. La compañía argumentó que hacer cumplir la desindexación a nivel mundial resultaría en la violación de la libertad de expresión en otros países.

II

La autoridad de protección de datos francesa, CNIL (Comisión Nacional de Información y Libertades), no estaba satisfecha con la forma en que Google implementó la decisión en Francia. Notificó a la compañía, solicitando que los resultados se excluyeran de todos los dominios de Google, es decir, que estos resultados no se mostrarían si se realizaran búsquedas en todos los sitios web de Google en todo el mundo.

En respuesta, Google decidió expandir las eliminaciones según los criterios de geolocalización de las direcciones IP de búsqueda. Los resultados de búsqueda fueron, entonces, excluidos a todos los usuarios con la IP del país

de origen de las solicitudes finalmente aceptadas por Google, dentro de la Unión Europea. En la práctica, esto significa que una solicitud presentada por alguien en Alemania, por ejemplo, y aceptada por Google, daría como resultado la eliminación del enlace mencionado en la solicitud de todos los dominios europeos de la empresa y la desindexación de este enlace en todos los demás dominios para usuarios con una IP alemana. Es decir, los usuarios ubicados en Alemania, no verían tales resultados, incluso accediendo a Google.com.

CNIL, sin embargo, continuó considerando que la forma en que Google implementa el Derecho al Olvido era inadecuada, entendiendo que la desindexación debería ocurrir de manera global en todo el mundo e impuso a Google una multa de 100.000 euros además de peticionar informe al Consejo de Estado Francés quien planteó una cuestión prejudicial ante el TJUE el 21 de agosto de 2017[262] sobre las siguientes cuestiones:

1) ¿Debe interpretarse el «derecho de retirada», según ha sido consagrado por el Tribunal de Justicia de la Unión Europea en su sentencia de 13 de mayo de 2014 1 sobre la base de las disposiciones de los artículos 12, letra b), y 14, letra a), de la Directiva de 24 de octubre de 1995, 2 en el sentido de que el gestor de un motor de búsqueda que estima una solicitud de retirada está obligado a efectuar dicha retirada respecto de la totalidad de los nombres de dominio de su motor, de tal manera que los vínculos controvertidos dejen de mostrarse independientemente del lugar desde el que se realice la búsqueda a partir del nombre del solicitante, incluso fuera del ámbito de aplicación territorial de la Directiva de 24 de octubre de 1995?

[262] http://curia.europa.eu/juris/document/document.jsf?docid=195494&doclang=ES (último acceso agosto 2019)

2) En caso de respuesta negativa a esta primera cuestión, ¿debe interpretarse el «derecho de retirada», según ha sido consagrado por el Tribunal de Justicia de la Unión Europea en su sentencia antes citada, en el sentido de que el gestor de un motor de búsqueda que estima una solicitud de retirada solamente está obligado a suprimir los vínculos controvertidos de los resultados obtenidos como consecuencia de una búsqueda realizada a partir del nombre del solicitante en el nombre de dominio correspondiente al Estado en el que se considera que se ha efectuado la solicitud o, de manera más general, en los nombres de dominio del motor de búsqueda que corresponden a las extensiones nacionales de dicho motor para el conjunto de los Estados miembros de la Unión Europea?

3) Además, como complemento de la obligación mencionada en la segunda cuestión, ¿debe interpretarse el «derecho de retirada», según ha sido consagrado por el Tribunal de Justicia de la Unión Europea en su sentencia antes citada, en el sentido de que el gestor de un motor de búsqueda que estima una solicitud de retirada está obligado a suprimir, mediante la técnica denominada de «bloqueo geográfico», desde una dirección IP supuestamente localizada en el Estado de residencia del beneficiario del «derecho de retirada», los resultados controvertidos obtenidos como consecuencia de una búsqueda realizada a partir de su nombre, o incluso, de manera más general, desde una dirección IP supuestamente localizada en uno de los Estados miembros sujetos a la Directiva de 24 de octubre de 1995, y ello independientemente del nombre de dominio utilizado por el internauta que efectúa la búsqueda?

11.2. Las conclusiones del Abogado General.

I

En el informe previo a la setencia, las conclusiones del Abogado General[263] fueron las siguientes:

A la primera cuestión, el Abogado General señala que mediante su primera cuestión prejudicial, la CNIL, el Defensor del Pueblo francés, y los Gobiernos francés, italiano y austriaco invocan la necesidad de una protección eficaz y completa del derecho a la protección de los datos personales, garantizado por el artículo 8 de la CEDF, y el efecto útil del derecho a la retirada de enlaces, que se deriva de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, alegando que, para garantizar la efectividad de esos derechos, es preciso que la obligación de retirada de enlaces sea mundial.

Esa parece ser también la postura adoptada por Article 29 WP en sus Directrices sobre la ejecución de la sentencia de 26 de noviembre de 2014[264].

El Abogado General explica que, en efecto, ese grupo señala « [que] con el fin de dotar de plenos efectos los derechos de los interesados definidos en la sentencia del Tribunal de Justicia, las decisiones de retirada de enlaces deben ejecutarse de modo que se garantice una protección eficaz y completa de los derechos de los interesados y que la legislación europea no pueda eludirse. En ese sentido, la limitación de la retirada de enlaces a los dominios de la Unión Europea basándose en que los usuarios suelen acceder a los motores de búsqueda a través de sus dominios nacionales no puede constituir un medio suficiente para garantizar de forma satisfactoria los derechos de los

[263] http://curia.europa.eu/juris/document/document.jsf?text=&docid=209688&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=10365274

[264] Disponible en https://ec.europa.eu/justice/article-29/documentation/index_en.htm

interesados de conformidad con la sentencia del Tribunal de Justicia. En la práctica, eso supone que toda retirada debería aplicarse también a todos los dominios concernidos, incluidos los dominios .com».

Otros actores del ecosistema y la propia Comisión Europea sostienen, en esencia, que la instauración de un derecho a la retirada de enlaces mundial sobre la base del Derecho de la Unión no sería compatible ni con dicho Derecho, ni con el Derecho internacional público, y sentaría un peligroso precedente que alentaría a los regímenes autoritarios a exigir también la aplicación a nivel mundial de sus decisiones de censura.

A la vista de lo planteado, el Abogado General fundamenta que "La idea de una retirada de enlaces a nivel mundial puede parecer atractiva por su carácter radical, simpleza y eficacia. Sin embargo, esa solución no me convence, pues se centra únicamente en una cara de la moneda, la de la protección de los datos de una persona" ya que si se aceptara la retirada de enlaces mundial, las autoridades de la Unión no podrían definir ni determinar un derecho a recibir información y, aún menos, ponderarlo con los derechos fundamentales a la protección de los datos y a la vida privada. Además, ese interés del público en acceder a determinada información varía forzosamente en función de su ubicación geográfica, de un Estado tercero a otro.

Continúa informando que, por otra parte, existiría entonces el riesgo de que la Unión impidiera a personas que se encuentran en un tercer país acceder a la información. Permitir a una autoridad de la Unión que ordene una retirada de enlaces a nivel mundial transmitiría un mensaje nefasto a los terceros países, que también podrían ordenar una retirada al amparo de sus propias leyes. Imaginemos que, por el motivo que sea, terceros países interpreten algunas de

sus normas de modo que se impida a personas que se encuentran en un Estado miembro de la Unión el acceso a una información buscada. Existiría un riesgo real de nivelar a la baja, en detrimento de la libertad de expresión, a escala europea y mundial.

Para el Abogado General, los retos que se plantean en este asunto no exigen pues que las disposiciones de la Directiva 95/46 se apliquen fuera del territorio de la Unión. Sin embargo, eso no significa que el Derecho de la Unión no pueda imponer en ningún caso a un gestor de un motor de búsqueda como Google que lleve a cabo actuaciones a nivel mundial. No se excluye que puedan surgir situaciones en las que el interés de la Unión exija aplicar las disposiciones de la Directiva 95/46 más allá del territorio de la Unión. No obstante, en una situación como la del presente asunto, el Abogado General no ve motivo alguno para aplicar de ese modo las disposiciones de la Directiva 95/46.

Por consiguiente, el Abogado general propone al Tribunal de Justicia que responda a la primera cuestión prejudicial que las disposiciones de los artículos 12, letra b), y 14, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que el gestor de un motor de búsqueda que estima una solicitud de retirada de enlaces no está obligado a efectuar dicha retirada respecto de la totalidad de los nombres de dominio de su motor, de tal manera que los enlaces controvertidos dejen de mostrarse independientemente del lugar desde el que se realice la búsqueda a partir del nombre del solicitante.

En relación a la segunda y tercera pregunta, ya que la primera propone que sea respondida en sentido negativo, las aborda de manera conjunta.

II

En estas dos cuestiones prejudiciales, la autorida francesa de protección de datos establece un vínculo indisociable entre, por un lado, el nombre de dominio de un motor de búsqueda, y, por otro, el lugar desde el que se efectúa la búsqueda en Internet a partir del nombre de la persona afectada. El Abogado General subraya que, en lo que respecta a la primera cuestión prejudicial, es natural que se establezca ese vínculo: si el gestor de un motor de búsqueda hace inaccesibles los resultados de una búsqueda en todos sus nombres de dominio, es evidente que los enlaces controvertidos dejan de aparecer, con independencia del lugar desde el que se efectúe la búsqueda.

En cambio, habida cuenta de que propone que se responda en sentido negativo a la primera cuestión prejudicial, ese vínculo deja de existir. En efecto, como destaca el propio órgano jurisdiccional remitente, toda persona tiene la posibilidad de realizar sus búsquedas en cualquier nombre de dominio del motor de búsqueda. Por ejemplo, la extensión geográfica google.fr no se limita a las búsquedas realizadas desde Francia.

Continúa fundamentando que, sin embargo, esa posibilidad puede limitarse mediante bloqueo geográfico.

El bloqueo geográfico es una técnica que limita el acceso al contenido publicado en Internet en función de la localización geográfica del usuario. En un sistema de bloqueo geográfico, la localización del usuario se determina mediante técnicas de geolocalización, como la comprobación de la dirección IP del usuario. El bloqueo geográfico, que constituye una forma de censura, se considera injustificado en el Derecho del mercado interior de la Unión en el que ha sido objeto, en particular, de un reglamento cuya finalidad es

impedir a los comerciantes que ejercen su actividad en un Estado miembro que bloqueen o limiten el acceso a sus interfaces en línea a clientes de otros Estados miembros que desean realizar transacciones transfronterizas.

Una vez que se admite el bloqueo geográfico carece de importancia el nombre de dominio del gestor del motor de búsqueda que se utilice. Por consiguiente, propone analizar la tercera cuestión prejudicial antes que la segunda.

Fundamenta el Abogado General que en la sentencia Google Spain y Google, el Tribunal de Justicia declaró que el gestor de un motor de búsqueda debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que la actividad del citado motor satisface las exigencias de la Directiva 95/46 para que las garantías establecidas en ella puedan tener pleno efecto y pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada.

Continúa explicando que, una vez declarado el derecho a la retirada de enlaces, incumbe pues al gestor de un motor de búsqueda adoptar todas las medidas a su alcance para garantizar una retirada eficaz y completa. Dicho gestor debe acometer todas las posibles actuaciones desde el punto de vista técnico. En lo que concierne al procedimiento principal, estas actuaciones incluyen, en particular, la técnica denominada de «bloqueo geográfico», con independencia del nombre de dominio utilizado por el internauta que lleva a cabo la búsqueda.

III

De esta manera, el Abogado General propone que la retirada de enlaces no debe hacerse a nivel nacional sino, a nivel de la Unión Europea en base a que, dado que la Directiva 95/46 tiene «por objeto asegurar un alto nivel de protección dentro de la [Unión]», instaura un sistema completo de protección de datos que rebasa la fronteras nacionales. "Basado en el antiguo artículo 100 del Tratado de Constitución de la Unión Europea[265] se enmarca en una lógica de mercado interior que implica, conviene recordarlo, un espacio sin fronteras interiores"

De ello resulta que una retirada de enlaces a nivel nacional iría en contra de ese objetivo de armonización y del efecto útil de las disposiciones de la Directiva 95/46.

Continúa el Abogado General diciendo que, basado en el artículo 16 TFUE, el Reglamento n.º 2016/679 transciende del planteamiento del mercado interior de la Directiva 95/46 y pretende instaurar un sistema completo de protección de datos personales en la Unión. Ese Reglamento hace sistemáticamente referencia a la Unión, al territorio de la Unión o a los Estados miembros. Por ello acaba proponiendo pues que se responda a las cuestiones prejudiciales segunda y tercera que el gestor de un motor de búsqueda está obligado a suprimir los enlaces controvertidos de los resultados obtenidos tras una búsqueda efectuada a partir del nombre del solicitante desde un lugar situado en la Unión Europea. En ese contexto, el gestor está obligado a adoptar todas las medidas a su alcance para garantizar una retirada de enlaces eficaz y completa. Ello incluye, en particular, la técnica del

[265] Actualmente artículo 114 TFUE

«bloqueo geográfico» desde una dirección IP supuestamente localizada en uno de los Estados miembros sujetos a la Directiva 95/46, con independencia del nombre de dominio que haya utilizado el internauta que realiza la búsqueda.

11.3. El fallo en la sentencia del TJUE en el asunto C-507/17.

I

La Gran Sala del TJUE comienza exponiendo cuales son las normas para la interpretación correcta de la cuestión prejudicial. Tras cita la Directiva 95/46, que era la norma de referencia aplicable, la Gran Sala del TJUE expone que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1; corrección de errores en el DO 2018, L 127, p. 3), que se basa en el artículo 16 TFUE, es aplicable, de conformidad con su artículo 99, apartado 2, a partir del 25 de mayo de 2018.

Así mismo, la Gran Sala expone que a aplicación en el Derecho francés de la Directiva 95/46 queda garantizada mediante la loi n.º 78-17, du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés.[266]

El TJUE entiende que procede examinar conjuntamente, en esencia, si los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 y el artículo 17, apartado 1, del Reglamento 2016/679 deben interpretarse en el

[266] Ley n.º 78-17, de 6 de enero de 1978, sobre informática, ficheros y llibertades. Citada Ud Supra.

sentido de que, cuando el gestor de un motor de búsqueda estima una solicitud de retirada de enlaces en virtud de estas disposiciones, está obligado a proceder a dicha retirada en todas las versiones de su motor de búsqueda o, por el contrario, solo está obligado a proceder a ella en las versiones de este que corresponden al conjunto de los Estados miembros o incluso únicamente en la correspondiente al Estado miembro en el que se haya presentado la solicitud de retirada de enlaces, combinándola, en su caso, con el uso de la técnica denominada "bloqueo geográfico", a fin de garantizar que un internauta no pueda acceder, sea cual sea la versión nacional del motor de búsqueda utilizada, a los enlaces objeto del derecho de retirada durante una búsqueda efectuada desde una dirección IP supuestamente localizada en el Estado miembro de residencia del beneficiario del derecho a la retirada de enlaces o, de manera más general, en un Estado miembro.

Para el TJUE, con arreglo al artículo 17, apartado 1, del Reglamento 2016/679, el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan y el responsable del tratamiento estará obligado a suprimir lo antes posible esos datos cuando concurra alguna de las circunstancias enumeradas en esta disposición. El artículo 17, apartado 3, de este Reglamento especifica que el artículo 17, apartado 1, no se aplicará cuando el tratamiento sea necesario por alguna de las razones enunciadas en el propio apartado 3 de este artículo. Estas razones incluyen, entre otras, de conformidad con el artículo 17, apartado 3, letra a), de dicho Reglamento, el ejercicio, en particular, del derecho a la libertad de información de los internautas.

A su vez, del artículo 4, apartado 1, letra a), de la Directiva 95/46 y del artículo 3, apartado 1, del Reglamento 2016/679 se desprende que tanto la

Directiva como el Reglamento permiten a los interesados hacer valer su derecho a la retirada de enlaces frente al gestor de un motor de búsqueda que posea uno o varios establecimientos en el territorio de la Unión, en el marco de cuyas actividades realice el tratamiento de datos personales relativos a esos interesados, independientemente de que el tratamiento tenga lugar en la Unión o no.

Por todo lo anterior, continúa exponiendo el TJUE, del considerando 10 de la Directiva 95/46 y de los considerandos 10, 11 y 13 del Reglamento 2016/679, que se adoptó sobre la base del artículo 16 TFUE, se desprende que el objetivo tanto de la Directiva como del Reglamento consiste en garantizar un elevado nivel de protección de los datos personales en toda la Unión.

El Tribunal expone que Internet es una red mundial sin fronteras y los motores de búsqueda confieren carácter "ubicuo" a la información y a los enlaces contenidos en una lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona física[267].

II

El TJUE considera que, en un mundo globalizado, el acceso de los internautas, en particular de aquéllos que se hallan fuera de la Unión, a un

[267] Ver Sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317, apartado 80, y y Sentencia de 17 de octubre de 2017, Bolagsupplysningen e Ilsjan, C-194/16, EU:C:2017:766, apartado 48. En este apartado 48 se fundamenta que "Sin embargo, habida cuenta de la naturaleza ubicua de los datos y los contenidos puestos en línea en un sitio de Internet y de que el alcance de su difusión es, en principio, universal (véase, en este sentido, la sentencia de 25 de octubre de 2011, eDate Advertising y otros, C-509/09 y C-161/10, EU:C:2011:685, apartado 46), una demanda que tenga por objeto la rectificación de los primeros y la supresión de los segundos es única e indivisible y, en consecuencia, sólo puede interponerse ante un tribunal competente para conocer íntegramente de una acción de indemnización del daño, en virtud de la jurisprudencia resultante de las sentencias de 7 de marzo de 1995, Shevill y otros (C-68/93, EU:C:1995:61), apartado 32, y de 25 de octubre de 2011, eDate Advertising y otros (C-509/09 y C-161/10, EU:C:2011:685), apartado 48, y no ante un tribunal que carece de esta competencia."

enlace que remite a información sobre una persona cuyo centro de interés está situado en la Unión puede tener efectos inmediatos y sustanciales sobre dicha persona dentro de la propia Unión. Tales consideraciones podrían justificar que el legislador de la Unión fuera competente para establecer la obligación de que el gestor de un motor de búsqueda, cuando estime una solicitud de retirada de enlaces formulada por tal persona, retire dichos enlaces de todas las versiones de su motor. Sin embargo, el TJUE subraya también que muchos otros Estados ajenos a la Unión no contemplan el derecho a la retirada de enlaces o lo abordan desde una perspectiva diferente.

Considera además que el derecho a la protección de los datos personales no constituye un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. A esto cabe añadir que el equilibrio entre los derechos al respeto de la vida privada y a la protección de los datos personales, por un lado, y la libertad de información de los internautas, por otro lado, puede variar significativamente en las distintas partes del mundo.

Continúa la Sala considerando que, aunque el legislador de la Unión Europea ha instaurado un equilibrio entre ese derecho y esa libertad en lo que respecta a la Unión es preciso observar que, en cambio, en la situación actual, el legislador no ha establecido tal equilibrio en lo que respecta al alcance de la retirada de enlaces fuera de la Unión. No se desprende en modo alguno que el legislador de la Unión haya optado por garantizar la protección de datos de los particulares más allá del territorio de los Estados miembros. Tampoco se desprende que el legislador haya pretendido imponer a un gestor que, como Google, queda comprendido en el ámbito de aplicación de la Directiva o del

Reglamento, la obligación de retirar enlaces también de las versiones nacionales de su motor de búsqueda que no correspondan a los Estados miembros. El TJUE fundamenta en este sentido que, de hecho, aun cuando los artículos 56 y 60 a 66 del Reglamento 2016/679 proporcionan a las autoridades de control de los Estados miembros los instrumentos y mecanismos que les permiten, en su caso, cooperar para llegar a una decisión común basada en un equilibrio entre los derechos del interesado al respeto de su vida privada y a la protección de los datos personales que le conciernan y el interés del público de los distintos Estados miembros en tener acceso a la información, el Derecho de la Unión no prevé actualmente tales instrumentos y mecanismos de cooperación en lo que se refiere al alcance de la retirada de enlaces fuera de la Unión.

III

Visto todo lo anterior el Tribunal ultima que no puede exigirse al gestor de un motor de búsqueda, en virtud de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 y del artículo 17, apartado 1, del Reglamento 2016/679, que proceda a la retirada de enlaces en todas las versiones de su motor. En definitiva, el gestor de un motor de búsqueda que estime una solicitud de retirada de enlaces presentada por el interesado, no está obligado, con arreglo al Derecho de la Unión, a proceder a dicha retirada en todas las versiones de su motor.

Esto anterior no quita que, el Derecho de la Unión obliga al gestor de un motor de búsqueda a retirar los enlaces en las versiones de su motor que correspondan al conjunto de los Estados miembros y a adoptar medidas suficientemente eficaces para garantizar la protección efectiva de los derechos

fundamentales del interesado. Así pues, la retirada de enlaces deberá acompañarse, en caso necesario, de medidas que impidan de manera efectiva o, al menos, dificulten seriamente el acceso a los enlaces objeto de la solicitud de retirada por parte de los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros, a través de la lista de resultados obtenida tras esa búsqueda efectuada desde una versión de ese motor "de fuera de la Unión". El órgano jurisdiccional nacional deberá comprobar que las medidas adoptadas por Google Inc. cumplen estos requisitos.

Interesa resaltar la "clausula de salvaguardia" que ha estalecido el TJUE. La Gran Sala subraya que, aunque el Derecho de la Unión no exige, en la situación actual, que, cuando se estime una retirada de enlaces, esta se realice en todas las versiones del motor de búsqueda de que se trate, tampoco lo prohíbe. Por lo tanto, una autoridad de control o judicial de un Estado miembro sigue siendo competente para realizar, de conformidad con los estándares nacionales de protección de los derechos fundamentales, una ponderación entre, por un lado, los derechos del interesado al respeto de su vida privada y a la protección de los datos personales que le conciernan y, por otro lado, el derecho a la libertad de información y, al término de esta ponderación, exigir, en su caso, al gestor del motor de búsqueda que proceda a retirar los enlaces de todas las versiones de dicho motor.

12. El Derecho al Olvido en el RGPD. Especial referencia al Blockchain.

I

El Derecho al Olvido ha sido positivizado en la legislación europea por prmera vez mediate el RGPD. La Guía Europea sobre protección de datos[268] lo concibe como un "derecho a borrar" y lo justifica en virtud de que proporcionar a los interesados el derecho a que se borren sus propios datos es particularmente importante para la aplicación efectiva de los principios de protección de datos, y en particular el principio de minimización de datos.

El artículo 17 del RGPD establece que:

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

[268] Supra

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

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1,

en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

II

Dado lo expuesto, hay que estudiar el Derecho al Olvido en la Unión Europea a la luz de los considerandos establecidos en el mismo RGPD.

El considerando 65 del RGPD subraya que los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «Derecho al Olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el

ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

El considerando 66 establece que a fin de reforzar el «Derecho al Olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

Sigue el considerando 67 explicando que entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema. Para reforzar aún más el control sobre sus propios datos, continúa diciendo el considerando 68, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un

responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna 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. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los

datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

El considerando 69 expone que en los casos en que los datos personales puedan ser tratados lícitamente porque 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 o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los 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, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor. A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se

tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas (considerando 71).

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar

perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

El considerando 76, finalmente, establece que la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

III

En definitiva, el conjunto de derechos que reconoce el RGPD, los buscadores de Internet deben respetar los derechos de supresión y retificación establecidos en el propio texto legal de conformidad con el artículo 19[269].

Así el artículo 16 del RGPD, vistos los considerandos 39 y 59 del propio texto legal[270][271], establece que el interesado tendrá derecho a obtener sin

[269] El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo sol·licita.

[270] Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento

[271] Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición.

dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, o a que inste su oposición (considerandos 50 y 59 entre otros[272]) de conformidad con el artículo 21 RGPD que establece que:

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la

[272] Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición

elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 -del mismo articulo 21- será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE[273], el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1[274], el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

[273] 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).(DOCE 31-7-2002)

[274] 1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

IV

El RGPD no especifica si el Derecho al Olvido se aplica al blockchain. De manera sencilla, el blockchain es una estructura de datos en la que la información contenida se agrupa en bloques a los que se les añade la información relativas a otro bloque de la cadena anterior en una línea temporal. Esto hace que la información contenida en un bloque solo puede ser cambiada modificando todos los bloques anteriores o posteriores.

La legislación parece obviar lo que sucedería si se aplicase, por cualquier causa, el Derecho al Olvido en el mundo digital. ¿ Qué pasaría con el resto de bloques o informaciones cuya autenticidad y veracidad garantiza la cadena de blockchain? La legislación no comtempla cómo se gestionará el blockchain en estos casos ni cómo afecta a la cadena de verificación la desaparición de un dato ni si ese dato sebe ser olvidado en toda la cadena o en un bloque.

13. El Tratamiento de datos desde el punto de vista del Big Data y el Internet de las Cosas.

13.1. Big Data, Internet de las Cosas y Unión Europea.

El tratamiento de datos aplicable al Big Data y al IOT se encuentra recogido en los artículos 18 y 19 del RGPD que establecen en primer lugar, el Derecho a la limitación del tratamiento. Así:

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la

supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. 2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

El art. 19 establece la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento dodne el responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

El artículo 22 del RGPD, a su vez, indica que:

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1[275], salvo que se aplique el artículo 9, apartado 2, letra a)[276] o g), y se hayan

[275] 1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física

[276] a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados

tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

En definitiva, las excepciones a la prohibición general de tratamiento de las categorías especiales de datos personales deben establecerse de forma explícita, cuando el interesado dé su consentimiento explícito o concurran determinadas razones vinculadas al interés público, razones sanitarias, de seguridad, o cuando sea necesario para permitir el ejercicio de libertad fundamentales por razones de interés público, de conformidad con el artículo 9.

Se dan dos definiciones novedosas en el RGPD que antes no se recogían en la anterior legislación y que son de extrema importancia en muchos de los datos obtenidos y tratados a través del Internet de las Cosas debido a la autentificación del sistema para reconocer al usuario. En concreto, el artículo 4 RGPD nos define, por un lado, los "datos genéticos" que son aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona; por otro lado, nos define lo que son los "datos biométricos" que son aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o

miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Así las cosas, y una vez obtenidos los datos de los usuarios, y a la hora de tratarlos, el art. 5 RGPD legisla que:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerarà incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

Se observa como en este apartado se establecen unos principios -o normas de actuación- relativos a la protección de datos y que deben ser respetados: La exactitud, la lealtad, la transparencia, la licitud, etc.

Para el RGPD, el principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con que finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

En el mismo orden de cosas, el articulo 47 RGPS subraya que estos principios relativos a la protección de datos -y que obligatoriamente deben de ser tenidos en cuenta tanto en el tratamiento, masivo o no, de los datos como de su obtención, como por ejemplo vía Internet de las Cosas- son:

- La limitación de la finalidad,

- La minimización de los datos,

- Los periodos de conservación limitados,

- La calidad de los datos,

- La protección de los datos desde el diseño y por defecto, la base del tratamiento,

- El tratamiento de categorías especiales de datos personales,

- Las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes

13.2. La licitud en el tratamiento de los datos obtenidos.

I

El RGPD establece que el tratamiento debe ser lícito -es decir que no todo dato aunque se haya recogito se puede tratar- cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato. Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.

Es crucial saber cuándo se tendrá que considerar lícito el tratamiento porque sinó debiera ser posible ejercitar el Derecho al Olvido.

El RGPD no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo

de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y subraya que "leal".

II

Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

También establece que el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Para el RGPD, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse

cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles.

III

La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para lo que el RGPD denomina el "tratamiento ulterior".

Con objeto de determinar si el fin del "tratamiento ulterior" es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular, con el concepto jurídico indeterminado, de las "expectativas razonables" del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la

operación de tratamiento original como en la operación de tratamiento ulterior prevista.

IV

El RGPD continúa considerando – estableciendo una suerte de ponderación de intereses- que el interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las "expectativas razonables" de los interesados basadas en su relación con el responsable[277].

Sobre el interés legítimo del controlador de datos, el considerando 47 se refiere al tratamiento de datos personales estrictamente necesarios con el fin de prevenir el fraude que se basaría en el derecho a la propiedad, o el tratamiento de datos personales para fines de marketing directo que se basa en la libertad de realizar un negocio o empresa. Ambas razones serán la base para el considerando 48, que designa "la transmisión de ciertos datos dentro de grupos de empresas" como un interés legítimo y para el considerando 49, que se refiere al procesamiento de datos con el fin de garantizar la red y la seguridad de la información.

[277] Siguiendo la recomendación de Article 29 Working Party en informe de 06/2014 disponble en https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf

V

Hay que decir que, aunque no es el objeto de este estudio, el tema del interés legítmo del controlador ha dado lugar a interesantes debates sobre cómo debe entenderse y si cabría extrapolarlo al interés legítimo de otra parte que no sea extríctamente del controlador de los datos.

No parece, sin embargo, que este teoría de las "espectativas razonables" del RGPD vaya en consonancia con lo establecido -para esta teoría- por la jurisprudencia del TEDH el cual fundamentó[278], mutatis mutandi, que, para ser previsible, la ley nacional debe establecer límites a los poderes de las autoridades: la ley debe definir el tipo de información que puede procesarse, las categorías de personas sobre las cuales se puede recopilar información , las circunstancias en que se pueden tomar tales medidas, las personas autorizadas a acceder a estos datos y los límites de retención de estos datos.

Así, el TEDH dictaminó que las operaciones realizadas con datos personales, como la comunicación de los datos a un tercero, sí que están dentro de las expectativas razonables del interesado. Sin embargo, el TEDH señaló[279] que el uso adicional de los datos persiguió un propósito diferente que estaba más allá de las expectativas del solicitante y concluyó que esto equivalía a una interferencia con el derecho del solicitante a la vida privada, fundamentando en otra sentencia[280]que, en todo caso, el interés del controlador no puede entrar en juego con los intereses y derechos privados y muchos menos sin el conocimiento del interesado[281].

[278] Rotaru vs Romania [GC], Appl. No. 28341/95
[279] M.S. vs Sweden, Appl. No. 20837/92
[280] S. and Marper vs UK, Appl. No. 30562/04 y 30566/04
[281] K.H. y otros contra. ESlovakia Appl. No. 32881/04

VI

El RGPD continúa, a modo ejemplificador, estableciendo que el interés legítimo podría darse cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior.

Sobre este aspecto, el TJUE ya tiene jurisprudencia[282] al fundamentar que debería haber criterios para determinar los datos relevantes con respecto al propósito del procesamiento, así como para determinar el límite de tiempo apropiado para la retención de datos.

El TJUE fue aún más lejos en otro asunto al declarar[283] que la legislación que prescribía una retención general e indiscriminada de datos excede los límites de lo estrictamente necesario y no eso puede considerarse justificado.

Sigue recordando el RGPD que, dado que corresponde al legislador de cada país, establecer por ley la base jurídica para el tratamiento de datos personales

[282] Asuntos acumulados C-293/12 and C-594/12, Digital Rights Ireland Ltd vs Minister for Communications.
[283] Asuntos acumulados C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department vs Tom Watson and Others

por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

También considera el RGPD que los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados, y también considera que no se ve afectados los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero.

El RGPD también considera que constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información.

Con la finalidad de tratamiento con fines distintos de aquellos para los que hayan sido recogidos inicialmente, el RGPD establece -para el caso de operadores privados- que solo debe permitirse cuando sea compatible con los fines de su recogida inicial, considerando que, en tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales sinó que vuelve otra vez con la teoría de las “expectativas

razonables". Al operador público se le permitirá el tratamiento de datos para la salvaguarda de la democracia en virtud del interés público, o para temas de salud pública[284].

Sobre este aspecto, El TJUE dictaminó en el caso de Bara[285] que el requisito de un procesamiento justo de los datos personales exige que una administración pública informe a los interesados cuando transfiera sus datos personales a otra administración pública.

VII

Importante es la consideración que establece el RGPD en relación a la especial protección que merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

Debe incluirse entre tales datos personales -de especial protección- los datos de carácter personal que revelen el origen racial o étnico.

El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

[284] Sobre este aspecto, ver informe Art 29 Workin Party. Citado supra, dodne aconseja que el poder público debiera indicar qué tratamientos puede hacer con los datos.
[285] Caso C-201/14, Smaranda Bara and Others vs Președintele Casei Naționale de Asigurări de Sănătate.

El RGPD establece que los datos personales que se consideran de especial protección no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el mismo RGPD, ya que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del RGPD al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En los datos de especial tratamiento, además de los requisitos específicos de ese tratamiento especial, deben aplicarse los principios generales del RGPD, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

13.3. El Derecho al Olvido de los datos del niño en la legislación de la Unión Europea.

I

Estudio aparte merece el Derecho al Olvido sobre los datos recopilados y tratados que pertenezcan o incidan sobre menores de edad, ya que le es de aplicación plenamente el art. 17 RGPD sobre el ejercicio al Derecho a Olvido y parte de la consideración 38 del mismo texto legal sobre que los niños son

sujetos de especial protección con independencia de la manera de cómo se dio el consentimiento ya que se debe presumir que un menor de edad no es consciente de lo que implica ceder sus datos y el tratamiento que ello conlleva.

El considerando 65 del RGPD establece que, en particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el RGPD. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño.

A la vista del art. 17 y de los considerandos citados, cabe entender que los derechos del niño están por encima de otros derechos ya que cuando cedió sus datos no sabía las implicacions de hacerlo. El propio RGPD establece que en casos de interés público, sanidad, etc, también se dan derechos de terceros que se deben ponderar caso por caso.

Merece mención el artículo 7.3 del RGPD que establece en su último inciso que que "será tan fácil retirar el consentimiento como darlo". Por tanto, en el caso del niño, se debiera tener en cuenta que los procesos para ejercer el derecho de borrado sean fáciles de acceder y comprender para un niño y que sea tan fácil dar los datos como ejercer el Derecho al Olvido.

II

Aunque parece que el RGPD establece una normativa clara al respecto y bien estructurada, un análisis en profundidad de la cuestión nos lleva a considerar que la legislación nace desfasada y no adaptada ni al Big Data ni al Internet de las cosas.

Parece que el RGPD está solo pensando en las páginas webs o en Servicios en línea prestados por proveedores de Internet donde los datos cedidos son fácilmente identificables e individualizables. Y decimos datos cedidos porque no queda claro para nada si esos datos son los cedidos voluntariamente por el menor o también abarcan los cedidos mediante "observación" de datos.

14. Soluciones técnicas propuestas al Derecho al Olvido

I

La búsqueda de contenidos en Internet es crucial para mucha gente, ya que permite a los usuarios ir "saltando" de página en página, sin conocer la dirección exacta de ésta o el contenido que puede tener. Casi el 80% de los usuarios de Internet, navega a través de buscadores[286] y este porcentaje crece día a día.

Es difícil explicar cómo funciona Internet, ya que su algoritmo de búsqueda es un secreto empresarial[287] fuertemente protegido por Google.

No sabemos cómo Google determina la relevancia de las páginas, aunque sí que la empresa ofrece algunas pistas.

[286] http://pewinternet.org/reports/2012/Seacrh-Engine-Use-2012.aspx
[287] ZITTRAIN, J; "The future of the Internet- And How to stop It "(Yale university 2009)

De acuerdo a las explicaciones ofrecidas por Google[288], se utiliza un software denominado "rastreador web" para descubrir páginas web de dominio público. El rastreador más conocido es "Googlebot". Los rastreadores consultan las páginas web y siguen los enlaces que aparecen en ellas, al igual que haría cualquier usuario al navegar por el contenido de la Web. Pasan de un enlace a otro y recopilan datos sobre esas páginas web que proporcionan a los servidores de Google.

El proceso de rastreo comienza con una lista de direcciones web de rastreos anteriores y de sitemaps proporcionada por los propietarios de sitios web. Al acceder a estos sitios web, los rastreadores de Google buscan enlaces a otras páginas para visitarlas. El software presta especial atención a los nuevos sitios, a los cambios en los sitios actuales y a los enlaces inactivos.

Los programas informáticos determinan qué sitios rastrear, con que frecuencia y cual es el número de páginas que se deben explorar en cada sitio.

A la hora de indexar la información, Google considera que la Web es como una biblioteca pública cada vez mayor con miles de millones de libros y sin un sistema de archivo. En resumen, Google recopila las páginas durante el proceso de rastreo y, a continuación, crea un índice, por lo que sabemos exactamente dónde tenemos que buscar. Al igual que el índice del final de un libro, el índice de Google incluye información sobre las palabras y dónde aparecen. Cuando haces una búsqueda, en el nivel más básico, nuestros algoritmos buscan los términos de consulta en el índice para encontrar las páginas adecuadas.

[288] http://www.google.es/intl/es/insidesearch/howsearchworks/crawling-indexing.html

A partir de ese momento, el proceso de búsqueda se vuelve mucho más complejo. Los sistemas de indexación de Google tienen en cuenta muchos aspectos diferentes de las páginas, como cuándo se publicaron, si contienen fotos y vídeos, etc.

II

Google[289] explica que para cada búsqueda hay miles o millones de páginas web con información útil. Los algoritmos son fórmulas y procesos informáticos que convierten las preguntas en respuestas. Actualmente, los algoritmos de Google se basan "en más de 200 señales" únicas o "pistas" que permiten adivinar lo que realmente se podría estar buscando. Estas señales incluyen, entre otros, los términos de los sitios web, la actualidad del contenido, la región desde donde se hace la búsqueda y el PageRank.

Google asegura que "actualizamos constantemente nuestros sistemas y tecnologías para ofrecer mejores resultados". Es decir, realiza ajustes para que los resultados sean cada vez más relevantes lo que conlleva cada vez un mayor criterio subjetivo a la hora de ofrecer resultados.[290]

A través de sus algoritmos, Google calcula el PageRank[291]. El Page Rank es la puntuación que se le asigna a la página web, en función de las "señales" y que hace que una página nos salga más arriba o más abajo en la búsqueda.

Google reconoce que a veces edita manualmente – con un "toque humano"- los resultados de sus índices, por diversas razones, ya sean legales, abusos sexuales, etc.[292][293].

[289] http://www.google.es/intl/es/insidesearch/howsearchworks/algorithms.html
[290] Allyson HAYNES STUART, "Google search resuts:Buried if not forgotten". North Carolina Journal of Law and Technology. Volume 15, Issue 3:spring 2014
[291] Marca patentada por Google en 1999.

De todo lo anterior hay que concluir que el buscador de Google no es neutro y que Google tiene un gran poder sobre la reputación de las personas[294]. De ahí que haya que entenderse que las soluciones propuestas tengan que pasar necesariamente por Google, ya que es propietario del algoritmo de búsqueda.

Pero hay que entender que Google no puede ser un mero sujeto pasivo que deba recibir órdenes de supresión de datos, sino que debe de ser parte de la solución.

III

Hay quien dice, como Linde[295], que "Los operadores económicos no tienen (ni tienen por qué tener) entre sus objetivos otorgar derechos a los ciudadanos, pues su finalidad principal o exclusiva es obtener beneficios. Solamente desde un sistema jurídico protector que incluya medidas legislativas apropiadas, autoridades de supervisión con amplios poderes y jueces competentes la protección estará asegurada"

Hay que estudiar entonces cómo se puede asegurar esa protección.

La conferencia europea de Autoridaddes de Protección de datos, de 5 de junio de 2014, resuelve que "The globalisation of data processing and exchanges

[292] Por ejemplo, http://www.google.com/insidesearch/howsearchworks/fighting-spam.html (última visita 15 de diciembre de 2018)
[293] http://searchengineland.com/google-bing-have-whitelistsexception-lists-for-algorithms-67732 (última visita 15 de diciembre de 2018)
[294] CANNON, A.W. "Regulating Adwords: Consumer protection in a Market where the Commodity is Speech." SETTON HALL L. REVIEW.291,296 (2009)
[295] LINDE , E. "Algunas novedades sobre la protección de los consumidores y usuarios". Revista de derecho de la Unión Europea, ISSN 1695-1085, Nº. 26, 2014, págs. 259-260

of data also demands a comprehensive approach, taking into account not only the European but also the international framework."[296].

Es decir, se vuelve a hablar de que tiene que haber un enfoque Internacional. Un enfoque que hasta ahora, hay que entender, no se le ha dado.

Y ese enfoque Internacional ha de concluirse que tiene que dejar zanjada la cuestión no sólo del Derecho al Olvido en Internet, sino de toda la problemática asociada al Big Data y al IoT.

En la 36ª Conferencia de Autoridades de Protección de datos, realizada en octubre de 2014, se ha reconocido a los metadatos asociados al Big Data como "datos personales"[297].

En esta misma conferencia, ya se reconoce que hay un problema con la cantidad de datos – que va en aumento-, anónimos y no anónimos, que se están gestionando. Y que hay que salvaguardar la privacidad de los individuales y utilizar los datos sólo para el propósito que fueron recolectados[298].

Hay que concluir que se necesita un enfoque global -como reconocen todos los Convenios, Resoluciones, y Leyes internacionales- y unitario. El Derecho al Olvido no es ya solo una cosa de los Buscadores, que son ciertamente un número limitado de empresas, sino algo que abarca ya a una ingente pluralidad de actores que conforman una "memoria digital" tal y como mantenemos en esta tesis. El Derecho al olvido no es solo una cosa de

[296]http://www.agpd.es/portalwebAGPD/internacional/Europa/conferencias/Conf_primavera/common/Resolution_Convention_108_Strasbourg_2014.pdf (útima visita 12 de dieciembre de 2018)
[297] http://www.privacyconference2014.org/media/16718/Declaraci%C3%B3n-de-Mauricio-sobre-el-Internet-de-las-Cosas.pdf (última visita 11 de dciembre de 2018)
[298] http://www.privacyconference2014.org/media/16602/Resolution-Big-Data.pdf (última visita 12 de diciembre de 2018).

buscadores; más bien es un derecho a ejercer ante los buscadores de manera marginal.

Ciertamente las soluciones que se ha propuesto hasta ahora se centran únicamente en los buscadores.

IV

Algunos autores, entre ellos Haynes Stuart[299], han propuesto un tipo de solución intermedia que denominan "Guiding Google's Choice".

Según Haynes, Google debería reconocer que ha información que no debería aparecer en sus resultados de búsqueda, por ser perjudicial. Propone que Google continúe mostrando los datos de manera "normal", pero que se ofrezca a reubicar los enlaces cuando el "usuario" ha intentado contactar con la página de hospedaje de datos y no ha conseguido que retiren la información.

Esta solución propone que la solución no venga dada por la información que se muestra, sino por el posicionamiento de dicha información.

Haynes se refiere siempre a información que cae dentro de la categoría de "datos protegidos" según la política de Google[300] como puede ser información de contacto, números de teléfono, firmas, etc.

Con eso se consigue que los resultados de búsqueda sobre los datos de esa persona, no aparezcan en las primeras páginas.

[299] HAYNES STUART, A"Google search resuts:Buried if not forgotten". North Carolina Journal of Law and Technology. Volume 15, Issue 3:spring (2014)
[300] https://www.google.es/policies/privacy/ (última visita 14 de diciembre de 2018)

Para este autor, se trata de una solución intermedia que es menos severa que el borrado o la supresión de datos.

Bajo esta propuesta, el "estándar" es menor que requerir a los tribunales que dicten una sentencia de borrado de datos, pero más efectivo en relación a la rapidez con la que se puede conseguir.

Y señala que además estas medidas van dirigidas a mantener el buen nombre de Google, pues los estudios revelan que se tiende a culpar a Google o a Facebook de los efectos negativos de los datos que muestras como en el cyber bulling[301] Sin embargo, tenemos que entender que el problema no se elimina. Los datos siguen estando ahí, ubicados en un "page Rank" posterior pero visibles en todo caso.

Propone además la implicación de Google en los casos de demanda de borrado de información sensible que no entren dentro de las políticas de privacidad específicas de la compañía.

a) información confidencial y personal

La problemática con estos datos confidenciales y personales que no caen dentro de las políticas de privacidad, es que Google les da el mismo tratamiento que a cualquier dato "no confidencial". Haynes cree que Google podría ayudar tremendamente a las personas que han intentado borrar este tipo de datos de la página de hospedaje sin resultado. Y se basa en que muchas veces la parte responsable de la información es difícil de encontrar.

b) Información relativa a menores.

[301] WHITCOM D, "Cyber-Bullyng cases put heat on Google, Facebook," REUTERS (9 de marzo de de 2010)

Haynes observa, y así se puede comprobar en Google[302], que Google ayuda a quitar el contenido relativo a "abuso de menores". Pero si seleccionas esta opción, por ejemplo en Estados Unidos, te ofrece un link al National Center for Missing and Exploited Children o información general sobre cómo mantener segura a tu familia en internet.

Haynes considera que Google debería permitir el envío de información y tomar acciones de manera unilateral.

c) La información es falsa, difamatoria o actualmente no relevante.

Haynes confirma que esta categoría es la más controvertida, pues puede atentar contra la "libertad de expresión".

Pero Google no está obligada a retirar dicha información si no es bajo requerimiento judicial. En Estados Unidos no están obligados por la sección 230 de la "Communications Decency Act", y en Europa, Google contempla que "procesará" la información[303].

Para el autor, Google debería involucrarse en determinar el posicionamiento de la información, y todo ello en su propio beneficio ya que sería considerada una empresa más transparente.

No obstante, se han señalado algunas críticas a este sistema. Tal y como afirma Haynes, el "guiado de Google" es una solución pragmática. Y sin duda lo es. Pero entendemos que dista mucho de ser una solución "ideal" y que garantice seguridad jurídica y rapidez a todos las partes de ecosistema.

[302] http://www.google.com/intl/es_ES/+/policy/content.html (última visita 16 de diciembre de 2018)
[303] https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es

Pero hay que concluir que todo se hace depender finalmente de la "buena voluntad" de Google, y a la ampliación o no de su política de privacidad.

No menos importante es el problema de legislaciones territoriales que implica esta medida. Se observa como los bienes jurídicos a proteger no son los mismos en Europa que en Estados Unidos u otras partes del mundo. La libertad de opinión no es lo mismo que la libertad de información.

No sólo lo anterior sino que además no se crea ningún cuerpo jurisprudencial ni doctrinal al respecto. Ante una petición individual, la eliminación de la búsqueda -o su retraso de posiciones en el buscador- depende de un abogado de Google. Se pueden dar resoluciones diferentes a igual problemática, y sin posibilidad de revisión. La revisión sólo podrá venir de los Tribunales de Justicia, lo que conlleva mucho tiempo y dinero, cosa alejada de la finalidad inmediata de proteger información sobre un tercero particular.

Además, tal y como está planteada esta solución intermedia, se entiende que los resultados de búsqueda no desaparecen, sino que quedan relegados a posiciones inferiores en la búsqueda.

No sólo esto. Puede ser que sea una solución con una empresa como Google, pero no se soluciona el problema con otras empresas o con otro tipo de datos menos tangibles y visibles, como puede ser todo lo referido al Big Data o los recogidos en el Internet de las Cosas.

Observamos además como el hecho de que todo dependa de Google, puede dar lugar a retirada de datos de una manera injusta, pues puede ser que los datos si sean relevantes o no sean difamatorios. O el hecho de que se acabe borrando más información de la necesaria.

No hay que olvidar que el buscador es el "core businees" de Google. Un aluvión de peticiones, y una necesidad por parte de Google de no entrar en más polémicas, puede perjudicar al sistema de búsquedas, y por lo tanto al resto de productos, a la finalidad de los buscadores y, en definitiva, ir en detrimento de la productividad de una compañía que acaba afectando a todos los usuarios.

Ante una petición individual -no ordenada por una autoridad judicial- cuando la propia empresa propietaria del buscador se convierte en juez y parte al resolver sobre una peticón de cancelación, el resultado no puede ser óptimo. El resultado a la petición puede llegar tarde y no ser correcto. Ante esto se puede argumetar que sin una "doctrina" constante sobre el Derecho al Olvido, que se aplique en todas partes por igual y que produzca "certidumbre" a las partes, no puede haber la necesaria seguridad jurídica. Pero para ello hay que concluir que hace falta que los legisladores entiendan la realidad poliédrica de Internet. No se puede dejar la solución del problema a Google. Google tiene que ser parte de la solución, pero no la solución por entero.

V

El mecanismo de ventanilla única, se trata de una idea debatida en el seno de la Comisión Europea[304], como propuesta de legislación, en 2013.

En enero de 2012, la Comisión Europea presentó un paquete legislativo para actualizar y modernizar los principios consagrados en la Directiva 95/46 y para intentar garantizar la protección de datos en el futuro.

[304] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010139%202014%20INIT (útima visita 16 de diciembre de 2018)

Este paquete legislativo incluye una comunicación política de los objetivos de la Comisión Europea (5852/12), y dos propuestas legislativas: un reglamento sobre 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) (5853/12) y una Directiva sobre la protección de datos personales tratados con fines de prevención, detección, investigación y enjuiciamiento de los delitos y las actividades judiciales relacionadas (5833/12).

Según la nota difundida por la propia Comisión Europea[305], bajo la presidencia de Lituania, estas propuestas están dirigidas a la construcción de un marco de protección de datos más fuerte y coherente en la UE, respaldada por una legislación más coherente que permitirá a la economía digital trabajar para el desarrollo de todo el mercado interior, potenciar el control personal de los propios datos y reforzar la seguridad jurídica y práctica para los operadores económicos y las autoridades públicas.

Fruto de este paquete legislativo, se propone el mecanismo del One-Stop-Shops, pensado para compañías que operan en diferentes Estados Miembros.

El principio de "ventanilla única", junto con el mecanismo de coherencia, es uno de los pilares centrales de la propuesta de la Comisión. De acuerdo con este principio, cuando el tratamiento de datos personales se realiza en más de un Estado miembro, una autoridad única de supervisión debería ser la competente en toda la Unión para el seguimiento de las actividades del "controlador" o del "procesador" de datos, y esta autoridad única debería tomar las decisiones correspondientes. La propuesta establece que la

[305] http://www.eu2013.lt/en/news/data-protection-council-supports-one-stop-shop-principle

autoridad competente que preste tales “one-stop-shop” debe ser la autoridad de supervisión de datos del Estado miembro en el que el “controlador” o “procesador” de datos tiene su establecimiento principal.

El Consejo expresó su apoyo al principio de que, en los casos transnacionales de envergadura, la regulación debe establecer un mecanismo de "ventanilla única" con el fin de llegar a una decisión única de supervisión, que debe ser rápido, garantizar la aplicación coherente, proporcionar seguridad jurídica y reducir la carga administrativa. Este es un factor importante para mejorar la relación coste-eficacia de las normas de protección de datos para los negocios internacionales, contribuyendo así al crecimiento de la economía digital.

La discusión se centró en cómo llegar a una sola decisión. La mayoría de los Estados miembros indicaron que la labor de expertos debe continuar por un modelo en el que una sola decisión de supervisión es tomada por la autoridad "principal establecimiento" de supervisión, mientras que la jurisdicción exclusiva de dicha autoridad podría limitarse al ejercicio de determinadas competencias.

El Consejo indicó que los expertos deben explorar métodos para potenciar la "proximidad" entre los individuos y la autoridad de control de toma de decisiones mediante la participación de las autoridades "locales" de supervisión en el proceso de toma de decisiones. Esta proximidad es un aspecto importante de la protección de los derechos individuales.

Otro elemento importante para aumentar la coherencia de la aplicación de las normas de protección de datos de la UE será la de explorar qué rol podría tener la Junta Europea de Protección de Datos (EDPB).

VI

Las críticas a este sistema se centran en que la propuesta de la Comisión no está lo suficientemente madurada ya que, si bien parece entenderse que la autoridad local gozará de plenos poderes, nada se dice de que poderes ostentará fuera de su propia jurisdicción.

Además, hay que señalar el hecho de que la autoridad competente será aquella donde el controlador o proveedor tenga su establecimiento principal, que claramente puede ser que sea fuera de la Unión Europea.

Es ciertamente una medida tendente a la armonización de la legislación en todos los países miembros de la Unión Europea. Ha de entenderse que el legislador, pese a los avances que quiere realizar, sigue sin comprender la verdadera naturaleza de Internet y el alcance del Derecho a Olvido. Recordemos que la legislación habrá de prever también la protección de datos y el Derecho al Olvido en el Big Data y en el IoT, cosa que ahora no hace expresamente

El propio Consejo de Europa reconoce[306] que el método puede ser contrario al "remedio efectivo" al que hemos hecho referencia en otros apartados[307]. Hay que entender que es porque el mecanismo no es ágil, no permite que sea un tribunal quién lo juzgue, y porque no tiene en cuenta que puede ser que haya controladores y procesadores activos en diferentes países.

Hay que hacer notar que sí que está previsto que un tribunal juzgue el caso en una segunda instancia, pero deviene igualmente "inefectivo" el remedio, pues

[306] Ver nota Supra. Punto 5
[307] De hecho puede ser contarrio al art. 47 de la Carta de Derechos Fundamentales que prevé el derecho a un juicio justo delante de un Tribunal. De igual manera el art. 13 de la Carta Europea de Derechos Humanos.

se dilata el tiempo de respuesta esperando una sentencia y es bastante probable que el tribunal local hay de emprender acciones con otros tribunales de otros estados miembros.

Hay que entender, de igual manera, que el poder de control de la autoridad supervisora de datos de un país sobre empresas situadas fuera la Unión Europea es nulo, y limitado si incluso está dentro de un país miembro. Las sanciones y el control pueden quedar en nada. Se fía la "ventanilla única" a la cooperación entre los diferentes estados miembros más que en la competencia exclusiva de alguien para tomar dirimir sobre los derechos en juego.

VII

Otra de las soluciones propuestas es que toda la información que se introduzca tenga una fecha de caducidad a partir de la cual se considerará que no es procedente y no podrá ser utilizada, ante lo cual surgen las siguientes preguntas ¿Qué fecha escogemos? ¿No se puede revocar esa caducidad? ¿Ante quién? ¿Cómo? ¿Cómo se restringe la copia de datos? ¿ Se aplica a los daos recogidos por el Intenet de las cosas o el Internet de los Sentidos? Otras técnicas interesantes están siendo aplicadas por, por ejemplo, Apple, que reacondiciona los datos pasadas 24 horas para que dejen de representar a una persona en concreto.

VIII

El derecho a la protección de los datos personales y el interés de las empresas así como el interés público a la trasparencia de la información necesitan encontrar una reconciliación apropiada.

Sin duda alguna, hay que entender que uno de los principales problemas que se abordan son las diferencias legales entre los países y el alcance de las resoluciones judiciales que sobre el efecto se puedan dictar. La protección de datos y la libertad de información, así como el interés público, no se entiende igual en todo el mundo. Sobre el concepto de interés público, la concepción democrática, y la motivación que se realiza por las Administraciones Públicas podríamos realizar otra Tesis Doctoral. Tan solo esbozar sobre este aspecto que la época actual no parece muy propicia para que la Administración Pública pueda poseer tan grandes poderes exorbitantes sobre nuestros datos como les atribuye el RGPD.

Una de las propuestas para intenta solucionar el problema, se vierte sobre la premisa de que se tiene que dar una "solución internacional" al problema del Derecho al Olvido, porque en Internet no hay fronteras. Ya comentábamos anteriormente cómo nuestros datos pueden haber sido capturados en Rusia, y pueden esta guardados en Estonia o en Sudáfrica.

Los partidarios de esta solución[308] concluyen que hay una incapacidad política de dar respuesta a la protección de nuestros datos. Esto es así por la territorialidad de los Estados, donde sí que hay fronteras. Se argumenta que esta idea tiene que ser superada en lo relativo a la legislación de Internet, ya que los intereses privados -tanto de individuales como de empresas- y públicos tienen fronteras borrosas.

Para los que fundamentan esta doctrina, se tiene que dar una respuesta que tenga en cuenta la extraterritorialidad jurídica. Y como hemos visto al principio, son los propios convenios internacionales los que hablan de

[308] Entre otros, FREIRE E ALMEIDA. "Um Tribunal Internacional para a Internet". Ed. Amazon

cooperación Internacional. Una cooperación internacional que hasta ahora no se ha elevado hasta donde tiene que llegar para proteger a los ciudadanos y a las empresas de Internet. Nuestros datos –muchos de ellos aportados por nosotros mismos conscientemente- se venden y se compran, dentro de unas relaciones comerciales.

La solución debe aportar seguridad jurídica, tranquilidad, coherencia y permanencia para que las partes sepan exactamente cuáles son las reglas del juego sin que tengan que atender a las diferentes concepciones jurídicas que se dan en las diferentes legislaciones. Recordemos que la libertad de expresión y de información no se conceptúa de igual manera en todos los países.

La razón es fácil de entender. No se puede comprender jurídicamente desde un país diferente decisiones adoptadas por tribunales u organismos de otros países con una distinta concepción jurídica. Decisiones que pueden parecer incluso arbitrarias, cosa que tiene que evitarse a toda costa[309] en aras de la seguridad jurídica de todo el ecosistema y más si tenemos en cuenta, tal y como mantenemos en esta Tesis, la relación entre los datos y el concepto de personalidad con las implicaciones que hemos visto que conlleva en la autodeterminación informativa y con los Derechos Humanos.

[309] Resolution 52 of the 37th General Conference in 2013, UNESCO

15. Reflexiones sobre el concepto de personalidad

I

El Derecho al Olvido tiene que ver con el desarrollo de nuestra propia identidad en Internet. Nadie puede negar a la persona el derecho a desarrollarse y mostrase tal y como se quiere mostrar.

Como se ha estado observando en esta Tesis, el concepto de personalidad y el de desarrollo de la personalidad es algo muy común en las sentencias del TEDH.

Con la irrupción de Internet, el concepto de personalidad -entendido como aquel derecho a ser uno mismo y expresarlo ante los demás- escapa al control de la propia persona.

Aunque no exista una positivación legal del concepto de personalidad[310], en sentido legal, la personalidad puede ser definida como la capacidad para ser titular de derechos y obligaciones. Y se adquiere desde el nacimiento tanto de las personas físicas como de las jurídicas.

La palabra "persona" deriva del latín "personare"; es un término que denota "larva histrionalis", que sígnifica "mascara". La persona actúa como un actor, llevando una máscara cuya importancia era que su voz se oyese fuerte y clara en el escenario.[311]

[310] En la constitución italiana y alemana si que se menciona el concepto de personalidad.
[311] QUINTANA ADRIANO, E. "The Natural Person, Legal Entity or Juridical Person and Juridical Personality". *Penn State Journal of Law & International Affairs. Volumen 4.*

Cornuletti[312] considera que la personalidad se da cuando en la persona se unen el componente legal y el componente económico. Esa unión es la que dota a la persona de personalidad.

En definitiva, es cuando se produce la individualidad; la capacidad para ser distinguido de otro ser. Personalidad va íntimamente unida al concepto de identidad que se recoge en el artículo 8 del CEDH como expresión de la vida privada. "Contar con una identidad es presupuesto para la propia dignidad de la persona, para ser titular de derechos y obligaciones, para tener una existencia en el mundo del Derecho y por tanto en el de los derechos."[313]

Para Kelsen[314], esos derechos y obligaciones son los que configuran a la persona y justamente eso es lo que produce la personalidad.

Habrá quien niegue que la interacción con el mundo virtual no afecta nuestra personalidad ya que no modifica en nada las obligaciones de una persona. Aunque fuese cierto, no se puede negar que la interrelación y, por tanto, la configuración de la personalidad "digital" conlleva o puede conllevar interacciones con los derechos de los cuales una persona es titular.

II

En el ecosistema de la Web nadie está a salvo de que puedan verter opiniones contrarias a la personalidad de un determinado individuo. Pueden ser incluso falsas y que atenten contra su honor o den una imagen distorsionada de esa persona.

[312] CARNELUTTI, F." Teoría General de la Ley" (1955)
[313] DE LA QUADRA SALCEDO Y PIÑAR MAÑAS. " Sociedad digital y Derecho" Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. Madrid, 2018.
[314] KELSEN, H " Teoría pura de la ley" (1934)

Lo mismo pasa con las Redes Sociales donde la interacción, tanto activa como pasiva, va configurando digitalmente la personalidad de un individuo.

En relación al Big Data, tal y como fundamenta como dice Piñar Mañas, la recolección y tratamiento masivo de datos, su incorporación a bases de datos, su cesión a terceros y el cambio de finalidades pueden hacer que una persona sea categorizada en un estrato de personalidad en la cual no se ve, no se siente o no quiere verse representado. Eso sin hablar de que al encasillarte en un determinado grupo compacto de personalidad puede ser que, inconscientemente, se produzca un cambio porgramado de hábitos, tendencias o creencias; esto está fuera del ámbito de la presente tesis.

En España, el Tribunal Supremo, en Sentencia de 15 de octubre de 2015 fundamenta que el Derecho al Olvido digital "no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país".

Lo expresado por el Tribunal Supremo viene a ser la observación de que nadie tiene derecho a reescribir su propia historia alterando su identidad. Esto

tiene sentido en el campo de los buscadores o del derecho a la información cuando se ha cometido un acto que se considera que tiene interés público y se transmite en virtud del derecho a la libertad de información. Nada habría que objetar sobre ello.

III

Vayamos un poco más allá y establezcamos el marco completo de Internet tal y como se ha estabalecido en esta tesis.

Nos encontramos ante una sociedad que interactúa con su entorno de dos maneras: De manera presencial y de manera virtual. ¿Cuál de ellas es la real? Sin entrar una teorización de filosfía del derecho fuera del alcance de esta tesis, cabe responder que las dos son reales. Las dos formas de relacionarnos con el entorno son reales y puede que sean diferentes. Doctrinalmente ya se diferencia la identidad digital de la que denominan real[315] y se establecen dos tipos de personas: la real y la digital[316]. Aunque no estemos de acuerdo en esta distinción sobre diferentes tipos de personas y personalidades, en todo caso, es ya materia del campo de la psicología el adentrarse en cuál de las dos formas de manifestación de nuestra personalidad o de relación –de interacción "en el ámbito real o digital"- es la más auténtica y la que más demuestra nuestra personalidad: Si la realizada socialmente o la realizada mediante la cesión de millones de datos, muchos de ellos personales y cedidos para ser recopilados y tratados de manera inconsciente por parte del individuo y que muchas veces muestran una personalidad que no queremos que sea mostrada a los demás.

[315] SULLIVAN C. "*Digital Identity: An Emergent Legal Concept The role and legal nature of digital identity in commercial transactions",* University of Adelaide Press, (2011).
[316] SOLOVE, D. *The digital person. Technology and privacy in the Information Age,* New York University Press, (2004).

La legislación, en cambio sigue tratando la pesonalidad como un concepto de realización unívoca entre el sujeto y la sociedad. Las comisiones o las omisiones de actos -u opiniones- propios y puntuales pueden ser objeto de inserción en internet y de exhibición ante terceros y emisión de opiniones ante ello. No la trata como un concepto de identidad.

El Tribunal Constitucional Alemán, en sentencia de 10 de octubre de 2018[317] señala que la personalidad es una manifestación de la identidad, y que la personalidad es titular de derechos funda. La sentencia fundamenta que uno de los propósitos del derecho general de la personalidad es garantizar las condiciones básicas que permiten a los individuos desarrollar y proteger su individualidad de una manera autodeterminada. Por lo tanto, continúa, no garantiza la protección contra nada que pueda perjudicar el desarrollo autodeterminado de la personalidad; en cualquier caso, ninguna persona puede desarrollar su individualidad independientemente de las condiciones y afiliaciones externas. Sin embargo, donde el desarrollo autodeterminado y la protección de la personalidad están específicamente amenazados, está cubierto por la protección del derecho general de la personalidad, que sirve para cerrar brechas legales." En definitiva la identidad propia, la real en una democracia, no la que atribuye tasadamente la ley, es parte esencial del libre desarrollo de la personalidad y de la dignidad humana. Pero no basta con construcciones grandilocuentes, pues la identidad en definitiva condiciona la vida misma de la persona, su quehacer cotidiano. Su desarrollo normal y tranquilo como persona"[318]

[317] Disponible en inglés en http://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2017/10/rs20171010_1bvr201916en.pdf?__blob=publicationFile&v=1

[318] DE LA QUADRA SALCEDO Y PIÑAR MAÑAS. Íb. Supra.

Piñar Mañas[319] expone como la identidad se manifiesta en dos esferas: La pública y la privada. La democracia, continua diciendo, implica que se sepa lo menos posible de las personas pero que a su vez implica también conocer lo necesario para mantener el orden social y los derechos fundamentales de las personas. Las dictaduras quieren saber todo de las personas para controlarlas y mantener el poder.

Esta distinción entre personalidad pública y privada ya se da, aunque no con esta terminología, en el RGPD. Las administraciones públicas pueden tratar los datos recolectados de manera más extensiva que las empresas particulares y gozan de ciertas prerrogativas tal y como se expondrá en el siguiente capítulo en el apartado de tratamiento de los datos en la Unión Europea.

IV

Lo expuesto hasta ahora muestra como la legislación se centra en defender la individualidad de las personas o lo que es lo mismo la manifestación de la personalidad cuando se produce una "intromisión ilegítima[320]" en la personalidad como sinónimo de identidad de la persona siempre y cuando se produzcan o puedan producirse consecuencias para la persona.

No consideramos que haga falta una intromisión ilegítima para que la individualidad de una persona, su identidad –cosa diferente de su identificación-, quede comprometida. Tal y como está concebida la legislación –que no tiene en cuenta ni el Big Data, por falta de concreción jurídica del concepto tal y como hemos visto, ni el Internet de las cosas- la intromisión puede ser todo lo legítima que se proponga ya que atienda a las

[319] DE LA QUADRA SALCEDO Y PIÑAR MAÑAS. Íb. Supra.
[320] GARRIGA DOMINGUEZ, A. "Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua". Ed. Dikynson. (2016)

finalidades para las cuales se ha dado permiso. Pero, como mantenemos, no se tiene en cuenta que múltiples datos aislados que sean tratados y unidos pueden dar lugar a que esa intromisión devenga "derivadamente" ilegítima ya sea porque muestre, descubra o manifieste aspectos que sean configuradores de la esencia de la personalidad y que identifiquen o muestren la identidad de la persona y que ésta no quiera que se sepan o divulguen y mucho menos que se exploten comercialmente, cosa que puede influir en el libre desarrollo de la personalidad[321] ya que se nos puede mostrar solo una visión del universo y no otras -aunque esto es un ámbito ateniente a la psiclogía- o que las Administraciones Públicas los utilicen para determinados fines amparados en un difuso e indeterminado "interés general" no motivado o atendiendo a motivaciones espúreas muy alejadas del verdadero concepto de democracia.

Tampoco consideramos que la intromisión en la identidad de las personas puediera ser merecedora de reproche si solo comporta o puede comportar consecuencias jurídicas. Si bien esto es cierto con las leyes civiles actuales, estas no están adaptadas a los escenarios futuros donde la identidad digital será mucho más importante que la identidad "real"[322] y que puede ser ampliamente influenciable por factores externos -de nuevo nos encontramos otra vez más en el campo de la psicología pero también en el de la realidad como Inteligencia Artificial, genoma, robots domésticos, smarts cities,

[321] PIÑAR MAÑAS es de la misma opinión aunque concluye por diferentes vías. Ver, DE LA QUADRA SALCEDO Y PILAR MAÑAS. Íb. Supra.
[322] Entre otros, SCHMIDT E. Y COHEN J. "*El futuro Digital"* Ediciones Anaya, Madrid (2014) .

computación cuántica[323] e Internet de las cosas- ya que es imposible ser permeable a los que nos rodea.

En definitiva entendemos que parte esencial del problema es que se produce una fusión del concepto jurídico de identidad con el de identificación con todo lo que ello acarrea de problemas éticos y morales que no son objeto de la presente tesis. Tan solo podemos observar que las normas jurídicas actuales no se adaptan a este esquema ya que la tecnología va muy por delante del Derecho. Tal vez, tal y como sugiere Piñar Mañas[324], que cita a García de Enterría, ante este escenario tecnológico tan cambiante y desconocido tal vez sería bueno volver a los principios básicos del Derecho. Aquí el Derecho al Olvido tiene algo que decir, pues aunque no se pueda cambiar el pasado ni falsearlo ya que las personas tienen que ser responsables de sus actos, no es menos cierto que la recopilación y tratamiento de datos masiva -inadvertida muchas veces- lleva a desvelar parámetros esenciales de nuestra personalidad, identidad e identificación llegando a configurarla o definirla. De alguna manera se tiene que dar el poder a las personas de ejercer su derecho fundamental a que estos aspectos íntimos no sean tratados económicamente o utilizados, ya sea en si mismos o por tratamiento o agregación, para fines ajenos a su finalidad inicial.

[323] https://www.lavanguardia.com/ciencia/20191023/471156519790/ordenador-cuantico-google-supremacia-computacion-cuantica.html
[324] DE LA QUADRA SALCEDO Y PIÑAR MAÑAS. Íb. Supra.

16. Conclusiones.

Internet ha cambiado el mundo. No es algo temporal, pasajero o que esté de moda. Es una parte más de nuestra vida.

Internet no es solo una página web o un buscador. Es la interconexión que realizan diferentes máquinas o aparatos y que, gracias a ella, nos aporta un valor añadido en forma de servicio, producto o intangible material como puede ser una idea, concepto, opinión u agrupación por preferencias o perfiles o apoyo a la toma de decisiones por poner unos ejemplos.

No es objeto de esta tesis el debatir sobre este tema pero se puede decir, sin nigún tipo de duda, que no es que haya dos mundos separados, el real o físico y el virtual, sino que todo forma parte de la misma realidad en la que nos movemos.

A nadie se le escapa la idea de que las personas somos titulares, por el mero hecho de existir, del derecho a la privacidad. Hay cosas nuestras que forman parte de la esfera más íntima. De igual manera si para las marcas nadie discute su derecho a tener una marca o imagen personal y reconocida, nadie debería negar el derecho a una persona ya no solo a la integridad de su imagen sino el derecho a proyectar determinada marca o imagen personal.

El Derecho al Olvido no es un tema baladí en la sociedad actual y futura. Nuestro rastro en internet, conocido como “huella digital” va a condicionar nuestro futuro. No tiene nada que ver con el hecho de que el nombre de una persona salga en los resultados de un buscador, que también, sino en el hecho de que cada vez nuestros datos son captados, diseccionados, analizados y puestos a disposición de terceros por muchos dispositivos electrónicos, y eso

no está recogido por la legislación ni la jurisprudencia o la doctrina. Se le añade la problemática de que muchas veces no somos conscientes o no desearíamos que se supiesen o se tuviesen en cuenta bajo ningún concepto esos datos "cedidos". Además esos datos que Internet -en general- sabe de nosotros puede ser que no hayan sido cedidos directamente por su titular o que, por ejemplo, la informción disponible en abierto sobre una persona – en un buscador- no haya sido dipuesta a terceros por la libre voluntad del titular o que simplemente sean falsos, no veraces, inexactos, sesgados y manipulados o que proyecten una imagen personal que no se quiera dar como puede ser el caso de Redes Sociales o "tags" de fotos.

En definitiva, las personas carecen del control sobre sus datos.

El Derecho al Olvido es un derecho nuevo y direrente al de otros derechos, que se concibe como protección de diferentes derechos y libertades. Y esas diferencias son insoslayables en este momento. No sólo porque el derecho anglosajón y el europeo son diferentes, sino porque, como hemos señalado, no se puede obviar la realidad física de los diferentes estados y alcance de los tribunales nacionales. Y de la rapidez que se exige en la resolución de los casos en los que se reclama el Derecho al Olvido, ya que el mundo online está abierto a todo el mundo y la reduplicación de los datos -y por tanto su alcance- se produce a una velocidad impensable en el mundo offline.

Hay que concluir que el Derecho al Olvido y el control de la privacidad debieran ser entendidos de igual manera en todas partes y tener eficacia "erga omnes". Y eso sólo se puede conseguir con la cooperación internacional.

En definitiva, cada país conceptúa el Derecho al Olvido de una manera diferente como hemos visto, aunque teleológicamente la conceptualización del Derecho al Olvido es bien similar.

La problemática sobre este aspecto radica en que, en un mundo cada vez más abierto, la legislación de cada Estado de manera indiviual, o incluso legislada en un espacio cerrado como el europeo, tiene difícil encaje. Se han podido ir "desperdigando" datos privados por todas las partes del mundo.

Además muchas compañías que obtienen, tratan o muestran datos son corporaciones intenacionales con sedes en diferentes países y sometidas a diferente legislación y en donde la decisión de ejecutar cualquier decisión de un juez o autoridad de un país tercero es pácticamente imposible.

El Derecho al Olvido, aunque es un derecho nuevo, es un derecho limitado por otros derechos conceptuados como fundamentales.

El Derecho al Olvido se conceptualiza legalmente en todo el mundo como un derecho que sería solo aplicable frente a los buscadores de Internet o empresas que trabajan en el mundo de la Web. Si nos fijamos en la legislación, el Derecho al Olvido se conceptualiza a través de la creencia de que los datos que se tienen que olvidar son únicos y localizables. No tiene en cuenta el Big Data ni los datos recabados mediante el Internet de las Cosas.

Sería deseable, y creemos que necesario, que el Derecho al Olvido se legislase a escala lo más global posible y que tuviese en cuenta el Big Data y el Internet de las Cosas, dejándolo abierto a las nuevas realidades tecnológicas.

La tecnología actual y futura hará que el concepto de personalidad y el derecho a la propia imagen varíen en su concepción actual. No sería deseable una legislación ad-hoc ante cada nuevo suceso o desarrollo tecnológico que fuese ocurriendo pues la tecnología siempre irá por delante del Derecho.

Con las nuevas tecnologías y el Big Data, identidad e identificación personal acabarán confluyendo y volviéndese conceptos borrosos entre ellos. El Derecho al Olvido debe garantizar, en este sentido, que esa confluencia garantice los derechos fundamentales de las personas ya no solo por la intromisión de las empresas privadas sino por la intromisión expansiva de las administraciones públicas.

CAPÍTULO IV: EL CONSENTIMIENTO

1. Aproximación conceptual al consentimiento legal.

I

El consentimiento válido presupone la capacidad de la persona para darlo. Las normas que regulan la capacidad para consentir no son iguales en todos los paises, ni incluso dentro de la propia Unión Europea.

La RAE, en su diccionario jurídico, define "consentimiento"[325] de manera general como "acción u acto de consentir" -"permitir algo o condescender en que se haga"[326]-, así como la "manifestación de voluntad, expresa o tácita, por la que un sujeto se vincula jurídicamente".

De conformidad con los artículos 1254, 1261 y 1262 del código civil español, la RAE define el consentimiento como "requisito básico para el perfeccionamiento del contrato que consiste en la manifestación de voluntad de celebrarlo y de conformidad con su objeto y causa".

La RAE continua con la definición penal de consentimiento como un eximente que se da cuando el titular jurídico del derecho consiente que le lesionen ese bien jurídico del cual es titular.

Por su parte, en lenguaje jurídico de Estados Unidos podemos definir el consentimiento como "Voluntary Acquiescence to the proposal of another; the act

[325] https://dej.rae.es/lema/consentimiento
[326] https://dle.rae.es/srv/search?m=30&w=consentir

or result of reaching an accord; a concurrence of minds; actual willingness that an act or an infringement of an interest shall occur.

Consent is an act of reason and deliberation. A person who possesses and exercises sufficient mental capacity to make an intelligent decision demonstrates consent by performing an act recommended by another. Consent assumes a physical power to act and a reflective, determined, and unencumbered exertion of these powers. It is an act unaffected by Fraud, duress, or sometimes even mistake when these factors are not the reason for the consent. Consent is implied in every agreement."[327].

II

El derecho de Estados Unidos, al igual que el inglés[328], surge de la interpretación de las diferentes controversias que se ha venido dando y que han sido resueltas por los diferentes Tribunales. De ahí que la jurisprudencia sea auténtica y genuina fuente de Derecho. Es lo que se conoce como el "judge-made law", donde los precedentes -el caso concreto- tienen una importancia capital para resolver los casos, sin que se pueda atender a una codificación estructurada como en el derecho continental.

La casuística, como decimos, es el elemento primordial para resolver las diferentes controversias. Y esto mismo es aplicable al Big Data y, en consecuencia, al consentimiento. Esto es así porque, en el fondo, la cesión de nuestros datos, sean personales o no, se enmarcan dentro de un contrato entre las partes que puede ser

[327] West's Encyclopedia of American Law, edition 2. The Gale Group, Inc. (2008)
[328] Ya desde 1066, con el reinado de Guillermo I de Inglaterra

derivado, por ejemplo, de la compra de un aparato conectado al Internet de las Cosas[329].

Es el caso de la Sentencia Schloendorff [330], el que marca el "nacimiento legal" de la jurisprudencia sobre la teoría del consentimiento informado y libre en Estados Unidos, en donde los doctores diagnosticaron a la Sra. Schloendorff un tumor y sugirieron cirugía, que ella rechazó. Los médicos, sin embargo, decidieron operarla igualmente. Pero más tarde, la Sra. Schloendorff desarrolló gangrena y le tuvieron que amputar los dedos.

El Tribunal falló que "todo ser humano de edad adulta y que esté en pleno uso de sus facultades mentales tiene el derecho de determinar lo que se le hace a su cuerpo; un cirujano que realiza una operación sin el consentimiento de su paciente comete una agresión de la que es responsable de los daños resultantes. Esto es cierto excepto en casos de emergencia donde el paciente está inconsciente y cuando es necesario operar antes de que se pueda obtener el consentimiento."

Sin embargo, en Estados Unidos el "nacimiento legal" doctrinal de la teoria del consentimiento se marca en la obra "The Right to Privacy"[331] de los abogados Barren y Brendays, escrita en 1890, que subrayaban que la privacidad decae cuando una persona otorga su expreso consentimiento o cuando es él mismo el que publica sus datos. En el caso Marks vs. Jaffa[332], en 1893 , ya se cita la doctrina contenida en este libro fundamentando que nadie, sin su consentimiento, puede utilitzar la imagen o el nombre de una persona ya que se consideró que la imagen es propiedad de una persona. Esta jurisprudencia fue modificada en 1899 por la

[329] Piénsese, por ejemplo, en un asistente virtual.
[330] Véase Schloendorff v. Society of New York Hospital, 105 N.E. 92, 93
[331] Harvard Law Review vol. IV, núm. 5, 15 de diciembre de 1890,
[332] Marks v. Jaffa, 26 N.Y.S. 908, 909

sentencia Atkinson v. John E. Doherty & Co[333]al considerar que el concepto de imagen no se encuentra incluido en el concepto de propiedad.

La teorización de la privacidad en Estados Unidos, tal y como explica la profesora Saldaña[334], fue sistematizada por W. L. Prosser[335]quien expone que existe violación de la propiedad con "la apropiación de ciertos elementos de la personalidad, como el nombre, la imagen o la voz, con fines de lucro (appropiation of some elements of an individual's personality), protegiéndose a través de la correspondiente privacy tort el daño ocasionado al utilizarse por terceros los atributos de la personalidad sin previo consentimiento"[336].

III

En Rusia, en virtud de los artículos 23 y 24 de su Constitución[337], el "consentimiento"-aunque sin definirlo- es algo totalmente ligado a la protección de datos. Nótese aquí que la Constitución rusa ha querido distinguir entre consentimiento y "consentimiento voluntario"[338] ya que cuando es voluntario, lo recalca.

IV

En China, se han aprobado Especificaciones de Seguridad Personal[339](GB/T 35273—2017) de manera similar al RGPD europeo, donde no se define el

[333] Atkinson v. John E. Doherty & Co., 80 N.W. 285, 286, 288-289
[334] SALDAÑA, M.N. Íbidem. Supra en 129
[335] PROSSER, W.L. "Privacy", Californian Law Review. Disponible en https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview
[336] SALDAÑA, M.N. Íbidem.
[337] Disponible en http://www.constitution.ru/en/10003000-03.htm (último acceso abril 2019)
[338] Véase articulo 21 Consttución Rusa.
[339] Disponible en https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf (última visita agosto 2019).

consentimiento pero sí que menciona que tiene que ser por escrito o por declaración afirmativa.

La palabra consentimiento solo se usa en ciertos casos. Las secciones 5.3 (Autorización para la recopilación de información personal) y 5.4 (Exenciones para la búsqueda de consentimiento) simplemente usan la palabra "consentimiento", mientras que la sección 5.5 va un paso más allá al referirse al "consentimiento explícito" para la recopilación de información confidencial personal

Es significativo que el borrador original de las Especificaciones publicado para comentario público requiriese el consentimiento explícito para todo, pero el término "explícito" se eliminó en las secciones de la versión final. Por lo tanto, al igual que en la legislación rusa, es una interpretación razonable decir que el consentimiento es diferente y "quizás menos" que el consentimiento explícito.[340]

V

En el ámbito de la Unión Europea, a la vista de lo establecido en el artículo 8 CEDF[341], el consentimiento para la obtención y tratamiento de datos es un tema crucial en la legislación del RGPD, aunque el consentimiento, como tal, ya se recogía en la Directiva del Consejo 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.

[340] SACKS, S. "China's Emerging Data Privacy System and GDPR". Centre for strategic and international studies.

[341] Sobre los datos de caráccter personal: Estos datos se tratarán 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.

Así, el consentimiento actualmente está definido en el Art. 4 RGPD, que expone que el "consentimiento del interesado" es 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.

Los considerandos del RGPD nos dan una idea muy aproximada de la "interpretatiu legis" del concepto de consentimiento en el ámbito de la Unión Europea.

Así, el el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado[342]de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, cabe entender que el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

De igual manera, el RGPD considera que para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado[343] o sobre alguna otra base legítima establecida conforme a Derecho, y que cuando el

[342] Otros autores añaden la proporcionalidad o el respeto a los Derechos Humanos.
[343] Ver art 6.1 RGPD

tratamiento se lleva a cabo con el consentimiento del interesado -curiosa hipèrbole legal; no sabemos qué pasará cuando se lleva a cabo sin el consentimiento-, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. Tiene que haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace, considerando además que para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento.

A tenor del considerando 71, no se produciría consentimiento, salvo que sea explícito, en el tratamiento de datos que incluya la elaboración de perfiles consistente en cualquier forma de tratamiento de los 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, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Interesa destacar, que no se contempla en el RGPD el consentimiento tácito o el llamado consentimiento "opt-out", dodne si el consentimiento no es expresamente declinado -como por ejemplo, marcando una casilla- se presume como concedido.

VI

Article 29 Working Party, en su Dictamen 15/2011 sobre la definición del consentimiento[344], fundamenta que el concepto de consentimiento no es igual en

[344] Disponible en https://ec.europa.eu/justice/article-29/documentation/index_en.htm

todos los paises europeos -ni incluso en la normativa europea-, y este criterio se ha venido configurando muchas veces en legislaciones sectoriales específicas e interactuará con el adoptado en la normativa de protección de datos.

Además, el Dictamen recuerda que el consentimiento es uno de los pilares básicos -aunque no el único- para el tratamiento de datos, y que este consentimiento tiene que utilizarse en un contexto adecuado y tiene que reunir todos los elementos indispensables, entre ellos el elemento de inequívoco, es decir, que venga confirmado por las acciones posteriores de la persona titular.

No deja de resultar interesante -y confusa cuando menos, desde una perspectiva legal, tal y como observaremos sobre todo en el consentimiento del menor- la fundamentación que realiza dicho informe al establecer que "El concepto de consentimiento también se utiliza en otros ámbitos del Derecho, especialmente en el Derecho contractual. En este contexto, para garantizar la validez de un contrato se tendrán en cuenta otros criterios distintos de los especificados en la Directiva, tales como la edad, la influencia indebida, etc. No existe contradicción sino solapamiento entre el ámbito del Derecho civil y el ámbito de aplicación de la Directiva: esta no aborda las condiciones generales de validez del consentimiento en el ámbito del Derecho civil, pero tampoco las excluye. Esto significa, por ejemplo, que para examinar la validez de un contrato en el marco del artículo 7, letra b), de la Directiva, habrá que tener en cuenta los requisitos de Derecho civil. Además de la aplicación de las condiciones generales de validez del consentimiento previstas en el Derecho civil, el consentimiento exigido en el artículo 7, letra a), también debe interpretarse teniendo en cuenta el artículo 2, letra h), de la Directiva[345]."

[345] Art 29 WP hablaba aquí sobre el borrador de Directiva, cuya numeración de artículos fue modificada en la redacción final. En concreto hablaba sobre la definición de consentimiento que

En el mismo informe 15/2011[346], Article 29 WP nos glosa cada uno de los elementos del consentimiento en base a la legislación europea.

VII

Y es que efectivamente, el consentimiento es parte fundamental en la validez de los contratos y no puede entenderse sin considerarla un requisito de éstos. Solo podemos prestar nuestro consentimiento cuando conocemos realmente que cosa estamos contratando, porqué se establecen unas determinadas prestaciones y para qué.

Pero no hay que pensar únicamente en el binomio consumidor-prestador del Servicio o de la entrega del bien.

El consentimiento para el tratamieto de datos también se puede dar en las relaciones con las Administraciones Públicas o en el ámbito laboral, por poner dos ejemplos.

Surgen grandes dudas, en estos dos supuestos –pero también en otros- sobre si el consentimiento llega a su perfección[347].

El articulo 6.1, apartados e) y f) , del RGPD señala que el consentimiento será lícito cuando se den, entre otras, alguna de las siguientes circunstancias:

Por un lado, que el tratamiento se necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

ahora aparece en art.7, letra 11. En su redacción original decía "«toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.»"

[346] Ib. Supra

[347] Entre otros, ver informe Art 29 WP, 2/2017 sobre el tratamiento de datos en el Trabajo.

responsable del tratamiento. Esto es aplicable al ámbito de las Administraciones Públicas.

Por otro lado, que el tratamiento sea 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. Esto sería aplicable al ámbito laboral y al ámbito de las Administraciones Públicas.

En estos dos ámbitos analizados existe lo que se ha denominado un "desequilibrio de poder"[348], tal y como se ha definido en el campo de la psicologia en relación con la cesión de datos[349].

El considerando 43 RGPD establece que para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Y continúa considerando que se presumirá que el consentimiento no se ha dado libremente cuando (este consentimiento) no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea

[348] Informe 15/2011 Art 29 WP. Ib. Supra.
[349] Ver COHEN, J.E , "*Configuring the Networked Self: Law, Code, and the Play of Everyday Practice"* (Yale University Press, 2012); HILDEBRANDT, M "Profiling and the Rule of Law" (2009)

dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

En el caso de las Administraciones Públicas, el "desequilibrio de poder" es evidente. De la lectura del articulo 6.1. e) no parece que, salvo que sea obligatoria la posición "pasiva" del administrado por razones de "interés público" o "ejercicio de poder público", las Administraciones Públicas puedan tratar los datos que poseen de la manera que quieran. Solo en estos casos, estarán autorizadas a tratar los datos del administrado aunque sea sin su consentimiento.

No está de menos recordar que el interés público deberá estar motivado suficientemente y el ejercicio del poder público no podrá ser arbitrario o contrario al fin teleológico por el cual se puede ejercer -la denominada en la doctrina administrativa la "desviación de poder"-.

Imaginemos una Administración Pública que nos pide un número de teléfono móvil para acceder, por ejemplo, a servicios de salud o de transporte. ¿Podría utilitzar la Administración ese teléfono que le hemos proporcionado para otro sevicio como la notificación de una multa? Este esquema no parece ajustarse a lo querido por el legislador europeo. O al menos no de conformidad con el articulo 6.1 e) y 6.1 f) en relación con el artículo 7.4 RGPD que establece que a la hora de "evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato."

Sin embargo, a las Administraciones públicas simepre les queda la clausula del articulo 6.1.c) que establece que el tratamiento será lícito cuando "el tratamiento

es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;"

Este artículo recién citado entronca con la prerrogativa que tiene la administración pública de obligar a un administrado a proporcionar determinados datos personales -y a poder tratarlos- de manera obligatoria sin que sea opcional (el proporcionarlos o no) para acceder a ese servicio. Es decir, la administración tiene la prerrogativa de imponer como obligatorio la cesión de determinados datos para acceder a un servicio.

El informe Art 29 WP 15/2011[350] considera que la cesión de datos tiene que ser "no condicionada". No existirá la libre elección de los administrados e incluso, aunque la contraprestación de la Administración se pueda obtener de otra manera, los costes pueden ser exsorbitantes o sufrir perjucio evidente[351]. De esta manera, "el consentimiento solo puede ser válido si el interesado puede realmente elegir y no existe riesgo de engaño, intimidación, coerción o consecuencias negativas importantes (por ejemplo, costes adicionales sustanciales) si no da su consentimiento. El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad."[352]. El mismo Art 29 considera que la presión para consentir "puede manifestarse de formas muy distintas"[353].

En el supuesto del ámbito laboral también surgen los problemas de consentimiento. También existe, obviamente, un "desequilibrio de poder" entre

[350] Ib. Supra
[351] El Consideando 43 del RPD establece in fine que" El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".
[352] Informe Art 29 WP. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679.
[353] Informe Art 29 WP. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679.

empresa y trabajador. Por lo tanto, la problemática expresada anteriormente se reproduce con casi igual intensidad.

2. Consentimiento, Big Data e Internet de las Cosas.

I

Es una de las premisas de esta tesis y que se ha ido confirmando ante lo expuesto y ante lo que se expondrá: La normativa actual no sirve para abordar el tema del Big Data, y el consentimiento, pieza clave, es buena muestra de ello.

En cuanto al consentimiento, en uso de webs o aplicacions web, la norma general de otorgamiento del consentimiento es el "consentimiento implícito". Aquí, el solo hecho de usar un servicio, generalmente otorgado con una sola casilla de verificación en un formulario de “términos y condiciones” muy largo, es suficiente para otorgar el consentimiento para usar los datos de una persona.

En este escenario, podemos dar como válido que, salvo casos muy concretos, los individuos no tendrán una idea clara de que datos se han intercambiado. Es posible que hayan rellenado el nombre, la dirección y otros detalles en un formulario, pero no sabrán durante cuánto tiempo se almacenarán estos datos. En última instancia, es difícil para una persona saber a quién se le ha otorgado acceso a su información privada. No solo eso, sinó que además una persona puede estar consintiendo el uso de cookies, con toda la problemática que hemos abordado.

II

El consentimiento en la era del Big Data -tanto del tratamiento como de la recolección, cabe recordar- y del Internet de las Cosas, presenta varios problemas fundamentales.

En primer lugar, existe una vorágine por parte de las empresas a la hora de conseguir datos de los clientes; datos que muchas veces no son necesarios para el cumplimiento del objeto del contrato pero que parece que se recopilan "por si acaso" o en aras de "mejorar el servicio".

En segundo lugar, no solo recopilan datos de clientes sino de terceras personas que no son clientes pero que actúan dentro del radio de recolección de datos o que han interactuado con el cliente de determinada manera. Se crea, por tanto, un perfil de personas que "interactúan" con el cliente pudiendo establecer quién es su grupo familiar, su grupo de amistades, su grupo de trabajo, etc.

En tercer lugar, aunque no se recojan, en bruto, datos personales, se puede dar el efecto de que esos datos no personales, en combinación con otros, nos acaben mostrando datos sobre la personalidad individualizada o la identidad de una persona.

En cuarto lugar, se puede producir lo que denomino la "fatiga del consentimiento" entendiendo ésta como aquella que se produce cuando estamos dipuestos a ceder algún tipo de datos pero no todos. Decae nuestro consentimiento en la cesión de algún tipo de datos, que puede ser sobrevenida, pero no nos es posible discriminarlos en nuestra relación con el IoT que nos presta el servicio y, del cual, no podemos o queremos prescindir.

Se ha creado una suerte de contrato de adhesión entre el uso del IoT y la recolección y tratamiento de nuestros datos a gran escala. En definitiva, las personas no tienen libertad de elección sobre sus propios datos.

En quinto lugar, nos encontramos con toda la problemática relativa al consentimiento de los menores e incapacitados.

En sexto lugar, nos encontramos con que muchas veces, la cesión y tratamiento de datos se excluyen expresamente del contrato de prestación del servicio.

En séptimo lugar, el tratamiento masivo de los datos derivados de su obtención, se puede producir automáticamente y a gran escala haciendo perder de facto cualquier tipo de derecho que el titular creyese que podía tener sobre esos datos. Los datos pueden haber sido tratados en un instante, es decir indexados, incorporados a otra base de datos, linkados a otra información, segregados o cualquier tipo de operación que con ellos se pueda hacer dada la tecnología y la capacidad de tratamiento disponible.

En octavo lugar, las expectativas "razonables" de uso de los datos por parte del responsable del tratamiento, y sobre los cuales se realiza el consentimiento, son sobrepasadas de manera impensable por el rápido desarrollo de la tecnología.

En noveno lugar, se fia la problemática del consentimiento al "uso reponsable de la información"[354] que se comparte por parte de los usuarios.

III

Así, el informe 15/2011 establece, tal y como hemos visto anteriormente, que para que el consentimiento sea libre tiene que ser "no condicionado" ya que, en

[354] PIÑAR MAÑAS, JL y otros, "Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad" Ed. Reus.

principio, existe un "desequilibro de poder" entre el usuario y el prestador del Servicio; "el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distintas) que impida que este ejerza su libre voluntad."

Puede darse que para poder utilizar una aplicación, por ejemplo, se tenga que ceder datos que no son estrictamete necesarios para el servicio que se pretende utilizar, sinó que van "más allá"[355], cosa que hace que "en términos generales, el consentimiento quedará invalidado"[356].

3. La posición de los interesados ante el consentimiento para el tratamiento masivo de datos en la legislacion europea.

3.1. Información y acceso a los datos recabados.

I

Caba decir, a modo general, que para la legislación de la Unión Europea el tratamiento será licito si, tan solo, se ha prestado el consentimiento -aunque hay otras razones-[357].

A efectos de estudiar el consentimiento que se debe prestar para que los datos puedan ser recogidos y tratados, interesa, en primer lugar, destacar aquí los articulo 13 a 15 del RGPD, dado que configuran los derechos de los

[355] Art 29 WP. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Versión de 10 de abril de 2018.
[356] Art 29 WP. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Versión de 10 de abril de 2018.
[357] El art 6.1 del RGPD establece que " El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;(...)"

interesados sobre los cuales se han recogido los datos personales así como las obligaciones de los responsables del tratamiento de los datos[358].

En primer lugar, el artículo 13 RGPD establece que:

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f)[359], los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias

[358] Estos artículos fueron ampliamente enmendados en los trámites de lectura. Ver, por ejemplo, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014AP0212&from=EN

[359] 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.

indicadas en los artículos 46 o 47 o el artículo 49, apartado 1[360], párrafo segundo, referencia a las garantías adecuadas o apropiada y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a)[361], o el artículo 9, apartado 2, letra a)[362], la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está

[360] Se refiere a la transferencia internacional de datos y a países que garanticen portección a los titulares de datos, mediante acuerdos de cooperación o, en su defecto, cuando haya consentimiento u obligación legal tasada en el art. 49.1
[361] El interesado ha dado su consentimiento explícito.
[362] Ver nota anterior.

obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4[363], 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.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Por su parte, el artículo 14 RGPD en relación a la información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado establece que:

[363] El art.22 RGPD establece que 1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1[364], párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

[364] Ver nota Supra.

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f)[365], los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a)[366], la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4[367], 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.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

[365] Ver nota Supra
[366] Ver nota Supra
[367] Ver nota Supra

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1[368], o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar

[368] El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Para acabar, el artículo 15 ralativo a los derechos de acceso del interesado, establece que:

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) 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;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) 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;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4[369], 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.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46[370] relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos.

[369] Ver nota. Supra
[370] Referente a las garantías necesarias para la rasnferencia de datos.

Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

En definitiva, el RGPD considera que los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Todo interesado tiene el derecho a conocer los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento.

II

Estos derechos recogidos en los artículos 13 a 15 no son en modo alguno una innovación del RGPD. Ya estaba estipulado en la Sección 34 de la antigua Ley Federal de Protección de Datos de Alemania[371] (Bundesdatenschutzgestz, BDSG).

La Sección 34 de BDSG estipulaba que se podría solicitar información sobre:

a) todos los datos almacenados sobre la persona con derecho a recibir la información;

b) el origen de los datos, es decir, dónde y cuándo se recopilaron, o de quién se originaron los datos;

[371] Vigente hasta 2018. Disponible en https://rm.coe.int/09000016806af19d

c) el propósito respectivo del almacenamiento de los datos; y,

d) si los datos se transmitieron a terceros, todos los destinatarios categorías de destinatarios a quienes se transmitieron los datos almacenados;

Si se compara el art. 15 RGPD con la Sección 34 citada, rápidamente se hace evidente que existen paralelismos considerables.

El legislador belga también recogía el derecho de acceso al artículo 10 de la Ley de 8 de diciembre de 1992[372] que permitía que el interesado requiera que el controlador no solo confirme que los datos relacionados con él se estén procesando o no, así como información sobre dicho procesamiento (propósito, categorías de datos con los que se relaciona y con quién y cualquier información disponible sobre el origen de estos datos, la lógica subyacente al procesamiento en caso de decisiones automatizadas en el sentido del Artículo 12a), pero también su comunicación, en una forma inteligible, así como información sobre los derechos del interesado en virtud de los artículos 12 (derecho de rectificación y oposición) y 14 (derecho de presentar una solicitud ante el Presidente del Tribunal de Primera Instancia).

El legislador francés, por su parte, implementó el derecho de acceso al artículo 39 de la Ley de Protección de Datos donde el interesado puede requerir que el controlador confirme que sus datos se están procesando, información sobre el procesamiento (propósito, destinatario de datos, categorías de datos procesados, transferencias de datos, información sobre lógica subyacente al procesamiento automatizado en caso de una decisión tomada en base a ello), así como una copia de los datos (contra el pago, si corresponde, de una suma que no puede exceder el costo de reproducción).

[372] https://www.senseball.com/es/politica-privacidad

III

Estos derechos, además de no ser de nueva creación, ya vienen avalados por la Jurisprudencia del TJUE.

Así, en el Asunto C-553/07 de 7 de mayo de 2009, el TJUE requiere que los Estados miembros otorguen un derecho de acceso a la información sobre los destinatarios o categorías de destinatarios de los datos, así como el contenido de la información comunicada no solo para el presente, sino también para el pasado. Corresponde a los Estados miembros establecer un plazo para mantener esta información y un acceso correlativo a la misma, lo cual, manifestaba el TJUE, es, en primer lugar, un buen equilibrio entre, por un lado, el interés del interesado en proteger su vida privada, en particular utilizando la intervención y los recursos previstos por la Directiva 95/46; en segundo lugar el TJUE requiere establecer regulaciones que limitan la retención de información sobre los destinatarios o categorías de destinatarios de los datos y el contenido de los datos transmitidos por un período de un año y, en consecuencia, limitan el acceso a esta información, mientras se mantienen los datos básicos mucho más tiempo, no sería un equilibrio justo de intereses y obligaciones a menos que se demuestre que una mayor retención de esa información sería una carga excesiva para el controlador.

De igual manera, en los Asuntos Acumulados C-141/12y C-372/12, el TJUE fundamenta que el artículo 12, letra a), de la Directiva 95/46 y el artículo 8, apartado 2, de la Carta de los Derechos Fundamentales de la Unión Europea deben interpretarse en el sentido de que el solicitante de un título tiene derecho a acceder a todos los datos personales que le conciernen y que sean objeto de un tratamiento por parte de las autoridades administrativas

nacionales en el sentido del artículo 2.b) de dicha Directiva. Para que este derecho se cumpla, es suficiente que el solicitante esté en posesión de una descripción completa de esos datos en una forma inteligible, es decir, un formulario que le permita a dicho solicitante conocer dichos datos.

En el Asunto C-201/14, de 1 de octubre de 2015, en relación a los artículos 10, 11 y 13 de la Directiva 95/46 / CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas en lo que respecta al tratamiento de datos personales y la libertad de circulación. de estos datos, el TJUE establece que deben interpretarse en el sentido de que excluye medidas nacionales, como las controvertidas en el procedimiento principal, que permiten a una administración pública de un Estado miembro transmitir datos personales a otra administración pública y su tratamiento posterior, sin que las personas interesadas sean informadas de dicha transmisión o tratamiento.

IV

Hay que señalar, sobre estos derechos de acceso, que la única excepción al derecho a obtener una copia de los datos sujetos a tratamiento en el artículo 15 es desconcertante. Según esta disposición, el derecho a obtener una copia no puede afectar negativamente los derechos y libertades de los demás.

La excepción es peligrosa en la medida en que está formulada de manera demasiado amplia y parece implicar que cualquier conflicto entre el derecho a obtener una copia y el derecho y las libertades de otro, siempre resolverán en detrimento del primero**.**

Por otro lado, El RGPD no especifica cómo realizar una solicitud válida. Por lo tanto, un individuo puede presentar una solicitud de acceso de interesado

verbalmente o por escrito. Por otro lado, no parece que una solicitud tenga que incluir la frase "solicitud de acceso del interesado" o el contenido del artículo 15 del RGPD. Además, hay que señalar que existe una gran dificultad, ya no solo técnica, debido al gran número de información que debe tenerse en cuenta, sino de la incertidumbre en cuanto a su transmisión a la persona interesada.

El Article 29 Working Party establece, en las Directrices sobre la toma de decisiones y la elaboración de perfiles individuales automatizados a los efectos del Reglamento 2016/679[373], que la elaboración de perfiles y la toma de decisiones automatizada se utilizan en un número creciente de sectores, tanto privados como públicos. La banca y las finanzas, la asistencia sanitaria, los impuestos, los seguros, el marketing y la publicidad son solo algunos ejemplos de los campos en los que están destinados a trabajar.

Los avances en tecnología y las capacidades de análisis de Big Data, inteligencia artificial y aprendizaje automático han facilitado la creación de perfiles y la toma de decisiones automatizadas con el potencial de impactar significativamente los derechos y libertades de las personas.

Como hemos venido diciendo a lo largo de la presente Tesis, la disponibilidad frecuente de datos personales en Internet y de los dispositivos de Internet de las cosas, y la capacidad de encontrar correlaciones y crear enlaces, pueden permitir determinar, analizar y predecir aspectos de la personalidad o el comportamiento de un individuo, sus intereses y comportamientos.

[373] Disponible en https://www.aepd.es/media/criterios/wp248rev01-es.pdf

Los datos personales tienen muchas aplicaciones comerciales, por ejemplo, se pueden utilizar para comercializar sus productos y servicios. La medicina, la educación, la atención médica y el transporte también pueden beneficiarse de estos procesos. Sin embargo, continua Art 29 WP, la elaboración de perfiles y la toma de decisiones automatizada pueden presentar riesgos significativos para las personas y las libertades que requieren garantías adecuadas. Estos procesos pueden ser opacos. Es posible que las personas no sepan que están siendo perfiladas o que no entiendan lo que está involucrado.Article 29 WP también considera que la elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. También se puede usar para especificar las preferencias y preferencias. Esto puede socavar su libertad de elegir, por ejemplo, ciertos productos o servicios como libros, música o noticias. En algunos casos, la elaboración de perfiles puede conducir a predicciones inexactas. En otros casos, puede conducir a la denegación de servicios y bienes y a una discriminación injustificada.

El RGPD, en definitiva, introduce nuevas disposiciones para abordar los problemas derivados de la elaboración de perfiles y la toma de decisiones automatizada, en particular, pero Art 29 WP considera, y yo coincido, en que estas disposiciones no son las más adecuadas para la privacidad.

3.2. La transferencia de datos.

El nuevo derecho a la portabilidad de los datos, que no tiene precedentes legales anteriores, tiene por objeto facultar a los interesados con respecto a

sus propios datos personales, ya que mejora su capacidad de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro[374].

El artículo 20 RGPD establece que:

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17[375]. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

[374] Article 29 Working Party, "Guidelines on the right to data portability". Disponible en su última versión en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

[375] El Derecho al Olvido

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

II

Sobre la redacción de este articulo, es importante mencionar el informe[376] de Article 29 Working Party.

El primer derecho que tiene el interesado es el de poder recibir y acceder los datos, que le incumban, que hayan sido tratados por el procesador de datos a partir de datos generados por el mismo interesado. El ejemplo más común aquí sería el de los datos sobre nosotros que recibimos por una app gracias a los datos personales que hemos cedido, como por ejemplo una aplicación de dar pasos, de salud, o sobre restaurantes o películas recomendadas.

El detalle que "incumban" al interesado no es baladí, pues en los datos generados por el interesado pueden "incumbir" a otras personas que también son titulares de derechos como son los datos de whatsupp, telegram, llamadas, etc y sobre los cuales, estos terceros, no han dado su consentimiento.

Conscientes de este problema, la citada guía de Art29 WP propone diferentes categorías de datos personales diferenciados entre ellos que estarán sujetos, o no, al nuevo derecho de portabilidad.

En primer lugar distingue entre los datos que da el usuario mediante un consentimiento activo, como puede ser su sexo o dónde vive. Unidos a estos datos se producen los datos que llama observados y que son aquellos que el

[376] Article 29 Working Party, "Guidelines on the right to data portability". Disponible en su última versión en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

usuario emite en su uso del dispositivo -como un móvil o el uso de un IOT- o del servicio que tiene contratado.

Frente a este tipo de datos, Art 29 WP distingue los datos inferidos o deducidos que son aquellos que son "creados" por el responsable de la base de datos en virtud de esos datos que son "facilitados" por el interesado como por ejemplo de los usos que hace un titular de una tajeta de crédito, se puede crear un perfil sobre esa persona; no solo financiero. Lo mismo podemos decir de las localizaciones y trayectos recogidos por aplicaciones famosas de conducción, por ejemplo.

Interesa destacar aquí que, el informe citado de Art. 29 WP considera que este tipo de datos, "no son datos facilitados por el usuario" y, "por lo tanto, no estarán dentro del alcance de este nuevo derecho".

En definitiva, para Art 29 WP, "la expresión «facilitados por» incluye los datos personales que guardan relación con la actividad del interesado o que se derivan de la observación del comportamiento de una persona, pero no los datos que resultan del análisis posterior de dicho comportamiento. Por el contrario, todos los datos personales que hayan sido creados por el responsable del tratamiento como parte del tratamiento de datos, p.ej. mediante un proceso de personalización o recomendación, mediante categorización del usuario o creación de perfiles, son datos que se deducen o infieren de los datos personales proporcionados por el interesado y no están cubiertos por el derecho a la portabilidad de los datos".

III

Ningún comentario -ni ninguna definición- hace sobre los datos que yo denomino como "higissianos[377]", y que Jose María Alonso Cebrián[378] denomina "semi" -aunque sin el mismo significado que yo les atribuyo-, que son aquellos datos personales proporcionados con el consentimiento del interesado o derivados de este consentimiento- que ya han sido tratados por

[377] El Bosón de Higgs, conocido periodísticamente como "la partícula de Dios" y que recibe su nombre gracias al Premio Nobel Peter Higgs es la partícula física elemental que es propiedad intrínseca de los cuerpos con masa. De la misma manera que el agua está hecha de moléculas de H_2O que no podemos ver, el campo de Higgs está formado por unas partículas de fuerza que llamaron "bosones de Higgs". El Bosón de Higgs es responsable de que las partículas tengan masa. Los datos higissianos serían, en esencia, datos personales cedidos voluntariamente pero que por tratamiento producen nuevas revelaciones sobre la persona, la personalidad o la identidad. Estos datos de Higgs serían los responsables de los Nuevos datos.

[378] Jose María Alonso Cebrían es el nombre del gran y ameno "Hacker"- como a él mismo le gusta autodenominarse- Chema Alonso, Ingeniero Informático y experto en ciberseguridad de gran renombre internacional, condecorado con diversas distinciones y que ha ocupado, entre otros, el puesto de Chief Data Officer en Telefónica. En la conferencia sobre Big Data celebrada en Barcelona el 7 de junio de 2019 en el Abad Oliba, definió como "datos semi" aquellos datos de una persona "que están por ahí" porque ya han sido tratados y forman parte de otra categoría de datos y que van o pueden ser tratados y que el "dueño"- en Telefónica el dueño es el emisor de los datos- no sabe ni que existen ni quién los tiene ahora, entre otras cosas. Se ha de suponer que los denomina "semi" en referencia a los datos informáticos "semistructurados" que es una categoría intermedia entre los datos estructurados y los que no lo están. Los datos estruturados serian aquellos ordenados y configurados de alguna manera en relación a sus atributos. Los que no están estructurados serían los datos en bruto. Hoy en día es muy difícil que los datos contenidos en una base de datos no estén estructurados de ninguna manera. Imaginemos un archivo de texto muy grande de 20.000 páginas, por ejemplo. En principio es un archivo no estructurado pues contiene palabras que no siguen ningún orden. Sin embargo, si le damos a buscar y ponemos, por ejemplo, la palabra "blanco", el programa es capaz de buscarla y mostrarla en el archivo. Este sería un ejemplo de archivo semisestructurado. La razón es porque la palabra "blanco" lleva incorporado un atributo –metadato- que permite incorporarla como tal. Esta categoría de dato semiestruturado viene a corresponder con los datos, definidos por Chema Alonso, como "semi". Entendemos que Chema es consciente de que tratando datos personales en Big Data no sería lo mismo exactamente que un dato desestructurado pues comenta la posibilidad de que se pueda identificar a una persona en concreto mediante técnicas. De ahí que entendemos que les denomine "semi" y no "semiestruturados" ya que les atribuye algo diferente aunque, como experto informático que es, lo que le salga es colocar un nombre al uso.
Es por eso que yo les denomino "higssianos" ya que nada tiene que ver con informática, matemáticas o psicología, sino con Derecho – aunque sea imposible separarlos en este caso-. El presupuesto conceptual de que parten es que son datos que no tienen que ser privados o personales, pero de los que se pueden obtener, por técnicas presentes o futuras, otros datos ya no solo identificativos sino relativos a los rasgos que definen la personalidad de un ser humano.

el titular de la base de datos, o por otro, y que pasan a formar parte de una nueva base de datos. Por ejemplo, si se recogen datos de las fechas en que alguien ha hecho uso de un servicio determinado, se puede inferir que ese individuo tiene cierto nivel económico o padece cierto problema de salud. Hasta aquí, de un dato voluntariamente cedido -si fuese el caso- podemos tratar una base de datos para inferir ciertos comportamientos. Comportamientos cuyo tratamiento será objeto y consecuencia de una propiedad intelectual del titular de la base de datos y del responsable.

Pues bien, estos datos que se han inferido, pasan a formar parte de otra base de datos, por poner un ejemplo sencillo, de personas con 4 hijos y con cierto nivel de renta, que puede ser utilizada para inferir directamente y sin ningún tipo de categorización o segmentación ciertos aspectos de la personalidad, identidad o identificación de la persona que emitió primigeniamente los datos; en definitiva, acaban revelando datos personales o confidenciales.

No se tienen que confundir los datos higssinos con los datos "latentes". Los datos latentes están ahí y permanecen ocultos hasta que alguien o algún motivo los descubren o los saca a la luz. Son datos que, en sí, no revelan ningún aspecto íntimo o configurador de la persona. En este aspecto, los datos latentes serían diferentes de los datos higssianos, aunque los dos podrían ser inferidos mediante análisis de datos semiestructurados.

No es menos cierto que aquí se plantean muchas dudas legales en el tratamiento del Big Data que no han sido ni planteadas. Ni a ciencia cierta podemos saber si son datos personales, si el emisor de datos es ya propietario de esos datos, que derechos le asisten al "emisor" de los datos o si hubo realmente consentimiento para ese tratamiento. Y eso por no decir que,

aunque los datos estén anonimizados -criterio necesario en principio para ceder a otros tus bases de datos-, con un nuevo tratamiento se pueden volver a "desanonimizar" indicando claramente a quién, o a qué familia o grupo individualizado de personas pertenecen esos datos, así como aspectos personalísimos y confidenciales. No sabemos tampoco si puede existir un Derecho al Olvido para esos datos nuevos generados ya que, a lo mejor no sabemos si existen. Los datos higgsianos sería un concepto dinámico.

Consideramos que quedan muchas lagunas por solventar y que una legislación generalista o no focalizada en unos principios muy claros -dictada así en aras de que no quiere quedarse desfasada enseguida por el desarrollo tecnológico, cabe entender- no puede resolver pero que claramente están lagunas afectan al individuo (queremos volver a resaltar en este punto que la clave está, como decíamos anteriormente, en los "principios"). Desde la configuración o inducción sobre aspectos de su personalidad, muy íntima a veces, que pueden chocar con la "autoderminación informativa"[379] hasta las potestades que se le conceden a las administraciones en virtud de un interés general que pocas veces éstas motivan correctamente y que puede llevar a intereses espúreos -aunque éste sea un debate ajeno a esta tesis-

Sorpende ver como, el citado informe de Art 29 WP, da simplemente unas recomendaciones sobre buenas prácticas y criterios poco claros sobre lo que el Big Data puede afectar a la persona, a parte de lo explicado justo en este punto: "la aplicación de herramientas que permitan a los interesados seleccionar los datos relevantes que desean recibir y transmitir y excluir,

[379] Sobre este aspecto, SCUDIERO, L. fundamenta que la portablidad de datos no es una herramienta efectiva para la autodeterminación informativa. Ver "Bringing Your Data Everywhere: A Legal Reading of the Right to Portability" Disponible en https://edpl.lexxion.eu/article/EDPL/2017/1/19.

cuando sea pertinente, los datos de otras personas, es una buena práctica para todos los responsables del tratamiento (tanto los «remitentes» como los «receptores»). Ello contribuiría en mayor medida a reducir los riesgos para los terceros cuyos datos personales puedan ser portados. Además, los responsables de los datos deberían poner en marcha mecanismos de consentimiento para otros interesados involucrados, a fin de facilitar la transmisión de los datos en aquellos casos en los que dichos interesados estén dispuestos a dar su consentimiento, p.ej. si también ellos desean trasladar sus datos a algún otro responsable del tratamiento. Dicha situación podría producirse, por ejemplo, en el caso de las redes sociales, pero es decisión de los responsables del tratamiento qué buena práctica seguir."

II

Y es que según la legislación europea, el responsable del tratamiento de los datos será el encagado de decidir sobre los datos personales recopilados. Así lo establece el art. 6.4 RGPD que dispone lo siguiente:

"(…), el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

4. El consentimiento de los menores de edad.

No se puede controlar la recopilación de datos que hacen los dispositivos IOT sobre los menores de edad. Además, el problema radica en que muchas veces no somos conscientes de la exposición a la que sometemos a los menores en relación a su personalidad y sus datos personales. Una huella que nunca será olvidada. Una huella que es propiedad de menores que han de ser objeto de especial protección[380].

La Convención de Derechos del Niño, de Naciones Unidas, de 20 de noviembre de 1989, establece en su art. 16 que "ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación".

[380] Véase por ejemplo la Declaración de Ginebra de 1924 sobre los Derechos del Niño; la Declaración de los Derechos del Niño de 1959 y el Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966.

Por su parte, el artículo 24 de la Carta Europea de los Derechos Fundamentales[381] establece en su artículo 24 que los niños tienen derecho a la protección y a los cuidados necesarios para su bienestar. Además, en todos los actos relativos a los niños llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del niño constituirá una consideración primordial.

4.1. El consentimiento de los menores sobre el tratamiento de sus datos en la legislación Europea.

4.1.1 La Unión Europea y el tratamiento de los datos del niño

I

La Unión Europea establece los derechos del niño como una de sus visiones estratégicas[382], para así proteger y promover por la propia Comisión y por todos los países miembros, esos derechos de los menores.

La Agenda de la Unión Europea para los Derechos del Niño[383] reconoce como uno de sus objetivos el logro de "un alto nivel de protección de los niños en el espacio digital, incluidos sus datos personales, al tiempo que defiende plenamente su derecho a acceder a Internet para beneficio de su desarrollo social y cultural".

A la vista de las comunicaciones emitidas por la Comisión Europea, ésta parece que sólo se centra en la exposición de los menores a Internet a través de webs, chats en línea, aplicaciones, juegos, etc -soslayando la exposición de menores a

[381] Disponible en https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003
[382]Entre otras, ver comunicación "'European Strategy for a Better Internet for Children" COM/2012/0196 final, 2 May0 2012; Comunicación "An EU Agenda for the Rights of the Child" COM/2011/0060 final, 15 Febrero 2011
[383] "An EU Agenda for the Rights of the Child", COM/2011/0060 final, 15 Febero 2011, 10.

dispositivos conectados a Internet- recordando que uno de cada tres usuarios es un niño[384] y que muchas veces están conectados sin la supervisión de un adulto.

La Comisión Europea entiende que, cuando los menores están conectados, pueden estar expuestos a contenidos y comportamientos nocivos como el acoso cibernético, el acoso sexual, la pornografía, la violencia o la autolesión. Se necesitan respuestas eficientes para evitar consecuencias negativas para su desarrollo cognitivo, social y emocional. Éste, sin duda, es una parte del problema muy importante, problemática y angustiosa para los padres pero no es todo el problema que se plantea.

Prueba de que la Comisión Europea no acaba de entender -o de poner en su justo valor- la problemática que afecta al menor en cuanto a la protección de su personalidad y de sus datos, son los objetivos que se han marcado en la estrategia para un mejor Internet para los menores[385], que se puede entender como una serie de acciones agrupadas en torno a los "siguientes objetivos principales:

- estimular la producción de contenido en línea creativo y educativo para niños, así como promover experiencias positivas en línea para niños pequeños;
- Ampliar la conciencia y el empoderamiento, incluida la enseñanza de la alfabetización digital y la seguridad en línea en todas las escuelas de la UE;

[384] https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids
[385] Se puede encontrar en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196%3AFIN

- Cree un entorno seguro para los niños a través de configuraciones de privacidad apropiadas para la edad, un uso más amplio de los controles parentales y la clasificación por edad y contenido;
- Combatir el material de abuso sexual infantil en línea y la explotación sexual infantil."[386]

Tal y como se comprueba, nada dice sobre la recopilación y tratamiento de los datos de los menores, ni expresa mención alguna al Internet de las Cosas donde se recopila, almacena y se trata información por parte de varios "stakeholders".

Viendo el papel adoptado por la Unión Europea, la legislación parece que no está muy madura en el tema del consentimiento, ni para adultos ni mucho menos para menores, ya que no tiene en cuenta el papel del Internet de las Cosas.

II

Así las cosas, el considerando 38 del RGPD razona que los niños merecen una protección específica de sus datos personales, ya que pueden ser 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, estableciendo la salvaguardia para casos de maltratos o abusos de que el consentimiento del titular de la

[386] https://ec.europa.eu/digital-single-market/en/european-strategy-deliver-better-internet-our-children

patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

De lo considerado anteriormente, el RGPD solo dedica dos incisos a un tema tan preocupante como puede ser el tema de los datos de menores.

El articulo 6. f) RGPD establece que:

"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. "

Y añade a continuación que "Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

Y el articulo 8, único dedicado enteramente al menor de edad, establece que:

1. Cuando se aplique el artículo 6, apartado 1, letra a)[387], en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

[387] Art 6.1.a) El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

La elección de la edad de 13 años no guarda ninguna explicación lógica, sino que ha sido tomada de la legislación de Esatdos Unidos[388] y con cierta idea de beneficiar a los negocios en línea[389] y de facilitar la interoperabilidad entre los mercados europeos y de Estados Unidos.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

III

Muchísimas dudas se plantean en relación a estos artículos.

En primer lugar si los intereses legítimos del responsable del tratamiento de datos, o de un tercero, tienen que pasar por encima de los derechos

[388] Ver Commission Staff Working Paper, Impact Assessment, SEC(2012) 72 final. Disponible en http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

[389] Ver Commité del Parlamento Europeo de Libertades Civiles, Justicia y Asuntos de Interior(LIBE), Amendments (1) 351 – 601, 2012/0011(COD), 4 Marzo 2013 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-504.340%2B01%2BDOC%2BPDF%2BV0%2F%2FEN>

fundamentales de un niño -que como hemos visto están recogidos en diversos tratados internacionales-.

En segundo lugar, el RGPD constituye una suerte de emancipación legal a los 16 años, atribuyendo como válido el consentimiento en contratos donde se comercia o están implícitos los datos del menor. Mediante una ley especial, modifica, entonces, la mayoría de edad y la capacidad para contratar sin atender a las legislaciones nacionales, por más que el RGPD establezca la clasula de salvaguarda, acabada de reproducir, del artículo 8.3 RGPD.

Hay un hecho y es que un menor de edad está consintiendo y perfeccionando un contrato, por más que el RGPD diga que no.

En tercer lugar, y para los menores de 16, el RGPD establece que habrá de existir el consentimiento de los padres o tutores pero "solo en la medida que se dio o autorizó". Confluyen aquí "intenciones" del mayor de edad imposibles de justificar legalmente, mezcladas con alcance del conocimiento.

En cuarto lugar, se deja al albur de los estados miembros el fijar una edad inferior a los 16 años, y nunca inferior a los 13.

En quinto lugar, el RGPD contiene conceptos jurídicos indeterminados como "esfuerzos razonables" del responsable de tratamiento y "tecnología disponible".

En sexto lugar, la Administración pública queda exenta, en el "ejercicio de sus funciones" de salvaguardar los derechos fundamentales del menor.

En séptimo lugar, nada dice el articulado sobre las capacidades del menor.

IV

No obstante, esos no son los únicos problemas que se presentan. De la lectura de la totalidad del artículo 6 y del artículo 9, sobre categorías especiales de datos, también se presentan ciertas dudas concernientes a la especial protección que deben tener los menores.

Parece desprenderse del artículo 6.1 un cierto "autocontrol" y "responsabilidad propia" de los menores en referencia a la cesión de sus datos en relación con el propósito de la cesión. Es lo que algunos autores han venido a llamar un control "ilusorio"[390].

Del mismo artículo 6.1 b, se deprende que los derechos específicos del responsable del tratamiento están por encima de los derechos del menor, al igual que cuando hay una obligación legal donde se deja al criterio, o al conocimiento, del responsable del tratamiento de datos si existe alguna norma legal que impida ese tratamiento, aunque sea para cumplir una obligación legal.

Igual responsabilidad se le da al responsable del tratamiento de datos a la hora de discernir cuáles son los "intereses vitales" de menor así como a la hora de discernir si el menor ha hecho "públicos sus datos" o si existe un "interés público vital", por citar alguna problemática también asociada.

[390] Véase, MACENATE, MILDA Y KOSTA, LENI que citan a otros autores"Consent for processing children's personal data in the EU: following in US footsteps?", Information & Communications Technology Law ,Volume 26, (2017) - Issue 2

4.1.2 La implementación del artículo 8 del RGPD en los Estados Miembros.

Tal y como hemos señalado anteriormente, el art. 8.1. RGPD establece que el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

A tenor de este artículo, divesos Estados Miembros se han lanzado a legislar sobre la edad de madurez del niño a la hora de considerar que hay un tratamiento lícito.

En Bélgica, la Ley de 30 de julio de 2018 sobre la protección de las personas físicas con respecto al procesamiento de datos personales se publicó en el Boletín oficial y entró en vigencia de inmediato el 5 de septiembre de 2018.

Los legisladores belgas han optado, de conformidad con el artículo 7 de la ley, por reducir los 16 años a los 13 años de edad. Si un niño es menor de 13 años, el procesamiento de sus datos personales solo será legal y válido si, y en la medida en que, el titular de la responsabilidad parental otorgue o autorice el consentimiento del niño. Por lo tanto, cada controlador de datos debe implementar un sistema adecuado que pueda verificar el consentimiento de los padres para niños menores de 13 años.

En Chipre, la Ley que regula el procesamiento de los datos de las personas naturales y la libertad de movimientos de dichos datos, la Ley 125(1) de 2018, recoge la madurez del niño para otorgar consentimiento a los 14 años en todos los casos.

En la República Checa, mediante ley publicada en su Boletín oficial el 24 de abril de 2019, se recoge la validez del consentimiento del menor a los 15 años en su artículo 7.

En Dinamarca, el consentimiento válido se otorga a los 13 años a tenor de la "regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act)".

En Finlandia, la ley 1050/2018 fija el consentimiento válido a los 13 años.

En Francia, la Ley 2018-493 de protección de datos personales, en virtud de su articulo 20, establece que el consentimiento será válido a los 15 años. A su vez, establece que si el niño es menor de 15 años, el consentimiento ha de ser mutuo junto con sus padres o tutores – aunque aún, a la hora de depositar esta Tesis, no se ha implementado la manera de hacerlo-.

De la misma manera, el artículo 59 de la ley citada establece que el niño mayor de 15 años puede impedir el acceso de sus datos médicos a sus progenitores o tutores en el curso de un estudio medico, una investigación o una evaluación

En Alemania, la Ley Federal de Protección de Datos cifra la edad de consentimiento en 16 años, al igual que en Italia (art. 2 de la ley Italiana de la Autoridad de Protección de Datos), o en Holanda en virtud del articulo 5 de la Ley de Implementación del RGPD (publicada en Boletin Oficial de 22 de mayo de 2018) o en Rumanía en virtud de su ley 190/2018 de protección de datos.

En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, fija en su artículo 7 la mayoría de edad en 14 años. Interesante es el artículo 84 de la ley donde se expone que los padres o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales, y añadiendo en su punto 2 que la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la legislación.

En Eslovenia, la ley ZVOP-2, sobre protección de datos personales, al igual que Francia, también fija la edad de consentimiento en 15 años.

En Suecia, el 14 de abril de 2018, se adoptó la Ley de protección de datos que sustiyuye a la anterior y en donde se fija la edad del consentimiento en los 13 años de edad.

De igual manera, en 13 años, está fijada la edad en el Reino Unido, a tenor de la sección novena de la Ley de protección de datos de 2018.

4.2. El consentimiento de los menores sobre el tratamiento de sus datos en Estados Unidos.

La Ley de protección de la privacidad en línea para niños (COPPA)[391] es una ley creada para proteger la privacidad de los niños menores de 13 años. La Ley fue aprobada por el Congreso de los Estados Unidos en 1998 y entró en vigor en abril de 2000. La Comisión Federal de Comercio (FTC) administra la COPPA.

La COPPA impone ciertos requisitos a los operadores de sitios web o servicios en línea dirigidos a niños menores de 13 años, y a los operadores de otros sitios web o servicios en línea que tienen conocimiento real de que están recopilando información personal en línea de un niño menor de 13 años[392], de conformidad con el apartado §312.2.

COPPA define el término de "operador" de manera amplia. Además de los sitios web estándar, según la FTC, los ejemplos de otros cubiertos por la COPPA incluyen[393]:

- aplicaciones móviles que envían o reciben información en línea (como juegos conectados a la red, aplicaciones de redes sociales o aplicaciones que ofrecen anuncios dirigidos por comportamiento).
- plataformas de juegos habilitadas para Internet.
- complementos.

[391] Se puede encontrar la versión final de la ley con sus enmiendas en https://www.ftc.gov/system/files/2012-31341.pdf
[392] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[393] https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

- redes publicitarias.
- servicios habilitados basados en la ubicación.
- servicios de protocolo de voz por Internet.
- juguetes conectados u otros dispositivos de Internet de las Cosas.

Se considera información personal de menor:

- Un nombre y apellido;

- Un domicilio u otra dirección física, incluido el nombre de la calle y el nombre de una ciudad o pueblo;

- Información de contacto en línea;

- Una pantalla o nombre de usuario que funciona de la misma manera que la información de contacto en línea, tal y como lo define la propia ley;

- Un número de teléfono;

- Un número de Seguro Social;

- Un identificador persistente que puede usarse para reconocer a un usuario a lo largo del tiempo y en diferentes sitios web o servicios en línea. Dicho identificador persistente incluye, entre otros, un número de cliente contenido en una cookie, una dirección de Protocolo de Internet (IP), un número de serie del procesador o dispositivo o un identificador de dispositivo único;

- Una fotografía, video o archivo de audio donde dicho archivo contiene la imagen o voz de un niño;

- Información de geolocalización suficiente para identificar el nombre de la calle y el nombre de una ciudad o pueblo; o

- Información sobre el niño o los padres de ese niño que el operador recopila en línea del niño y combina con un identificador.

Sigue añadiendo la COPPA que la divulgación de información personal significa compartir, vender, alquilar o transferir información personal a terceros.

Se instauran como obligaciones del operador de Internet

- Proporcionar un aviso en el sitio web o servicio en línea de la información que recopila de los niños, cómo utiliza dicha información y sus prácticas de divulgación para dicha información (§312.4 (b)).

- Obtener el consentimiento de los padres verificable antes de cualquier recopilación, uso y / o divulgación de información personal de niños (§312.5).

- Proporcionar un medio razonable para que un padre revise la información personal recopilada de un niño y se niegue a permitir su uso o mantenimiento adicional (§312.6).

- No condicionar la participación de un niño en un juego, la oferta de un premio u otra actividad en la que el niño divulgue más información personal de la que sea razonablemente necesaria para participar en dicha actividad (§312.7).

- Establecer y mantener procedimientos razonables para proteger la confidencialidad, seguridad e integridad de la información personal recopilada de los niños (§312.8).

En cuanto al consentimiento, se requiere, como requisito general, que un operador obtenga el consentimiento verificable de los padres antes de cualquier recopilación, uso o divulgación de información personal de los niños, incluido el consentimiento para cualquier cambio material en las prácticas de recopilación, uso o divulgación que los padres hayan consentido previamente.

Un operador debe dar al padre la opción de consentir la recopilación y el uso de la información personal del niño sin consentir la divulgación de su información personal a terceros.

En cuanto a los métodos para el consentimiento paterno verificable, se establece que:

(1) Un operador debe hacer esfuerzos razonables para obtener el consentimiento parental verificable, teniendo en cuenta la tecnología disponible. Cualquier método para obtener el consentimiento paterno verificable debe calcularse razonablemente, a la luz de la tecnología disponible, para garantizar que la persona que otorga el consentimiento sea el padre del niño.

Los métodos existentes para obtener el consentimiento de los padres verificables incluyen - de manera no tasada ya que se pueden instrumentalizar otros como los basados en nuevas tecnologías[394]- :

(i) Proporcionar un formulario de consentimiento para ser firmado por el padre y devuelto al operador por correo postal, fax o escaneo electrónico;

(ii) Requerir a un padre, en relación con una transacción monetaria, que use una tarjeta de crédito, tarjeta de débito u otro sistema de pago en línea que proporcione notificación de cada transacción discreta al titular de la cuenta principal;

(iii) Hacer que un padre llame a un número de teléfono gratuito con personal capacitado;

(iv) Hacer que un padre se conecte con personal capacitado a través de videoconferencia;

(v) Verificar la identidad de un padre al verificar una forma de identificación emitida por el gobierno contra las bases de datos de dicha información[395], donde el operador elimina la identificación del padre de sus registros inmediatamente después de que se complete dicha verificación; o

(vi) Si la información del menor no es de la categoría de divulgadas, tal y como lo define la ley en su apartado §312.2) se puede usar un correo electrónico junto con pasos adicionales para garantizar que la persona que otorga el consentimiento es el padre. Dichos pasos adicionales incluyen:

[394] La FTC propone por ejemplo los basados en tecnologia de reconocimieto facial. Véase https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance citado Ud Supra

[395] La FTC lo denomina knowledge-based challenge qüestions.

Enviar un correo electrónico de confirmación al padre después de recibir el consentimiento, u obtener una dirección postal o número de teléfono del padre y confirmar el consentimiento del padre por carta o llamada telefónica. Un operador que utiliza este método debe notificar que el padre puede revocar cualquier consentimiento otorgado en respuesta al correo electrónico anterior.

La Ley exige el consentimiento verificable de los padres antes de cualquier recopilación, uso o divulgación de información personal de un niño, *excepto*:

(1) Cuando el único propósito de recopilar el nombre o la información de contacto en línea del padre o hijo es notificar y obtener el consentimiento de los padres según §312.4 (c).

Según esta norma, si el operador no ha obtenido el consentimiento de los padres después de un tiempo razonable desde la fecha de la recopilación de información, el operador debe eliminar dicha información de sus registros.

(2) Cuando el propósito de recopilar la información de contacto en línea de un padre es proporcionar un aviso voluntario y, posteriormente, actualizar al padre sobre la participación del niño en un sitio web o servicio en línea que de otro modo no recopila, usa o divulga información personal de los niños. En tales casos, la información de contacto en línea de los padres no se puede usar ni divulgar para ningún otro propósito. En tales casos, el operador debe hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para garantizar que el padre reciba un aviso como se describe en §312.4 (c) (2);

(3) Cuando el único propósito de recopilar información de contacto en línea de un niño es responder directamente por única vez a una solicitud específica del niño, y cuando dicha información no se utiliza para volver a contactar al

niño o para cualquier otro propósito, no se divulga y el operador lo elimina de sus registros inmediatamente después de responder a la solicitud del niño;

(4) Cuando el propósito de recopilar la información de contacto en línea de un niño y de un padre es responder directamente más de una vez a la solicitud específica del niño, y cuando dicha información no se utiliza para ningún otro propósito, se divulga o se combina con cualquier otra información recopilada del niño. En tales casos, el operador debe hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para asegurarse de que el padre reciba la notificación como se describe en §312.4 (c) (3).

(5) Cuando el propósito de recopilar el nombre de un niño y de un padre y la información de contacto en línea, es proteger la seguridad de un niño, y donde dicha información no se usa o divulga para ningún propósito no relacionado con la seguridad del niño. En tales casos, el operador debe hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para notificar a los padres como se describe en §312.4 (c) (4);

(6) Cuando el propósito de recopilar el nombre de un niño y la información de contacto en línea es para:

(i) Proteger la seguridad o integridad de su sitio web o servicio en línea;

(ii) Tomar precauciones contra la responsabilidad;

(iii) Responder al proceso judicial; o

(iv) En la medida permitida por otras disposiciones de la ley, para proporcionar información a las agencias de aplicación de la ley o para una investigación sobre un asunto relacionado con la seguridad pública; y donde dicha información no se use para ningún otro propósito;

(7) Cuando un operador recopila un identificador persistente y ninguna otra información personal y dicho identificador se utiliza con el único propósito de proporcionar soporte para las operaciones internas del sitio web o servicio en línea. En tal caso, tampoco habrá obligación de notificar según §312.4; o

(8) Cuando un operador cubierto bajo el párrafo (2) de la definición de *sitio web o servicio en línea dirigido a niños* en §312.2 recolecta un identificador persistente y ninguna otra información personal de un usuario que interactúa afirmativamente con el operador y cuyo registro previo con ese operador indica que dicho usuario no es un niño. En tal caso, tampoco habrá obligación de notificar según §312.4.

La sección §312.6 establece los derechos de los padres de revisar la información proporcionada por sus hijos. Así la COPPA establece que:

A) A solicitud de un padre cuyo hijo ha proporcionado información personal a un sitio web o servicio en línea, el operador de ese sitio web o servicio en línea debe proporcionar a ese padre lo siguiente:

(1) Una descripción de los tipos específicos o categorías de información personal recopilada de los niños por el operador, como nombre, dirección, número de teléfono, dirección de correo electrónico, pasatiempos y actividades extracurriculares;

(2) La oportunidad en cualquier momento de negarse a permitir el uso posterior del operador o la futura recopilación en línea de información personal de ese niño, y de ordenar al operador que elimine la información personal del niño; y

(3) No obstante cualquier otra disposición de la ley, un medio de revisar cualquier información personal recopilada del niño. Los medios empleados por el operador para llevar a cabo esta disposición deben:

(i) Asegurarse de que el solicitante sea padre de ese niño, teniendo en cuenta la tecnología disponible; y

(ii) No ser excesivamente gravoso para el padre.

B) Ni un operador ni el agente del operador serán responsables bajo ninguna ley federal o estatal por cualquier divulgación realizada de buena fe y siguiendo procedimientos razonables para responder a una solicitud de divulgación de información personal bajo esta sección.

C) Sujeto a las limitaciones establecidas en §312.7, un operador puede rescindir cualquier servicio prestado a un niño cuyo padre se haya negado, en virtud del párrafo (a) (2) de esta sección- la §312.6- , a permitir que el operador use o recopile más datos personales, información de su hijo o que haya ordenado al operador que elimine la información personal del niño[396].

En definitiva, vemos como la COPPA es una ley muy avanzada que, interpretada de conformidad con el paso del tiempo, se revela mucho más útil, o como mínimo más de conformidad, con la realidad tecnológica, con el Big Data y con el uso del Internet de las Cosas, aunque fue lanzada para evitar el acoso comercial de los menores.[397]

[396] Sobre este aspecto, la FTC explica que "but only if the information at issue is reasonably necessary for the child's participation in that activity". Véase https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance citado Ud supra.
[397] Ver MACENAITE, MIDA Y KOSTA, ELENI. Íb. Supra.

Adolece, al igual que en la ley europea, de la necesidad de entender el consentimiento del menor de conformidad al uso indiscriminado de los algoritmos de captura de datos y su tratamiento. Adolece también de una cierta conexión con la realidad ya que, con el Internet de las Cosas, es de imposible cumplimiento y fía todo a la buena voluntad de las partes cuando claramete existe un "desequilibrio de poderes". Si no das acceso a tus datos, no puedes utilizar Internet de las Cosas, y lo que cedes no puede ser escogido por los padres o por los niños, sino que hay una obligatoriedad de ceñirse a lo que marca el sistema que se quiera usar.

CAPÍTULO V: CONCLUSIONES FINALES Y PROPUESTAS

PRIMERA: La tecnología está al alcance de todo el mundo. Y todo el mundo se mueve y se moverá gracias a la tecnología. La tecnología va muy por delante del Derecho. Con la irrupción del Big Data, gran parte de esta nueva tecnología trabaja con datos personales.

La protección de los datos personales se erige como un derecho distinto al derecho a la privacidad –aunque íntimamente ligado- y eso es indudablemente significativo, siendo este aspecto único para el ordenamiento jurídico europeo, al estar ausente de otros instrumentos internacionales de derechos humanos. La mayoría de ordenamientos internacionales tratan de configurar su legislación a partir de la legislación europea. Sin embargo, no se contempla por parte de la legislación internacional ninguna medida tendente a garantizar la auténtica "libertad no condicionada" por parte de los ciudadanos.

SEGUNDA: El Derecho al Olvido es un derecho que ha evolucionado hasta convertirse en un derecho autónomo y que trata de preservar el derecho fundamental a la privacidad de la persona. Sin embargo, la génesis del Derecho al Olvido no es la protección de los datos personales sino que su base conceptual se encuentra en los Derechos Humanos y la protección del libre desarrollo como persona del individuo, lo que le confiere unos matices y una singularidad diferentes a tal y como está planteado hoy en día.

Tal y como está concebido en las diferentes legislaciones, y dada la tecnología actual y la futura, el Derecho al Olvido tiene mucho más alcance del que se le supone hasta ahora dada su relación con el consentimiento en la

captación o uso de los datos. Las legislaciones y la jurisprudencia de los Tribunales tienden a tratar el Derecho al Olvido sobre un conjunto determinado de datos, de escaso tamaño, de fácil localización y siempre asociados a publicaciones en la web precisamente por esa concepción de simple derecho de protección de datos y por desconocimiento de las nuevas tecnologías. Sin embargo, no se relaciona con los Derechos Humanos, ya que aplica en ámbitos locales, ni con el Big Data, ni con la autodeterminación informativa y ni siquiera comprende tecnología que ya está en el mercado, como el Blockchain.

TERCERA: Se requiere un nuevo enfoque del consentimiento legal ya que con la llegada del Big Data y del Internet de las Cosas, la capacidad que existe para recoger, tratar, analizar, identificar y extraer valor nuevo e inesperado de datos viejos o datos aparentemente sin valor, son ilimitados. Los datos, además, pueden ser guardados eternamente de manera virtual y, el alcance de la información que pueden proporcionar esos datos al tratarlos, es ilimitado.

En definitiva, no existe el consentimiento efectivo dado de manera transparente.

CUARTA: No existe una definición legal de Big Data cuando claramente la recolección, recopilación y tratamiento de datos, sí la tienen. Si no hay consentimiento efectivo, o aún habiéndolo, se vulneran determinados derechos de la persona, debiera existir la posibilidad de ejercer un Derecho al Olvido de nuestros datos digitales.

Big Data, Derecho al Olvido y el consentimiento son, pues, tres piezas interrelacionadas y claves para el efectivo derecho a la libre configuración de

la personalidad, el respeto al derecho a la propia imagen, al derecho a la propia identidad y para la protección de los datos personales.

QUINTA: Sobre la falta de definición legal del Big Data, hay quien defiende que no es necesaria. De lo desarrollado en la presente Tesis podemos extraer que no todos los datos captados, almacenados y tratados pudieran formar parte de un posible concepto legal de Big Data ya que nunca tendrán efecto sobre la individualidad de las personas.

Las diferentes legislaciones que podrían ser aplicables en el caso del Big Data parten del error conceptual de que el Big Data solo tiene que ver con el tratamiento y fases siguientes. Sin embargo, la recopilación masiva de datos debiera ser parte también de la definición, y éste es un aspecto que se olvida.

Y esto es así porque la legislación potencialmente aplicable y que intenta proteger los datos personales parte, a mi entender de manera errónea, de que los datos sobre los cuales jurídicamente puede haber cierta controversia son datos puntuales e identificables. Nada más lejos de la realidad; el legislador parte de una concepción muy simplista que no tiene en cuenta el mundo de Internet donde los datos se captan por millones, se almacenan eternamente y donde se tratan miles de millones de datos por segundo. Todo ello sin que exista muchas veces el consentimiento del interesado.

Frente a la definición clásica de Big Data en donde se tienen que dar las 5 V- volumen, velocidad, variedad, veracidad y valor- habría que añadir, con tal de alcanzar una definición jurídica, y en el sentido en el cual se ha expuesto en la tesis, las 3 “I”: Identificables, Interrelacionados y que infieran sobre las personas.

En definitiva, el Big Data, en su concepción legal, debiera definirse como aquel proceso de recogida y tratamiento de datos humanos, o relacionados con sus acciones o actividades, que mediante cualquier procedimiento infiera o pueda inferir, por si mismo o mediante la agregación de otros datos o hechos o categorizaciones, en la esfera personal o en la personalidad o en la individualidad del sujeto así como en la posible identificación individualizada del sujeto emisor.

SEXTA: Si bien hay que reconocer beneficios en el uso del Big Data, se han analizado las posibles externalidades negativas que hay en su uso, ya sea por empresas privadas como de los Gobiernos. Ello es debido a razones, por ejemplo, de precisión, integridad, representatividad o sesgos en los datos.

De lege ferenda, los Gobiernos debieran, en aras de la democracia, la transparencia y el buen gobierno, exponer públicamente el algoritmo –para su escrutinio- que ha servido en cada caso para tomar decisiones políticas, sociales o sanitarias a partir del uso del Big Data.

SÉPTIMA: El derecho a la privacidad y el derecho a la propia imagen y a la identidad tienen que ser replanteados a la vista de las múltiples fuentes de recopilación de datos y de las diferentes formas de tratamiento e interrelación. Para ello hay que tener en cuenta los diferentes tipos de datos y la posibilidad de nueva agregación y análisis entre ellos.

La ley tiene que tener en cuenta los datos que, aunque no sean privados o confidenciales, por cualesquiera formas de tratamientos, puedan revelar la identidad de una persona o su identificación. La tesis propone la creación doctrinal de los datos higgsianos, que es un concepto dinámico. En todo caso

hay que tener en cuenta que llegar a un control total de los datos personales es una quimera y sería contraprudecente.

A su vez, el derecho a la privacidad, que se expande debido al impacto que tiene el Big Data, puede llegar a entrar en conflicto con otros derechos fundamentales de terceras personas y se tienen que establecer reglas claras para poder ponderar los derechos.

OCTAVA: El Derecho al Olvido no resuelve todo aquello que pretende el legislador. Hay que entender que esta situación se produce por la falta de encaje del Derecho ante la revolución de Internet. El legislador no viene entiendiendo la naturaleza poliédrica de Internet que poco tiene que ver con el mundo "offline".

Si de lo que se trata es de proteger los datos personales de los usuarios, ¿Cuál es la solución ideal para su concepción jurídica? ¿Por cuánto tiempo se tienen que guardar los datos personales? ¿Cuándo se consideran que ya no son relevantes? ¿Se tiene que crear una norma que se aplique automáticamente a todo el mundo?

Ya la Directiva 95/46 consideraba que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos.

Pues bien, la positivación jurídica debe ponderar todos estos derechos, y no tratar al Derecho al Olvido como únicamente una extensión de la cancelación de datos.

NOVENA: La ley otorga un protagonismo significativo a las Webs de Internet a la hora de conceptualizar el Derecho al Olvido. Ahora bien, debería tenerse en cuenta que el Derecho al Olvido también ha de operar con el Big Data y el Internet de las Cosas. Se tendrán que establecer ciertas presunciones legales a la hora de poder ejercitarlo frente a estas dos nuevas realidades. No se puede borrar el pasado, ni en el sentido de falsear la historia o de tener una segunda oportunidad en determinados aspectos, pero sí que deberá observarse si existe o puede existir un abuso por parte de las compañías que han recabado o tratados los datos personales o por parte de los Gobiernos en esa recolección o tratamiento, y deberán ponderarse los conflictos entre los Derechos de las personas y de las compañías o si realmente existe y se motiva un interés público en el caso de los Gobiernos. No existe una frontera nítida en este aspecto.

DÉCIMA: La tecnología puede mejorar la posición actual de recordar por defecto mediante la implementación de métodos de borrado o el reacondicionamiento de los datos, que se activan automáticamente, por factores que determinan si los datos deben borrarse. Esto cambiaría la posición actual a una nueva posición en donde se aplica el olvido o el reacondicionamiento por defecto ya que se considera más natural en tecnología y, por lo tanto, se ajusta más a nuestras expectativas sobre el olvido. El resultado sería que los sujetos de datos tendrían que confiar menos en el Derecho al Olvido para que se borren sus datos personales cuando sea necesario, sino que dependerán de la tecnología para hacer esto automáticamente.

Proporcionar a los interesados el derecho a que se borren sus propios datos es particularmente importante para la aplicación efectiva de los principios de

protección de datos que afectan a la personalidad, a la propia imagen, a la identificación y a la identidad y, en particular, el principio de minimización de datos (los datos personales deben limitarse a qué es necesario para los fines para los que se procesan esos datos) y a la autodeterminación informativa.

Para ello, propongo que sería conveniente una suerte de "ley de Faraday" donde se legislase que, transcurrido cierto tiempo, esos datos no pueden ser sometidos a tratamiento. Trascurrido ese periodo de tiempo, esos datos devendrían inmunes al tratamiento. Esto sería lo más deseable por diversas razones como por ejemplo la involuntariedad o el desconocimiento de que hemos cedido esos datos, o en el caso de los datos cedidos por menores de edad, o por muchas otras razones como evitar en cierta manera la discriminación. El borrado de datos debiera estalecerse por diseño.

DECIMOPRIMERA: El Derecho al Olvido se configura de una manera en donde los Estados siguen siendo el actor principal a la hora de poder ejercerlo y aplicarlo; la planta judicial de los Estados es la que vertebra la aplicación de este derecho. Los Estados no pueden, en reglas generales, actuar en el tema del Derecho al Olvido más allá de sus fronteras.

Sin embargo, la problemática del Derecho al Olvido traspasa las fronteras soberanas de los Estados.

El punto de partida en el olvido digital, se da a partir de la legislación vigente. Pero el desarrollo tecnológico es tan rápido y discurre por unos caminos tan complicados que es imposible abordar el asunto desde la perspectiva de una única legislación nacional, pues el mundo "virtual" no entiende de fronteras.

Las medidas de aplicación del Derecho al Olvido, debieran traspasar fronteras. Eso sería lo lógico, si consideramos que se pueden infringir Derechos Fundamentales. Las personas, por el mero hecho de existir tienen una dignidad y unos derechos que le son inalienables; esa es la concepción de las sociedades democráticas. No puede ser que esos derechos se restrinjan a determinados espacios territoriales -como parece hasta ahora fundamentar la Jurisprudencia en estos casos- aunque hay que ser conscientes de la problemática, por imposible, que encierra la llamada "gobernanza única" de Internet.

DECIMOSEGUNDA: Los diferentes convenios y tratados internacionales con rango de ley recogen recojen el concepto de "cooperación internacional" en el campo de la protección de datos.

A pesar de la complejidad de la "gobernanza" de Internet, la legislación internacional debiera garantizar esta cooperación internacional, adoptando medidas para hacerla cumplir y en concreto:

a) Garantizar que los derechos e intereses de las partes son respetados sin importar el lugar del mundo donde se pueda producir la vulneración.

b) Tomar las medidas correctivas necesarias, con eficacia "erga onmes" y de una manera rápida y efectiva.

Hay que concluir que, con la mentalidad actual sobre Internet, centrada únicamente en el universo web, se perjudica a todas las partes.

DECIMOTERCERA: A la hora de abordar el tratamiento de los datos, la legislación actual no aborda la problemática del factor multiplicador exponencial y expansivo de las bases de datos. La legislación debe garantizar

que el "olvido" de los datos se produce en cascada y no solo en la fuente primigenia. La legislación sobre flujo de datos debe contemplar también esta contingencia y no sólo establecer con que terceras partes se puede realizar la transferencia de datos.

DECIMOCUARTA: El marco legal del Derecho al Olvido debe garantizar, en la medida de lo posible, el ejercicio de la autodeterminación informativa y no plantearlo sólo como un remedio de última instancia cuando se ha vulnerado un Derecho de la persona. Para ello debe concebirse un Derecho al Olvido íntimamente ligado al Big Data y al Internet de las Cosas. Cuando se recopilan datos se deben establecer ciertas garantías tecnológicas de que los datos serán olvidados y no tratados o asociados a otras bases. Esto va mucho más allá del derecho de cancelación, oposición o rectificación. La legislación tiende a obviar que con la tecnología actual los datos son tratados o reduplicados, en muchos casos, en el preciso instante en que son recopilados o captados, cosa que hace imposible el olvido digital. Frente al olvido de los datos, lo que se ha impuesto es el recuerdo.

Un marco legal completo también beneficiaría a las tecnologías de blockchain, pues a la vez que garantizaría el borrado de datos, también garantizaría en que casos no se pueden borrar o hacerlos simplemente inaccesibles o estableciendo que datos se pueden olvidar o cuáles no y la manera de hacerlo para que así, la cadena del blockchain siguiese siendo totamente confiable. Esto es realmente importante en los blockchains públicos

DECIMOQUINTA: Con la irrupción de Internet, el concepto de personalidad -entendido como aquel derecho a ser uno mismo y expresarlo ante los demás- escapa al control de la propia persona y desborda el sentido atribuido legalmente

a este concepto. Identidad y personalidad son dos conceptos que se unen íntimamente y con una frontera borrosa en Internet y que configuran, a su vez, dos tipos de personalidad: La pública y la privada.

La personalidad ya no es una externalización que deviene de los actos de la persona sino que puede venir configurada por actos de terceros que la afecten.

Dentro del actual marco legislativo internacional, sería conveniente una evolución del concepto de personalidad en la medida que la "personalidad virtual" va a preponderar sobre la "personalidad real" y es la propia personalidad la que configura la identidad de las personas, que es un bien jurídico a proteger categorizado como Derecho Fundamental y que condiciona la vida misma de la persona.

La privacidad en concepto clásico se relaciona siempre con la persona. Pues bien, la nueva privacidad tiene que ser entendida no solo con la persona, sino también con la personalidad, concepto éste íntimamente unido al concepto de persona – y de su dignidad por tanto- pues manifiesta el modo de vivir, pensar o actuar.

DECIMOSEXTA: La personalidad virtual puede conllevar interacciones con los derechos de los cuales una persona es titular. En relación al Big Data, la recolección y tratamiento masivo de datos, su incorporación a bases de datos, su cesión a terceros y el cambio de finalidades pueden hacer que una persona sea categorizada en un estrato de personalidad en la cual no se ve, no se siente o no quiere verse representado y que puede condicionar cambios, aunque sea de manera inconsciente, en la manifestación de su personalidad.

La legislación y la jurisprudencia no tratan los datos generados y su tratamiento como un concepto de identidad. La identidad propia, es parte esencial del libre

desarrollo de la personalidad y de la dignidad humana. La recolección y el tratamiento de datos pueden dar lugar a que esa intromisión devenga ilegítima ya sea porque muestre, descubra o manifieste aspectos que sean configuradores de la esencia de la personalidad y que identifiquen o muestren la identidad de la persona de manera no autorizada o consentida por la persona.

DECIMOCTAVA: El consentimiento siempre ha estado en el centro de cualquier contrato de cesión de bienes entre personas. En primer lugar, una persona acepta que otra persona puede usar sus bienes. Luego llegan a un acuerdo sobre lo que la otra parte puede hacer con sus bienes.

En Internet, el consentimiento es mucho más complejo.

Debido a que los datos son tan valiosos, algunas compañías solicitan más datos de los que necesitan. Quieren mantenerlos "por si acaso". Después de todo, eliminar datos cuesta más que conservarlos .También comparten con terceros los datos que tienen. Los datos se han convertido en una clase de activos y esto ha generado incertidumbre y, ocasionalmente, malas prácticas.

Por lo tanto, el problema de privacidad de datos no surge de las empresas que solicitan datos en sí. Surge de los abusos de este proceso y por la adhesión obligatoria a determinados contratos si queremos utilizar determinados servicios, aparatos o aplicaciones. El marco legal existente no parece el adecuado para que podamos hablar de un consentimiento en su concepción clásica y mucho menos cuando hablamos de la manifestación de los poderes exorbitantes que tiene la Administración en relación a la recolección y tratamiento de datos.

La categorización legal del consentimiento como manifestación de una voluntad libre, específica, informada e inequívoca debiera ser expresa en

determinados datos personales y privados que afectan a la íntima personalidad del sujeto, su identidad y su identificación.

Por ejemplo, el actual marco legal europeo exige un "consentimiento reforzado" en determinados tipos de datos. Es decir, no exige que sea expreso aunque sí inequívoco; esto no es lo mismo.

El marco legal debiera contemplar la posibilidad de que de los datos que no estén estructurados y no sean datos privados o de "categoría especial", puedieran obtenerse datos que sí que se incardinarían dentro de esta categoría mostrándonos ya sea la personalidad, la identidad, la identificación o que puedan incidir en el derecho a la propia imagen por cualquier procedimiento.

DECIMONOVENA: Se produce un claro desequilibrio de poder en un marco legal donde el consentimiento se presume válido para poder proceder al tratamiento de los datos cuando se trata de una misión realizada en aras de un difuso interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

De igual modo no debiera permitirse la autorregulación del responsable del tratamiento en el sentido que el consentimiento se considera válido cuando sea 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.

La experiencia demuestra que ambas ficciones legales pueden ser sobrepasadas casi sin control y no protegen de manera cierta el bien jurídico que se pretende proteger.

VIGÉSIMA: Al hilo de la conclusión anterior, los hechos demuestran que el legislador internacional, y en este caso el europeo, no ha conjugado una justa ponderación entre el consentimiento personal y los exhorbitantes poderes que se le dan a las Administraciones para el tratamiento de determinados datos personales como los relativos a salud. Aunque sea un hecho posterior al depósito de la presente Tesis, la pandemia del COVID 19S, SARS-COV-2, ha puesto en entredicho la legislación europea sobre protección de datos y, en concreto, este aspecto. Se plantean serias dudas legales sobre la utilización de los datos personales, no solo los sanitarios sino los de geolocalización, que pueden recabar y tratar las Administraciones Públicas debido a su intrusión por la forma de obtenerlos, la posible falta de consentimiento, la posible falta de control democrático de los parlamentos nacionales debido a los estados de alarma instaurados y el desconocimiento de las aplicaciones o métodos por los cuales se obtienen.

A todo lo anterior se desconoce cómo se tratarán esos datos, cómo se almacenarán y durante cuanto tiempo, así como las posibles finalidades futuras (o leyes en las que se autorice el uso distinto de esos datos) que se les pueden dar a esos datos que pueden "trascender" de esa motivación de salud o interés público inicial.

La legislación al respecto debería acotar todo lo expuesto en esta conclusión ya que el hecho de su mera discusión pública, indica que la legislación -en este caso la europea- no es nada clara y puede vulnerar los propios principios que el RGPD dice proteger.

VIGÉSIMOPRIMERA: Los diferentes marcos legislativos muestran lagunas en cuanto a la aplicación del consentimiento. Legalmente no puede haber

consentimiento alguno cuando, del uso de un servicio, aparato, aplicación o Internet de las Cosas, se recogen datos personales de terceros que nada tienen que ver con quien ha contratado el servicio o es el propietario del aparato que está recopilando datos. Se produce con muchas frecuencia que esa recolección de datos se hace de manera inadvertida y no consentida. El marco legal debe prever la manera de que el usuario del Internet de las Cosas tenga un control efectivo sobre los datos que cede y sobre el consentimiento que otorga sobre ellos, sin entorpecer el normal funcionamiento del aparato pero garantizando también los derechos de terceros no relacionados. En este sentido expresar que la legislación debe evolucionar para garantizar el consentimiento en los datos que se usan por parte del responsable del tratamiento y no tanto el consentimiento de los datos que se recopilan ya que es imposible, y lo será más en el futuro, prestar consentimiento en todos los datos que se ceden; el bien jurídico a proteger es el consentimiento en el uso pero no en la cesión, aunque ello no implica que no deba existir una legislación clara en cuanto al consentimiento en la recopilación de datos sensibles.

El marco legislativo del consentimiento debiera prever lo que constituye un "uso" de datos personales y qué usos deberían permitirse o prohibirse, y según que estándares debería hacerse la determinación del consentimiento.

VIGÉSIMOSEGUNDA: El interés superior del menor es una cuestión de orden público y, aunque sea un concepto jurídico indeterminado, es categorizado como un derecho fundamental del niño y no puede quedar en un plano asbtracto. Las soluciones que se den al consentimiento del niño en la cesión de sus datos deben tener en cuenta el propio concepto de interés superior del menor. Con sus propias especialidades, decimos lo mismo del consentimiento dado por el incapacitado.

VIGÉSIMOTERCERA : Existe falta de coherencia en el marco legal de los diferentes paises en relación al consentimiento del niño. Por un lado, se observa que las diferentes legislaciones tienen en cuenta, a la hora de establecer los principios que han de guiar la legislación, el evitar los posibles perjuicios a los que se puede ver expuesto el menor en el uso de Internet. Pero a la hora de positivizar este Derecho, por diversas razones, "degradan" la mayoría de edad para consentir en Internet, no coincidiendo ésta con la edad legal establecida en general para consentir sobre la disposición de sus bienes, que coincide con la mayoría de edad legal establecida en cada Estado.

Además, en el ámbito de la Unión Europea, nos encontramos conque cada Estado puede establecer el consentimiento en Internet en una edad diferente a partir de los 13 años. Parece incoherente que el consentimiento, que tendría que estar armonizado, pueda variar en cada Estado miembro de la Unión llegándose a la paradoja que el menor, en un mundo donde los viajes entre Estados son frecuentes, puede haber consentido legalmente la cesión de sus datos en un Estado que no es el suyo pero que a su vez es un consentimiento no legal en su Estado de origen.

La legislación de Estados Unidos, aunque pueda parecer más avanzada, ha quedado obsoleta en cuanto a los objetivos que pretendía.

Sería deseable, en interés del menor, una legislación mundial a través de Tratado que clarificase el consentimiento del menor y sobre que datos en especial este consentimiento debiera ser reforzado y tutelado ya que la "huella digital" de un menor debiera ser ínfima, por no decir nula, con tal de permitir el libre desarrollo de su personalidad y la protección de su imagen.

BIBLIOGRAFÍA

ARTICLE 29 WORKING PARTY; "Opinión 2/2017 sobre el tratamiento de datos en el Trabajo". (2017).

ARTICLE 29 WORKING PARTY; "Opinion 3/2013 on purpose limitation". (2013).

ARTICLE 29 WORKING PARTY; "Guidelines on the right to data portability". (2017).

ARTICLE 29, WORKING PARTY; "Opinion 1/2008 on data protection issues related to search engines". (2008).

ARTICLE 29 WORKING PARTY; "Opinion 08/2012 providing further input on the data protection reform discussions". (2012).

ARTICLE 29 WORKING PARTY; "Opinion 03/2013 on purpose limitation". (2013).

ARTICLE 29 WORKING PARTY; "Opinion 06/2014 on the notion of legitimate interests". (2014).

ARTICLE 29 WORKING PARTY; "Guidelines on consent under Regulation 2016/679". (2017).

ARTICLE 29 WORKING PARTY; "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data".(2009).

ARTICLE 29 WORKING PARTY; “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679”. (2017).

ARTICLE 29 WORKING PARTY; “Opinion 08/2012 providing further input on the data protection reform DISCUSSIONS.protection reform discussions”. (2012).

ARTICLE 29 WORKING PARTY; “Overviwe of results of Public consultation on opinion on legitimate interest of the data controller under Article 7 of Directive 95/46/EC”. (2014).

ARTICLE 29 WORKING PARTY; “Opinion 15/2011 on the definition of consent”. (2011).

ASIM ZIA ET AL., “The Prospects and Limits of Algorithms in Simulating CreativeDecision Making”, 14 EMERGENCE 89, 97 (discussing the limits of algorithms in interpreting affordances). (2012).

AZURMENDI, Ana “Por un «Derecho al Olvido» para los europeos: aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014”. UNED. Revista de Derecho Político N.º 92, págs. 273-310. (2015).

BARBERÁN, Pascual: “aspectos jurídicos de las aplicaciones móviles (apps)”. Acta. (2016).

BARDES, GEORGE F. “Problems of profesional secrecy”. Boston College. Big Data, (2015).

BENNET, COLLIN J. “Distintos intentos por camuflar las ineptitudes de la protección de la privacidad estadounidense”. Revista Telos número 97. Telefónica. (2018).

BEYER,M “Gartner says solving ‘Big Data’ Challenge Involves More Than Just Managing Volumes of Data. Gartner. (2011)

BOIX PALOP, A., «El equilibrio entre los derechos del artículo 18 de la Constitución, el “Derecho al Olvido” y las libertades informativas tras la sentencia Google», Revista General de Derecho Administrativo, 38. (2015).

BOTANA A. G. Y OVEJERO A.M . “Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de Mayo de 2014 en la cuestión prejudicial planteada en el caso Google.”. (2014).

BYUNGKWON LIM, GARY MURPHY, FRIEDRICH POPP AND JAMES AMLER. “A Glimpse Into The Potential Future Of AI Regulation” https://www.debevoise.com. (2019)

CANNATACI JA AND MIFSUD-BONNICI JP, “Data protection comes of age: The data protection clauses in the European Constitutional Treaty.” Information & Communications Technology Law 14(1): 5–15. (2007).

CANNON, Alex W. “Regulating Adwords: Consumer protection in a Market where the Commodity is Speech.” SETTON HALL L. REVIEW.291,296. (2009).

CARNELUTTI, F.“ Teoría General de la Ley”. (1955).

CASAS BAAMONDE M.E; “El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional” Conferencia en XXI Congreso Nacional de Derecho Sanitario. (2014)

COHEN, JULIE E , “Configuring the Networked Self: Law, Code, and the Play of Everyday Practice” .Yale University Press. (2012).

COMISIÓN EUROPEA “An EU Agenda for the Rights of the Child”. (2011)

CONSEJO DE EUROPA. “Explanatory report to Convention 108”. (1981)

CORRAL TALCIANI, H.. “Configuración jurídica del derecho a la privacidad II: Concepto y delimitación”. Revista Chilena de Derecho, vol. 27 núm. 2, págs. 331-355. (2000).

CUERVO ALVAREZ, J. Blog de informàtica Jurídica

COHEN, “What Privacy Is For”, 106 Harv. L. Rev 1904, p.1920-21 (2013)

DE ANDRADE, N “Oblivion: The right to be different … from oneself. Reproposing the right to be forgotten”. Revista de los Estudios de Derecho y Ciencia Política de la UOC 13: pág 122–137. (2012)

DE HERT Y GUTWIRTH, “Reinventing Data Protection?”. Springer Sciences BV. (2009).

DE LA QUADRA SALCEDO Y PIÑAR MAÑAS. “ Sociedad digital y Derecho”. Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado. Madrid. (2018).

DE VERDA, J. R. . “Breves reflexiones sobre el llamado Derecho al Olvido”. Revista Actualidad Jurídica Iberoamericana. (2014).

DEVINS C, FELIN T., KAUFFMAN S, KOPPL R; "The Law and Big Data," Cornell Journal of Law and Public Policy: Vol. 27 : Iss. 2 , Article 3. (2017)

DUBIÉ, P. «Protección de datos y Derecho al Olvido», Derecho de los negocios, Año nº 14, Nº 154-155, págs. 1-16 empirical data in the law. (2004)

DURLAUF, STEVEN N AND BLUME, LAWRENCE E. Palgrave Macmillan, 2008. "The New Palgrave Dictionary of Economics Online". Palgrave Macmillan. 29 de marzo. (2011).

ENISA. European Union Agency For Network and information Security. "Privacy by design". (2015).

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". (2015).

EUROPEAN COMMISSION. "Handbook on European Data Protection Law". (2018).

EUROPEAN DATA PROTECTION SUPERVISOR, "Meeting the challenges of Big Data". (2015)

EUROPEAN DATA PROTECTION SUPERVISOR.,"In Good Health?" pág. 331-346. (2012)

EUROPEAN PARLIAMENT "The data protection regime in China in-depth analysis". Parlamento Europeo. (2016).

FEDERAL TRADE COMMISSION. "Big Data: A tool for inclusion or exclusion? Uderstanding the issues". (2016)

FREIRE E ALMEIDA. D “Um Tribunal Internacional para a Internet” . Ed Amazon. (2015).

FEILER, L., “The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, în European Journal Of Law And Technology” vol. 1, nr. 3. (2010).

FERRANDO VILLALBA, Mª L. La información de las Entidades de Crédito. Estudio especial de los informes comerciales bancarios” Valencia,Ed. Tirant lo Blanch. (2000).

FEUER, ALAN The Geek Squad de la Alcaldía, NY TIMES, 23 de marzo. (2013)

FRIEDEWALD, M; POHORYLES, RJ, “Technology and Privacy and Innovation” The European Journal of Social Science Research, vol. 26, nr. 1-2. (2013).

GARRIGA DOMÍNGUEZ, A. “Tratamiento de datos personales y derechos fundamentales “ Ed. Dykinson. Madrid. (2004)

GARRIGA DOMINGUEZ, A. “Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua”. Ed. Dikynson. (2016)

GONZALEZ FUSTER, G.“ “¿Un debate cada vez más fundamental o cada vez menos?”. Revista Telos. número 97. Telefónica. (2018)

GONZÁLEZ MURÚA, “Comentarios a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al art. 18.4 de la Constitución y la protección de

datos personales", Revista Vasca de Administración Pública, núm. 37. (1993).

GOODRICH P., "Rhetoric and Modern Law". The Oxford handbook of english law and literature. (2014).

GOODWIN LIU, Educación, Igualdad y Ciudadanía Nacional, 116 YALE LJ 330, 334. (2006).

GREEN J, Facebook Knows You're Gay Before You Do, Am. Blog http://americablog.com/2013/03/ facebook-might-know-youre-gay-before-you-do.html. (2013).

GREENGARD S.,"Internet of things".MIT Press Essential Knowledge serie. Versión Kindle. (2015)

HANMING F; "Externality Versus Public Goods". Duke University (2014)

HART, HLA "Are there any natural rights?" The Philosophical Review 64(2): pag 175–191. (1955)

HAYNES STUART A, "Google search resuts:Buried if not forgotten". North Carolina Journal of Law and Technology. Volume 15. (2013).

HILDEBRANDT, M "Profiling and the Rule of Law". (2009)

HUSTINGS, P "Restaurar la confianza al otro lado del Atlántico". Revista Telos número 97. Telefónica. (2018)

HUSTINX P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation". Comisión Europea. (2014)

IBM. “The Four V’s of Big Data¨. (2014) .

KELSEN, H “ Teoría pura de la ley”. (1934)

KELLER,D , “Intermediaries and free expression under the gdpr”, Standford University;comunicaciones de Center for Internet and Society at Stanford Law Schooll; Internet Society. (2015)

KHERA, K “Case commentary: right to be forgotten”en Jamia Law Jornal. (2018).

LAFFONT, J.J., “Externalities In: The New Palgrave” Dictionary of Economics. Second Edition. (2008).

LANCASTER, A., ”My Scale Just Told the Cloud I’m Fat: AccessManagement, Security, Privacy and IOT.” en Wiki AllSeen Alliance, Gateway Agent Project. (2015).

LANEY DOUG, “3D Data Management: Controlling Data Volume, Velocity and Variety” (Metra Group Research Note). (2001).

LATONERO, M.. “Big Data Analytics and Human Rights. In M. Land & J. Aronson (Eds.), New Technologies for Human Rights Law and Practice (pp. 149-161).Cambridge:Cambridge University Press. (2018).

LATONERO, M que cita a ARONSON J, “Mobile Phones, Social Media, and Big Data in Human Rights Fact-Finding: Possibilities, Challenges, and Limitations,” in P. Alston and S. Knuckey (eds.), The Transformation of Human Rights Fact-Finding .Oxford: Oxford University Press. (2015).

LASSALLE, J.M “Ciberleviatán el colapso de la democracia liberal frente a la revolución digital” Editorial Marcial Pons. (2019).

LERMAN, J. “Big Data and its exclusions”. Standford. law. rev. online 55. (2013).

M. BALKIN, J “Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation” UCDAVIS Law Review. (2018).

MACENATE, M Y KOSTA, L “Consent for processing children’s personal data in the EU: following in US footsteps?”. Information & Communications Technology Law. (2017).

MANRIQUE, T, “elucubraciones acerca del derecho fundamental al olvido en el Perú y en el derecho comparado, a propósito de su reconocimiento y evolución” California Silicon Valley School of the Law. (2017).

MCDERMOTT Y , “Conceptualising the right to data protection in an era of Big Data”. Big Data & Society January-June. (2017).

MICHAL KOSINSKI ET AL., Private Traits and Attributes Are Predictable From Digital Records of Human Behavior, 110 Proceedings of the Nat’l Acad. of Scis. 5802, 5803–04. (2013).

MURILLO DE LA CUEVA, L “Informática y protección de datos personales”.Madrid. Centro de estudiós Políticos y Constitucionales. (1993).

MURILLO DE LA CUEVA, L. “El derecho a la autodeterminación informativa y la protección de datos personales” Ed BIBLID. (2008).

NEBRERA GONZÁLEZ, M "¿El fin del Estado?", en C ESPALIU (ed.), El Estado en la encrucijada, retos y desafíos de la sociedad internacional del siglo CXXI, Thomson Reuters ARANZADI. (2016).

NEBRERA GONZÁLEZ, MONTSERRAT "El conflicto entre tribunales en el Espacio Europeo como oportunidad para una nueva Constitución", en BERNAT-N TIFFON (coord.), Actas de las Jornadas Ps icológico-Criminológicas, Mc Graw Hill- ESERP, Barcelona. (2018).

NEBRERA GONZÁLEZ, M"Libertad y seguridad en Estados regionalmente integrados", en V. MOLINARES y J.LL. PÉREZ-FRANCESCH (compil.), Seguridad humana y derechos fundamentales, UN Editorial, Barranquilla. (2019).

NURALLEV, R."Right to Be Forgotten in the European Union and Russia" National Research University Higher School of Economics de Moscú. (2018).

ORREGO, C.A. "Una aproximación al contenido constitucional del derecho de autodeterminación informativa en el ordenamiento jurídico peruano" Anuario de Derecho Constitucional Latino-Americano año XIX. Bogotá. (2013).

ORZA LINARES, RM, y RUIZ TARRÍAS, S ."Neutralidad de la red y otros retos para el futuro de Internet".Conference. Huygens Editorial. Páginas 371 a 378." "El Derecho al Olvido en Internet". (2011)

OWEN Fiss, M. "Grupos y la cláusula de igual protección", 5 PHIL. & PUB. AFF. 107, 147-56 (1976).

PACE, A. "El derecho a la propia imagen en la sociedad de los mass media" Revista Española de Derecho Constitucional, núm. 52, pags. 33-52. (1998).

PAGALLO, U. Y DURANTE,M. "The Pros and Cons of Legal Automation and its Governance" 7(2) European Journal of Risk Regulation 323-334. (2016).

PAGALLO, U "Cracking down on Autonomy: Three Challenges to Design in IT Law'"14(4) Ethics and Information Technology 319-328. (2014).

PAGALLO U, "Designing Data Protection Safeguards Ethically"2(2) Information 247-265. (2011).

PAGALLO,U. "On the Principle of Privacy by Design and its Limits: Technology, Ethics, and the Rule of Law" en: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) European Data Protection: In Good Health?. Springer, Dordrecht. (2012).

PARLAMENTO EUROPEO. "The data protection regime in China IN-DEPTH ANALYSIS". Bruselas. (2018).

PÉREZ LUÑO, A. E.: "Los derechos humanos en la sociedad tecnológica" Ed. Universitas. (2012).

PÉREZ LUÑO, A. E.: "Derechos humanos, Estado de Derecho y Constitución". Editorial Tecnos. 10 edición. (2019).

PIÑAR MAÑAS, JL Y OTROS, "Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad" Ed. Reus. (2016).

POZEN D., "The Mosaic Theory, National Security, and the Freedom of Information Act" (Note) 115 Yale Law Journal 628–79. (2005).

PROSSER, WILLYAM L. "Privacy", Californian Law Review. (1960).

QUENTIN H., "Rethinking Privacy in an Era of Big Data, N.Y. TIMES, June 4. (2012).

QUINTANA ADRIANO, E. "The Natural Person, Legal Entity or Juridical Person and Juridical Personality". Penn State Journal of Law & International Affairs. Volume 4. (2015).

RALLO LOMBARTE, A y MARTÍNEZ MARTÍNEZ, R (coord..): "Derecho y redes sociales". Thomson Reuters. (2010).

REINDERG JOEL R, "Resolving Conflicting International Data Privacy Rules in Cyberspace", Stanford Law review 52. (2000).

ROUVROY, A AND POULLET, Y. "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy" en : Reinventing Data Protection? Dordrecht, Netherlands: Springer, pp. 45–76. (2009).

RUTENBERG, J, "Datos en los que puede creer", NY TIMES, 23 de junio. (2013).

SACKS, S. "China's Emerging Data Privacy System and GDPR". Centre for strategic and international studies. (2018).

SALDAÑA, M.N. "The right to privacy. la génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de warren y brandeis". UNED. Revista de Derecho Político. (2012).

SANDRA B. HALE, t"he discourse of court interpreting:discourse practices of the law, the witness and the interpreter", 4–8, 31–32. (2004).

SCHMIDT E. Y COHEN J. "El futuro Digital" Ediciones Anaya, Madrid. (2014).

SCHMIDT-ASSMANN, E. "La Teoría General del Derecho administrativo como sistema objeto y fundamentos de la construcción sistemàtica"INAP. (2003).

SUÁREZ ESPINO, M. L.: «Los derechos de comunicación social en la jurisprudencia del Tribunal Europeo de Derechos Humanos y su influencia en el Tribunal Constitucional español», en la Revista de Derecho Constitucional Europeo de la Universidad de Granada, núm. 7. (2007).

SERRANO MAÍLLO, I.: «Las libertades informativas», en SÁNCHEZ GONZÁLEZ, S. (coord.).Dogmática y práctica de los derechos fundamentales, Tirant lo Blanch, Valencia. (2006).

SERRANO MAÍLLO, I: « el derecho a la libertad de expresión en la jurisprudencia del tribunal europeo de derechos humanos: dos casos españoles". UNED. Teoría y Realidad Constitucional, núm. 28, pp. 579-596. (2011).

SOLOVE, D.,"The digital person. Technology and privacy in the Information Age", New York University Press. (2004).

SULLIVAN C. "Digital Identity: An Emergent Legal Concept The role and legal nature of digital identity in commercial transactions", University of Adelaide Press. (2011).

THE GUARDIAN,https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems (última visita 9 de noviembre de 2018). (2011).

TENE, HAIM Y POLONETSKY "Big Data for All: Privacy and User Control in the Age of Analytics". Northwestern Journal of Technology and Intellectual Property Volumen 11. (2013).

VIJFVINKEL, M.M. "Technology and the right to be forgotten". Radboud University. (2016).

VIKTOR MAYER-SCHÖNBERGER,V. y CUKIER, K. "Big data: a revolución that will transform how we live,work, and think" Amazon. Versón Kindle. (2013)

VILLAVERDE MENÉNDEZ, "Protección de datos personales, derecho a ser informado y autodeterminación informática a propósito de la STC 254/1993", Revista de Derecho Constitucional, mayo-agosto 1994, pp. 189 a 223. (1994)

WARREN AND BRANDEIS," The Right to Privacy», 4 Harvard Law Review, 193. (1890).

WECHSLER S. 'The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten." Columbia Journal of Law & Social Problems . Vol. 49 Issue 1, p135-165. (2015)

WEST'S ENCYCLOPEDIA OF AMERICAN LAW, edition 2. The Gale Group, Inc. (2008)

WU, X., ZHU, X., WU, G.-Q. y DING, W. " Data Mining with Big Data."IEEE Transactions on Knowledge and Data Engineering, en especial pags, 97-107. (2014).

ZITTRAIN J.; "The future of the Internet- And How to stop It".Yale university. (2009).