COLEGIO UNIVERSITARIO DE ESTUDIOS FINANCIEROS

GRADO EN DERECHO

Trabajo Fin De Grado

PROTECCIÓN DE DATOS

DERECHO AL OLVIDO

Autor: Monroy López, Marta

Tutor: Berzosa López, Doctor D. Daniel

Madrid, abril de 2019

ÍNDICE

RESUMEN

El objetivo de este trabajo es hacer una comparativa en términos generales de las tres principales regulaciones existentes a día de hoy, como lo son Europa, Estados Unidos y China en materia de protección de datos, especialmente con relación al *derecho al olvido*, después de haber definido los derechos más relevantes en este tema. Analizaré los casos de *Google Spain* (*C-131/12)*, del cual ha surgido un nuevo e importante *derecho al olvido*, y el caso de *Google/CNIL (C-507/17)*, que actualmente está siendo muy discutido con relación al alcance que debe tener este derecho. Una vez hecha la comparativa entre las diferentes regulaciones podremos analizar como se resolvería la aplicación de estos casos si se hubiera dado en Estados Unidos o en China.

Palabras clave: Protección de datos – Derecho al olvido – Reglamento General de Protección de Datos (RGPD) - Desindexación

ABSTRACT

The objective of this research is to make a comparison in general terms of the three main existing regulations today, such as Europe, the United States and China in terms of data protection, especially in relation to the *right to be forgotten*, after having defined the most relevant rights in this subject. I will analyse *Google Spain* case (C-131/12), from which an important new *right to be forgotten* has arisen, and *Google/CNIL* case (C-507/17), which is currently being widely discussed in relation to the scope that this right should have. Once the comparison between the different regulations has been made, we will be able to analyse how the application of these cases would be resolved if it had taken place in the United States or China.

Key Words: Data Protection – Right to be forgotten – General Regulation of Data Protection (GRDP) – Right to delisting

ABREVIATURAS Y SIGLAS

ACC: La Administración del Ciberespacio China.

APD: Autoridades de Protección de Datos.

CCPA: Acta de Privacidad del Consumidor de California.

CIIs: Infraestructuras de información crítica.

CNIL: Comisión nacional de informática y derechos humanos.

CSL: Ley de Ciberseguridad China.

DUDH: Declaración Universal de Protección de Datos.

EEE: Espacio Económico Europeo.

FIPP: Principios de la Comisión Federal de Comercio de los Estados Unidos.

FTC: Principios de Prácticas Justas de Información de la Comisión Federal de Comercio de los Estados Unidos.

ISP: Proveedores de Servicios de Internet.

LAPO: Ley de Sanciones Administrativas del Orden Público en China.

LOPD: Ley Orgánica de Protección de Datos.

RGPD: Reglamento General de Protección de Datos.

RPC: República Popular de China.

SC-NPC: Comité Permanente de la Asamblea Popular Nacional.

TFUE: Tratado de Funcionamiento de la Unión Europea.

TJUE: Tribunal de Justicia de la Unión Europea.

UE: Unión Europea.

VPN: Red Privada Virtual.

1. INTRODUCCIÓN

«Cómo alguien dijo una vez: **"Dios perdona y olvida, pero la red nunca lo hace"** Con más y más datos privados flotando en la red, […] las personas deben tener derecho a que sus datos sean eliminados por completo».

VIVIANE REDING

Actualmente estamos en constante interacción a través de internet. Se están manejando grandes cantidades de datos personales en la red, los cuales se procesan, comparten, descargan, registran y se utilizan de todo tipo de formas con mucha frecuencia. Pero ¿tenemos los ciudadanos algún tipo de control sobre nuestra información personal?, ¿tenemos derecho a decidir que información personal se divulga, a quién y con que propósito? Y lo más importante, ¿tenemos derecho a que se *olvide* determinada información personal si esta nos está causando un perjuicio?

La respuesta a estas preguntas difiere dependiendo del lugar en el que nos encontremos. Si nos encontramos en Europa, el territorio más proteccionista en materia de protección de datos, podremos solicitar la cancelación, supresión o que desindexen nuestros datos, gracias al nuevo Reglamento General de Protección de Datos que entró en vigor en mayo de 2018. Sin embargo, si nos encontramos en Estados Unidos o China lo tendremos más complicado. En estos dos últimos no está reconocido un *derecho al olvido* como tal, pero existen una serie de leyes que en cierta medida protegen la privacidad y los datos personales. En especial, la nueva ley de ciberseguridad 2017 en China, que aún así, sigue violando los derechos fundamentales de sus ciudadanos.

El reconocimiento del *derecho al olvido* crea una controversia entre el derecho fundamental de protección de datos y el derecho a la vida privada, frente al derecho de libertad de expresión y acceso a información. Más adelante veremos los argumentos de ambas posturas.

Finalmente analizaré los puntos principales del conocido caso Google Spain del que nació un nuevo derecho al olvido y su continuación en el caso Google/CNIL donde se está estudiando hasta dónde puede llegar la aplicación de este derecho. Y para terminar, ¿que hubiera pasado si estos casos hubieran tenido lugar en Estados Unidos o China?

2. DERECHOS DE PROTECCIÓN DE DATOS

Para poder entender claramente la comparativa de regulaciones y analizar el caso de *Google Spain (c-131/12)* y posteriormente el Asunto *Google/CNIL (c-507/17),* es necesario pararnos a detallar previamente una serie de conceptos relevantes para este estudio.

2.1 Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos, en adelante DUDH, fue proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A (III) [1]. En relación con este trabajo debemos destacar el derecho a la libertad de expresión y a la vida privada a nivel *universal*.

2.1.1 Derecho a la libertad de opinión y expresión: El artículo 19 de la DUDH establece que «todos tendrán derecho a opinar sin interferencia» y «todos tendrán derecho a la libertad de expresión, este derecho incluirá la libertad de buscar, recibir y difundir información e ideas de todo tipo, independientemente de fronteras, ya sea oralmente, por escrito o impreso, en forma de arte, o por cualquier otro medio de su elección»[2].

2.1.2 Derecho a la vida privada: El artículo 12 declara 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 teles injerencias o ataques»[3].

2.2 Ley Orgánica de Protección de Datos

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en adelante LOPD, recoge en su Título III una cuestión tan esencial como son los derechos de las personas en el ámbito de la protección de los datos, podríamos considerarlos también *derechos digitales* [4]. Estos derechos son principalmente, el derecho

[1] Declaración Universal de los Derechos Humanos (DUDH) proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A (III)

[2] Artículo 19 de la Declaración Universal de los Derechos Humanos (DUDH)

[3] Artículo 12 de la Declaración Universal de los Derechos Humanos (DUDH)

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD)

a la información, el derecho a la obtención del consentimiento y los derechos ARCO, los cuales son, derecho de Acceso, Rectificación, Cancelación y Oposición al tratamiento[5].

Según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, los derechos ARCO constituyen las facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

Procedo a explicar de manera breve y concisa el significado principal de cada uno para entender de forma clara las diferencias entre ellos.

2.2.1 Derecho de Acceso: En el artículo 15 se define como el derecho que tiene toda persona a obtener información sobre el tratamiento de sus datos personales. El titular tiene derecho a conocer la finalidad, los destinatarios, el plazo de conservación, el origen de la información y las decisiones automatizadas[6].

2.2.2 Derecho de Rectificación: El artículo 16 permite la modificación de información personal, por ejemplo, corrección de errores, modificar datos inexactos o incompletos y garantizar la certeza de la información tratada[7].

2.2.3 Derecho de Cancelación: El derecho de cancelación se define en el artículo 16.3 de la LOPD como «La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión»[8].

2.2.4 Derecho de Oposición: Según el artículo 17, se permite al interesado, en los casos previstos en el Reglamento General de Protección de Datos, oponerse al tratamiento

[5] Velasco, J. (2016) Derecho de Acceso, Rectificación, Cancelación y Oposición. Big Data ISDE

[6] Artículo 15 de la Ley Orgánica de Protección de Datos (LOPD).

[7] Artículo 16 de la Ley Orgánica de Protección de Datos (LOPD).

[8] Artículo 16.3 de la Ley Orgánica de Protección de Datos (LOPD).

de sus datos personales. El responsable deberá cesar su tratamiento[9]. (En el apartado de Europa veremos que es el *tratamiento*).

2.3 Reglamento General de Protección de Datos

El Reglamento 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/CE (Reglamento general de protección de datos), en adelante RGPD, entró en aplicación el 25 de mayo de 2018, y amplia los derechos anteriormente mencionados[10].

2.3.1 Derecho a la Portabilidad: Este derecho regulado en el Artículo 20 del RGPD y al que se hace mención en el artículo 17 de la LOPD, permite al interesado obtener del responsable del tratamiento parte de sus datos personales, en un formato estructurado y claro, y reutilizarlos[11].

2.3.2 Derecho al Olvido: Derecho a controlar y preservar del conocimiento público y general determinados datos o hechos que les afectan o que no desean que sean conocidos. La Comisión Europea en 2010 definió el derecho al olvido como «el derecho de las personas a que sus datos ya no se procesen y eliminen cuando ya no sean necesarios para fines legítimos». A mediados de junio de 2015. El *derecho al olvido* se había convertido en *el derecho al olvido y a la supresión*, según lo estipulado en el artículo 17 del RGPD[12].

Envuelve dos conceptos relacionados pero diferentes en la ley de protección de datos de la UE: (i) el derecho de *supresión* que formaba parte de la Directiva de protección de datos; y ii) el derecho a *desindexar* derivado por el TJCE a mediados de 2015 de la Directiva de protección de datos en *Google Spain.*

[9] Artículo 17 de la Ley Orgánica de Protección de Datos (LOPD).

[10] El Reglamento 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/CE (RGPD).

[11] Artículo 20 del Reglamento General de Protección de Datos (RGPD).

[12] Artículo 17 del Reglamento General de Protección de Datos (RGPD).

El derecho de supresión (*erasure*)

La cancelación de los datos, se denomina en el nuevo RGPD *derecho de supresión*, y lleva aparejado el derecho al olvido, que se arbitra como la posibilidad del interesado de instar la supresión de los datos que se encuentren accesibles al público, por lo que el responsable de tratamiento de datos podrán adoptar medidas razonables y técnicas que informen a los responsables que traten los datos personales de que existe una solicitud de supresión de cualquier clase de enlace a tales datos[13].

El derecho a desindexar (*delisting*)

Indexar*:* «Registrar ordenadamente datos para elaborar un índice con ellos» RAE.

La indexación de internet se define como diversos métodos para incluir en el índice de internet el contenido de un sitio web. Determinados sitios web o intranet pueden utilizar un índice de *back-of-the-book*, mientras que los motores de búsqueda suelen utilizar palabras clave y metadatos. La indexación web también está adquiriendo importancia para los sitios web de periódicos o revistas con contenido actualizado[14].

La información de indexación web implica la asignación de palabras clave o frases a páginas web o sitios web dentro de un campo de meta-etiquetas, por lo que los sitios web pueden ser recuperados con un motor de búsqueda que se personaliza para buscar el campo de palabras clave.

Por lo tanto, el *derecho a desindexar*, es el derecho a poder eliminar de este índice o lista de resultados que tiene el motor de búsqueda, determinados enlaces que contengan información perjudicial para una persona cuando esta introduce, por ejemplo, su nombre como palabra clave en búsqueda.

Esta desindexación conlleva la desvinculación del sitio web en cuestión, lo que hace prácticamente imposible volver a encontrarlo a través de ese buscador, pero es importante tener en cuenta que esa información no ha sido eliminada, solo desvinculada. Por lo tanto, sigue existiendo en la red.

[13] Grupo Ático 34 (2018). Derecho al olvido en el RGPD. Blog de Protección de Datos para Empresas y Autónomos.

[14] Click Datos (2016) Diferencias entre el derecho de supresión de datos y el derecho al olvido.

3. DIFERENTES REGULACIONES EN PROTECCIÓN DE DATOS

3.1 Europa

3.1.1 Introducción

El Tratado de Lisboa introdujo cambios significativos en el marco jurídico de la protección de datos en la Unión Europea, en adelante UE[15]. Cabe destacar la introducción de una base jurídica explícita para la legislación en materia de protección de datos en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en adelante TFUE, así como la inclusión de un derecho a la protección de datos en la Carta de la Unión Europea.

Las normas de protección de datos de la UE se aplican al tratamiento de datos personales, por lo que en este Derecho se imponen ciertas obligaciones a aquellos que controlan y llevan a cabo el tratamiento de dichos datos. Los responsables del tratamiento de este tipo de datos se tienen que asegurar de que el procesamiento de los datos se hace respetando una serie de garantías y conforme a una base legal.

Esta regulación se recoge en el RGPD y permite a los Estados miembros de la UE aplicar determinadas disposiciones en el derecho interno.

La Directiva de 95/46/CE, sustituida por el RGPD, se movía en un contexto legislativo donde los regímenes jurídicos de los Estados miembros eran muy dispares, y existía una preocupación en el Parlamento Europeo sobre el impacto de los datos personales en relación con los derechos individuales. Por eso tomaron como objetivos, facilitar la libre circulación de datos personales en el mercado interior de la UE y proteger los derechos fundamentales[16].

El RGPD innova principalmente en: Derechos, Armonización, Competencias de ejecución y nuevas técnicas de regulación. Aunque en palabras de Hustinx: «... a pesar de toda la innovación, también hay una gran cantidad de continuidad. Todos los conceptos

[15] Tratado de Lisboa 2009. (DO C 306 de 17.12.2007).

[16] Lee Andrew Bygrave. Data Privacy Law: An International Perspective. Pag 53 – 75

y principios básicos familiares seguirán existiendo, con sujeción a algunas aclaraciones y cambios más pequeños en detalles»[17].

En este apartado se identificarán algunas de las características más relevantes que conforman la regulación de la UE en materia de protección de datos[18].

3.1.2 Características del Régimen de la UE

Podríamos decir, grosso modo, que el régimen de protección de datos en la Unión Europea es ómnibus, legitimador y en base a derechos. Decimos que es un régimen *general* porque (i) aplica las normas de protección de datos tanto a agentes públicos como privados; (ii) tiene neutralidad sectorial, aunque en ámbitos específicos que son *delicados* o en los que un mal tratamiento de los datos personales puede tener efectos perjudiciales sí proporciona protección más sectorial; y la (iii) aplicación de sus normas se realiza por organismos reguladores independientes especializados. Es un régimen *legitimador* porque el tratamiento de datos personales debe tener un fundamento jurídico (artículo 6 RGPD) y respetar las garantías (artículo 5 RGPD). Está basado en *derechos*, los cuales han sido reformulados buscando su mayor eficacia[19].

A continuación, abordaremos, de manera más concreta, algunos de los puntos más relevantes del RGPD.

3.1.3 Fundamentos

El fundamento de esta regulación la encontramos en la Carta de Derechos Fundamentes de la UE. Prestando especial atención a su artículo 8 relativo a la protección de datos personales. En este artículo encontramos que (i) Todo el mundo tiene derecho a la protección de los datos personales. Depende del lugar en el que nos encontremos, existirán diferencias en el concepto de datos personales, las cuales son muy relevantes.

[17] Hustinx, P. (2015) Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de reglamento del Consejo relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido (2010/C 66/01).

[18] Kuner, C. (2017) «The internet and the global Reach of EU Law»; Lynskey, O. (2015) «The Foundations of EU Data Protection Law».

[19] Lynskey, O. (2015) «The Foundations of EU Data Protection Law», págs. 15 – 45.

Pero la UE comparte el mismo concepto que veremos más adelante. (ii) Es necesario el consentimiento del usuario para el tratamiento de sus datos y especificar su fin. Los usuarios podrán acceder a sus datos personales y modificarlos. (iii) Una autoridad independiente será la encargada de controlar el cumplimiento de esta normativa[20].

La regulación europea enfatiza la seguridad de los datos personales, se debe garantizar una seguridad apropiada para el riesgo (articulo 32 RGPD), y además, establece en los artículos 33 y 34 del RGPD las notificaciones de violación de datos.

3.1.4 Ámbito de aplicación del RDPD

Personal

En el ámbito personal nos referimos a *Datos personales* y es «toda información relativa a cualquier persona física identificada o identificable»[21].

Tenemos tres elementos clave en este concepto que podemos encontrar en el Dictamen 4/2007 sobre Datos Personales, 20 junio de 2007 de la Comisión Europea[22]:

1) Con *toda la información* se refiere a: información que puede ser incorrecta o falsa, no tiene por qué estar cubierta por el derecho a la vida privada y el formato de la información no es relevante.
2) *Relativo a:* Es la información relacionada con la persona en cuestión.
    - Contenido: Es la información sobre una persona en particular independientemente de cualquier propósito por parte del controlador de datos o un tercero, o el impacto que esa información puede tener en el sujeto.
    - Propósito: Cuando los datos se utilizan para una finalidad determinada, como por ejemplo, para evaluar o influir en el estado o comportamiento de una persona.
    - Resultado: Dependiendo de las circunstancias, determinados derecho e intereses de la persona pueden sufrir un impacto por dichos datos.

Es importante tener en cuenta que «... no es necesario que los datos se enfoquen en alguien con el fin de considerar que se relaciona con él»

[20] Artículo 8 de la Carta de los Derechos Fundamentales de la UE

[21] Artículo 4.1 del Reglamento General de Protección de Datos

[22] Comisión Europea. Dictamen 4/2007 sobre Datos Personales, 20 junio de 2007

3) *Persona identificable* es «alguien que puede identificarse, directa o indirectamente, por referencia a un número de identificación (Dirección IP) o a uno o más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social» Se deben tener en cuenta los medios utilizados para identificar a la persona.

Tecnológico

Es importante prestar atención a la diferencia entre un *controlador de datos* y un *procesador de datos* ya que determina el actor responsable del cumplimiento, por lo tanto, frente al que los sujetos ejercerán sus derechos. Estas diferencias las encontramos en el artículo 4 del RGPD[23].

Tanto el controlador de datos como el procesador de datos se definen como «Persona física o jurídica, autoridad pública, organismo o cualquier otro organismo», pero se diferencian en que, el controlador de datos determina los fines y medios del tratamiento de los datos personales; mientras que el procesador de datos se limita a procesar los datos personales en nombre del responsable del tratamiento.

3.1.5 Régimen jurídico

Tratamiento de Datos

Para poder entender que significa la oposición al tratamiento y hasta dónde llega, debemos saber primero que se entiende por tratamiento. Este concepto viene definido en el artículo 4 del RGPD entre otros tantos. Según este artículo, es cualquier operación realizadas sobre datos personales, independientemente de si estas operaciones son automatizadas o no. Como por ejemplo «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»[24].

[23] Artículo 4 del Reglamento General de Protección de Datos (RGPD).

[24] Artículo 4.2 del Reglamento General de Protección de Datos (RGPD.

Para que sea lícito debe cumplir alguno de estos requisitos: consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, proteger los intereses vitales de alguna persona, interés público, perseguir interés legítimo[25].

Consentimiento

Vemos que el consentimiento es, en muchas ocasiones, un requisito indispensable. Este se entiende como la firma del interesado en forma de aceptación específica del tratamiento de sus datos personales siempre que sea informada[26]. Es decir, debe ser: libremente dado, firmado e informado.

Existen disposiciones específicas para los niños. «Consentimiento del niño en relación con los servicios de la sociedad de la información»: El procesamiento de los (i) datos personales del niño es lícito cuando tiene más de 16 años. Verificación de la autorización: el responsable del tratamiento debe hacer (ii) esfuerzos razonables, teniendo en cuenta la tecnología disponible.

Principios relativos al procesamiento de los datos personales

Se deben cumplir una serie de garantías que podemos encontrar en el artículo 5 del RGPD tales como: ser tratados de manera (i) lícita, leal y transparente; (ii) limitado a fines determinados, explícitos y legítimos; (iii) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; (iv) exactos y actualizados, y se adoptarán medidas razonables para su rectificación sin dilación. (v) mantener en una forma que permita la identificación de los sujetos de datos durante no más de lo necesario para los fines para los que se procesan los datos; (vi) Procesado de manera que garantice la seguridad adecuada de los datos personales (integridad y confidencialidad)[27]

Mayor Armonización

El objetivo del RGPD es armonizar el procesamiento de datos personales por parte de las organizaciones y crear así igualdad de oportunidades para la competencia dentro de la

[25] Artículo 6 del Reglamento General de Protección de Datos (RGPD.

[26] Artículo 4.11 del Reglamento General de Protección de Datos (RGPD.

[27] Artículo 5 del Reglamento General de Protección de Datos (RGPD).

UE. El Reglamento también se aplica fuera de la UE siempre que su procesamiento de datos afecte a las personas que viven en la Unión Europea[28].

Remedios, Responsabilidad y Sanciones

Este reglamento establece la posibilidad de exigir a determinados (i) organismos no lucrativos que ejerzan el derecho a remediar en nombre del interesado. Derecho a (ii) indemnización por daños materiales o inmateriales. (iii) Multas administrativas mejoradas. Todo esto aparece regulado en Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos[29].

Derechos del interesado

Los más importantes serían: Derecho de información (Arts. 12-14 RGPD), Derecho de acceso (Art 15 RGPD), Derecho de rectificación (Art 16 RGPD), Derecho a la portabilidad de los datos (Art. 20 RGPD), Prohibición de la toma de decisiones automatizada (Art. 22 RGPD). Los cuales ya han sido explicados anteriormente.

Reconocimiento del Derecho al Olvido

Artículo 17 RGPD *derecho al olvido y a la supresión* afirma que «el interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurran algunas de las circunstancias siguientes: que los datos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados, que el interesado retire el consentimiento, que se oponga al tratamiento o que el tratamiento no sea conforme con las disposiciones del Reglamento».

Consecuentemente el derecho al olvido está asociado a la facultad de supresión de los datos personales. Se asocia con la facultad de disposición de nuestros propios datos, no con la mera inexactitud o el carácter incompleto que se pudiera encontrar. Ello implica la

[28] Kuner, C. (2017) «The internet and the global Reach of EU Law», págs.52 – 85.

[29] Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

capacidad de exigir al responsable del tratamiento la supresión de los datos que se relacionan con su persona y la abstención de su difusión.[30]

Autoridades de Protección de Datos

Según el artículo 8.3 de la Carta de la UE, las Autoridades de Protección de Datos, en adelante las APD, son «autoridades públicas independientes que supervisan, mediante poderes de investigación y correctivos, la aplicación de la ley de protección de datos. Ofrecen asesoramiento experto sobre cuestiones de protección de datos y gestionan las reclamaciones presentadas contra las infracciones del RGPD y las leyes nacionales pertinentes. Hay uno en cada Estado miembro de la UE»[31].

Regímenes nacionales de privacidad de datos en Europa

Europa es el hogar de las leyes de privacidad de datos más antiguas, exhaustivas y completas. Europa, a través de sus instituciones supranacionales, es el promotor de las iniciativas internacionales más amplias en este ámbito[32].

Los puntos comunes para los regímenes nacionales de privacidad de datos en Europa son los siguientes:

i. Cobertura tanto del sector público como del privado;
ii. La cobertura de los sistemas automatizados y manuales de tratamiento de datos personales, con independencia de cómo estén estructurados los datos;
iii. Aplicación de definiciones generales de *datos personales*;
iv. La aplicación de amplios conjuntos de principios de procedimiento, algunos de los cuales rara vez se encuentran en regímenes de privacidad de datos de otros lugares.
v. Una regulación más estricta de determinadas categorías de datos sensibles (por ejemplo, los datos relativos a las creencias filosóficas, las preferencias sexuales, la etnia, orígenes);

[30] Córdoba, D. (2014) El "derecho al olvido" tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Revista de Jurisprudencia

[31] Maniacs (2018) ¿Qué son las Autoridades de Protección de Datos (APD)?; Artículo 8.3 de la Carta de los Derechos Fundamentales de la UE.

[32] Bygrave, Lee A. (2014) Data Privacy Law, an International Perspective, pág 100. Oxford University Press.

vi. Restricciones previas al flujo transfronterizo de datos personales a países que carecen de una protección adecuada de los datos;
vii. Establecimiento de apd independientes con amplios poderes discrecionales para supervisar la aplicación y el desarrollo de las normas sobre protección de datos;
viii. Canalizar las quejas sobre privacidad a estas agencias en lugar de a los tribunales;

Se hace hincapié en que Europa es más que la UE. Además, la tracción de las normas de privacidad de datos de la UE en los países europeos que no son Estados miembros de la UE o el Espacio Económico Europeo, en adelante EEE, puede ser débil.

Por ello se considera un régimen influyente. El ámbito geográfico de aplicación se encuentra regulado en el artículo 3 GDPR: (i) Tratamiento de datos en el contexto de las actividades del establecimiento de un responsable o procesador de datos en un Estado miembro de la UE; (ii) El procesamiento de datos de los residentes de la UE en los que se ofrecen bienes o servicios a los residentes de la UE o su comportamiento en la UE es supervisado; (iii) La legislación de los Estados miembros se aplica en el tercer país debido al derecho internacional público.

3.2 Estados Unidos

3.2.1 Introducción

Al otro lado del Atlántico, un gran número de países han adoptado regímenes de privacidad de datos que adoptan o están en gran medida en armonía con el enfoque europeo[33].

El más antiguo de estos regímenes es el canadiense. En Canadá todas las provincias y territorios canadienses han promulgado leyes de privacidad de datos, por ejemplo, cuenta con una legislación federal que cubre la privacidad de datos con relación al sector del gobierno federal, una legislación federal sobre el sector privado y existen ADP tanto a nivel federal como provincial.

[33] Bygrave, Lee A. (2014) Data Privacy Law, an International Perspective, págs. 102 – 116. Oxford University Press.

En América del Sur, las normas rudimentarias sobre privacidad de datos se manifestaron inicialmente en forma de derechos constitucionales de hábeas data. El hábeas data permite a una persona obtener, mediante una orden judicial, acceso a los datos que se mantienen sobre ella en las bases de datos del gobierno y, si procede, hacer que se rectifiquen o eliminen los datos

Sin embargo, Estados Unidos, en adelante EE. UU, la nación económica y militarmente más poderosa de la región y, de hecho, del mundo, ha evitado firmemente las soluciones legislativas generales para la privacidad de los datos.

3.2.2 Características generales en EE. UU

En EE. UU, dependiendo de dónde opere cada empresa, las normas y reglas para el tratamiento de datos varían entre estados, lo que implica la existencia de diferentes niveles de seguridad y exigencias.

A raíz de la aprobación del RGPD, y las presiones desde Europa por un endurecimiento de las normativas, varios estados modificaron sus leyes o introdujeron cláusulas nuevas. Por ejemplo, California aprobó en 2018 el *California Consumer Privacy Act*, en adelante CCPA, una norma inaudita en EE. UU por imponer, por primera vez, niveles de protección de datos muy similares a los presentes en el RGPD. También, Arizona ha introducido un nuevo sistema de notificación en caso de fallo de seguridad, mientras que Vermont ha aprobado leyes para exigir mayor transparencia a quienes tratan con información personal de los usuarios.

Las características más diferenciadoras de la regulación en materia de protección de datos en EE. UU podríamos decir (i) que el sector público y privado están regulados de forma limitada (ii) cuentan con regulación específica para el sector privado (iii) No existe un solo organismo de supervisión, y (iv) las empresas pueden acceder completamente a los datos de sus consumidores/usuarios[34].

[34] Goldman, E. (2013) La nueva ley de supresión de California debe ser eliminada. Forbes

3.2.3 Características específicas en EE. UU

a) Derecho a la privacidad

Hace año y medio, Donald Trump firmó una ley para permitir a los proveedores de servicios de Internet, en adelante ISP, vender datos de los consumidores sin consentimiento previo. Aunque las empresas de Internet como Facebook y Google ya tenían acceso a este tipo de información y recopilaban datos de los consumidores sin tener que pedir permiso, ahora los ISP pueden ir más allá y acceder a la información completa sobre todos los sitios web que visita un consumidor[35].

Ningún derecho al respeto a la vida privada se encuentra recogido de forma explícita en la Constitución de los EE. UU. Pero el Tribunal Supremo lo ha considerado implícito en: (i) La Primera Enmienda, libertad de culto, expresión, prensa, petición y reunión; (ii) Cuarta Enmienda, interdicción de registros e incautaciones irrazonables, es necesaria orden de registro para buscar personas o bienes; (iii) Quinta enmienda, protege frente a la auto incriminación y obligación de revelar información; (iv) Novena Enmienda, derechos de los ciudadanos; (v) Decimocuarta enmienda, ciudadanía, debido proceso estatal, igual protección[36].

Es importante hacer mención a la Cuarta Enmienda la cual dice: «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 verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas» para explicar brevemente el caso de Katz v. Estados Unidos 389 U.S 347 (1967)[37].

[35] Redondo, T. (2019) Protección de datos en Estados Unidos: ¿Cómo afecta a tu negocio? Mailjet.

[36] Nieves, M. (2011) El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego, págs. 280 – 289.

[37] Cuarta Enmienda de la Constitución de los Estados Unidos de América 1787.

Caso Katz v. Estados Unidos 389 U.S. 347 (1967)

Charles Katz utilizó una cabina telefónica pública para realizar apuestas ilegales desde Los Ángeles a Miami y Boston. Sin que Katz lo supiera, el FBI estaba grabando sus conversaciones a través de un dispositivo electrónico de escucha conectado al exterior de la cabina telefónica. Katz fue condenado gracias a estas grabaciones. Rechazó su condena, argumentando que las grabaciones se obtuvieron en violación de sus derechos de la Cuarta Enmienda.

La Corte sostuvo que la policía necesitaría una orden para buscar, pero en este caso, al no haber intrusión física en la cabina, falló a favor del FBI. También aclaró que la Cuarta Enmienda protege a las personas, no lugares. «La persona debe haber exhibido una expectativa real (subjetiva) de privacidad», «La sociedad debe reconocer que la expectativa es razonable»[38].

Ley Federal de Privacidad 1974

La Ley de Privacidad, Título 5, Sección 552a del Código de los Estados Unidos, aprobada por el Congreso en 1974 es un compendio del «código de prácticas de información justa» que intenta regular la recopilación, el mantenimiento, el uso y la diseminación de información personal de las agencias de la rama ejecutiva federal de Estados Unidos[39]. La Ley de Privacidad proporciona a los ciudadanos estadounidenses y a los extranjeros legalmente admitidos como residentes permanentes una mayor influencia en la forma en que se mantienen los registros sobre ellos y elimina las intrusiones innecesarias en la privacidad personal a través del mantenimiento de registros externos.

La Ley garantiza lo siguiente a las personas cuya información se recopila: (i**)** *No hay ningún sistema secreto* de mantenimiento de registros personales del Gobierno Federal. (ii) Los archivos de información personal federales se limitan a los que son claramente *necesarios*. (iii) Tienen la oportunidad de ver la información que se guarda sobre ellos y de *corregirla* si es incorrecto, irrelevante, inoportuno o incompleto. (iv) La información personal recopilada con un propósito *no puede utilizarse para otro fin sin su consentimiento.* (v) El derecho a *demandar al gobierno* por violaciones a la Ley,

[38] Tribunal Supremo de Estados Unidos. Caso: Katz vs. Estados Unidos, 389 U.S. 347, sentencia de 18 de diciembre de 1967.

[39] IBM Knowledge Center (2017) Informe de la Ley de Privacidad de 1974

incluyendo si el gobierno permite a otros ver tu documento personal, excepto si esta específicamente permitido por la ley. (vi) Si se divulga información, pueden *averiguar a quién se ha divulgado,* con qué propósito y en qué fecha. (vii) establecer salvaguardias administrativas y técnicas apropiadas para asegurar la *seguridad* de los registros.

En cuanto a la divulgación de los registros, existen normas detalladas. La regla general es que la divulgación está prohibida sin el consentimiento individual. Pero existen excepciones a esta regla como por ejemplo el *uso rutinario*, aunque este mismo se encuentra limitado por: (i) El uso debe ser compatible con el propósito de la recolección inicial, (ii) El aviso real del uso rutinario se debe dar al individuo pertinente (iii) Todos los usos rutinarios deben publicarse en el registro federal.

Principios de la Comisión Federal de Comercio de los Estados Unidos

Los principios de la Comisión Federal de Comercio de los Estados Unidos, en adelante los FIPP, son directrices que representan conceptos ampliamente aceptados en relación con la práctica de la información justa en el mercado electrónico.

Los Principios de Prácticas Justas de Información de la Comisión Federal de Comercio, en adelante FTC, son el resultado de la investigación de la Comisión sobre la forma en que las entidades recopilan y utilizan la información personal y las salvaguardias para garantizar que la práctica sea justa y proporcione una protección adecuada de la privacidad de la información en internet. La FTC ha estado estudiando cuestiones de privacidad en línea desde 1995, y en su informe de 1998 la Comisión describió los Principios de Prácticas Justas de Información de Aviso, Elección, Acceso y Seguridad ampliamente aceptados[40]. La FTC también identificó la aplicación, el uso de un mecanismo fiable para establecer sanciones por incumplimiento como un componente crítico de cualquier programa gubernamental o de autorregulación para proteger la privacidad en internet.

- *Aviso/conciencia:* Los consumidores deben ser notificados de las prácticas de información de una entidad antes de que se recopile cualquier información personal de ellos.

[40] Comisión Federal de Comercio (1998) Informe para el Congreso sobre la Privacidad en internet

- *Elección/consentimiento:* Ofrecer a los consumidores opciones para controlar la forma en que se utilizan sus datos (*opt-in, opt-out*). Aunque al proporcionar ciertos datos les hacen firmar un acuerdo (ej: médico) que suele decir que un «tercero puede tener acceso a la información que usted proporciona bajo ciertas condiciones», por lo que realmente el acceso a la información personal de los clientes está fuera de su control.
- *Acceso/participación:* **«**capacidad del consumidor para ver los datos recopilados y también para verificar y refutar su exactitud. Este acceso debe ser barato y oportuno para que sea útil al consumidor».
- *Integridad/seguridad:* Asegurarse de que los datos que recolectan sean exactos y seguro.
- *Ejecución/reprocesamiento:* Debe haber medidas de aplicación como: autorregulación de los recolectores de información, acciones civiles, sanciones del gobierno.

Limitaciones de la Ley Federal de Privacidad

Los tribunales federales tienen facultades limitadas como, por ejemplo, (i) no pueden ordenar cambios de comportamiento. Pueden ordenar acceso sujeto a los registros, enmiendas de inexactitudes en los registros y daños por lesiones sufridas. (ii) Agencias que ignoran las limitaciones de la excepción de uso rutinario, por ejemplo, los criterios de compatibilidad y de notificación real. (iii) Supervisión interna y externa ineficaz del cumplimiento por parte de las agencias federales.

Regulación Sectorial Específica

Regulación específica del sector ad hoc, se promulgó en respuesta a una controversia.
Ejemplos: (i) Ley de Informes de Crédito Justos de 1970; (ii) Ley de Protección de la Privacidad de Vídeo de 1998; (iii) Ley de Protección de la Privacidad del Conductor de 1994; (iv) Ley de protección de la privacidad en internet de los niños de 1998; (v) Ley de Control de la Agresión de la Ley de Pornografía y Marketing No Solicitado (CAN-SPAM) de 2003.

El Papel de la Comisión Federal de Comercio

Promueve la autorregulación de la industria. Requiere una acción caso por caso para abordar: *Agravio*: (i) Perjuicio sustancial, (ii) No compensado por los beneficios

compensatorios, (iii) El daño debe ser inevitable en la práctica. *Engaño* (i) Una representación, omisión o práctica que pueda inducir a error al consumidor, (ii) El acto/práctica se considera desde el punto de vista de un consumidor razonable, (iii) La representación debe ser material.

Casa Blanca – Orden Ejecutiva (enero 2017)

La Orden Ejecutiva No. 13768 del presidente Trump titulada «Mejorando la Seguridad Pública en el Interior de los Estados Unidos» incluye una sección que revoca políticas de privacidad, eliminando así los derechos de privacidad que habían sido extendidos a personas no estadounidenses:

«Sección 14: Las agencias, en la medida en que sea consistente con la ley aplicable, se asegurarán de que sus políticas de privacidad excluyan a las personas que no sean ciudadanos de los Estados Unidos o residentes permanentes legales de las protecciones de la Ley de Privacidad con respecto a la información personal identificable.

Sección 4: Ejecución de las Leyes de Inmigración en el Interior de los Estados Unidos. En cumplimiento de la política descrita en la sección 2 de esta orden, obligo a las agencias que empleen todos los medios legales para asegurar la fiel ejecución de las leyes de inmigración de los Estados Unidos contra todos los extranjeros que pueden ser expulsados de los Estados Unidos (incluyendo el intercambio de datos)» [41].

b) Derecho al Olvido

En los Estados Unidos no existe un *derecho al olvido* de la misma manera que en la Unión Europea, en su lugar cuentan con estatutos y sentencias judiciales que se acercan a un derecho al olvido muy limitado[42].

Lo más parecido podríamos encontrarlo, por ejemplo, en California, donde existe el *derecho a la supresión*, es decir, obligar a un sitio web a eliminar determinada

[41] Orden Ejecutiva de la Casa Blanca (2017) Mejorando la Seguridad Pública en el Interior de los Estados Unidos, Nº 13768, 25 enero; Orden Ejecutiva de la Casa Blanca (2017) Memorándum de Orientación de la Política de Privacidad, Nº 1, 25 abril;

[42] Walker, R. (2012) The Right to be forgotten, pág. 257. 64 Hastings Law Journal.

información, pero solo empleado a los menores y sobre contenido que ellos mismos hayan publicado[43].

En marzo de 2017, el senador del estado de Nueva York, Tony Avella y el asambleísta David Weprin presentaron un proyecto de ley A05323, titulado «*An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act*», para crear un derecho al olvido, similar al derecho creado por el Tribunal de Justicia de la Unión Europea, en adelante TJUE, en el caso Google Spain. Se propone el derecho a los ciudadanos a exigir a los motores de búsqueda y a los editores en internet que eliminen información que sea inexacta, «irrelevante», «inadecuada» o «excesiva», que «ya no sea relevante para el debate o el discurso público actual» y que «esté causando un daño demostrable al tema»[44].

Existen dos posturas enfrentadas con relación al derecho al olvido en los EE. UU.
Por un lado, se sostiene que la eliminación de contenido en internet violaría los derechos a la libertad de expresión y acceso a la información recogidos en la Primera Enmienda, a lo que se añaden los casos de la Corte Suprema como Cox Broadcasting v. Cohn, 420 U.S. 469 (1975), Smith v. Daily Mail, 443 U.S. 97 (1979), Florida Star v. BJF, 491 U.S. 524 (1989), y Bartnicki v. Vopper 532 U.S. 514 (2001). Estos casos junto con jurisprudencia apoyan que la publicación de información será difícilmente sancionada penal o civilmente, incluyendo información falsa e incluso difamación.

Además, la Sección 230(c)(1) de la Ley de Decencia en las Comunicaciones, 47 U.S.C. 230(c) prohíbe las *reclamaciones* contra los motores de búsqueda basadas en su vinculación con material supuestamente ilícito. Esta Sección, incluye tanto la solicitud de eliminación de los datos, como las medidas cautelares necesarias[45].

[43] Goldman, E. (2013) La nueva ley de supresión de California debe ser eliminada. Forbes; Norton Rose Fulbright (2017) Orden Ejecutiva de eliminación de la Ley de protección de la Privacidad para los canadienses

[44] Washington Post. Retrieved 17 March 2017.

[45] Sección 230 de la Ley de Decencia de Comunicaciones de 1996, también conocida como Ley de Telecomunicaciones 1996 (CDA)

Los proveedores de servicios en internet a veces pueden eliminar voluntariamente los enlaces al contenido si se presentan con una orden judicial que declare la información ilícita, pero los tribunales de los EE. UU. en general se niegan a obligarles a hacerlo.

Organizaciones de libertad de expresión, incluida la *Electronic Frontier Foundation*, también están preocupadas por los esfuerzos actuales de los reguladores franceses para que los efectos del derecho al olvido tengan alcance mundial. Lo que podría ir en contra de la Constitución de los EE. UU. (Caso Google/CNIL (c-507/17) el cual analizaremos más adelante).

Y por el lado contrario, el 88% de los estadounidenses apoyan este llamado *derecho al olvido* luchando por la defensa de los derechos fundamentales de los usuarios afectados, como son el respeto a la vida privada, la intimidad, y la reputación (honor). Las perspectivas de una legislación similar a la europea en los EE. UU. son escasas[46].

3.3 China

3.3.1 Introducción

En este apartado trataré la protección de los datos en internet de los ciudadanos chinos, la cual es muy diferente antes y después de mediados de 2010[47]. Antes los demandantes solo podían proteger indirectamente su privacidad en internet recurriendo a demandas por difamación. Sin embargo, en la actualidad existe una nueva ley aprobada en 2017 creada con el supuesto fin de controlar y defender los riesgos de ciberseguridad, pero la violación de los derechos y libertades de sus ciudadanos chinos en internet no cesa[48].

3.3.2 Características generales

Una de las características más llamativas es el aislamiento. Acto seguido encendemos nuestro móvil en China, no podemos acceder al correo electrónico de Gmail, ni a redes

[46] Heilweil, R. (2018) ¿Como de cerca está el derecho al olvido en América?

[47] Ning Yan, M. (2105) Protecting the Right to be Forgotten: Is Mainland China Ready. European Data Protection Law Review, págs. 190 – 205

[48] Ley de Seguridad de Internet de China. 1 junio 2017

sociales habituales como Facebook, Twitter, Instagram o Pinterest. Tampoco se puede utilizar Google, ni orientarse a través de la aplicación mapas de Apple. Y si desea acceder a información del exterior debe ser a través de un pequeño abanico de medios de comunicación internacionales[49].

Sin embargo, dentro del territorio chino existen otras plataformas similares a las mencionadas, por ejemplo, Baidu es Google, Weibo es Twitter, WeChat es Facebook, Instagram y WhatsApp, Alipay es Paypal, Youku es YouTube, y así hasta el infinito. La diferencia es que todas estas compañías cumplen con la legislación china. Esto significa que comparten todos los datos privados de los usuarios con el gobierno chino, filtran los resultados de sus búsquedas de acuerdo con las ordenes del partido comunista y censuran lo que les parece conveniente.

También se puede acceder al exterior utilizando una Red Privada Virtual, en adelante VPN, como muchas empresas y personas físicas hacen, pero los dirigentes chinos han decidido exigir que todos los proveedores de datos de titularidad pública cesen su acceso a estas VPN.
Al igual que el presidente Xi Jinping visitó las principales cadenas de televisión del país y dijo a sus periodistas que *deben estar al servicio del partido comunista y respetar su liderazgo.* Es decir, está prohibido publicar noticias propias, lo cual otorga a la prensa estatal el monopolio de la información, ya que está controlado directamente por el partido.

Esto demuestra la gran falta de respeto hacia los derechos humanos, como son el derecho de libertad de expresión e información y el derecho a la vida privada.

3.3.3 Características específicas

a) Jerarquía de Normas

(i) Constitución de la República Popular de China, en adelante RPC, (ii) Congreso Nacional del pueblo, (iii) Comité permanente del Congreso Nacional del pueblo, (iv)

[49] Aldama, Z. (2017) El gran salto atrás de China: el bloqueo del internet sin censura que preocupa a los activistas. El diario

Regulaciones administrativas por el Consejo de estado, (v) Regulaciones locales por los ministerios del Consejo de estado y otros organismos autorizados.

b) Legislación

Constitución de la República Popular de China 1982

Capitulo II, artículos 33 al 56, establecen los derechos y deberes fundamentales de los ciudadanos. Merecen especial atención los artículos: 35 libertad de palabra y prensa, 38 dignidad personal, 39 inviolabilidad domicilio, 40 libertad y secreto de correspondencia (violable en caso de seguridad del estado), 51 no perjudicar los intereses del Estado[50].

Leyes Penales

Séptima Enmienda a la ley penal 2009 del Comité Permanente de la Asamblea Popular Nacional, en adelante SC-NPC: (i) *Delito*: cuando cualquier miembro del personal de un órgano estatal o entidad relacionada, venda o proporcione ilegalmente información personal sobre los ciudadanos, obtenida o robada en el desempeño de los deberes. (ii) *Divulgación o venta de información personal:* Ninguna organización o individuo puede robar o adquirir ilegalmente de un ciudadano sus datos personales de internet, o proporcionar esa información a terceros.

Principios Generales del derecho civil 1986

Protege, entre otras cosas, un *derecho de reputación*; «la personalidad de los ciudadanos estará protegida por la ley, y se prohibirá el uso de insultos, injurias u otros medios que dañen la reputación de los ciudadanos o de las personas jurídicas»[51]. Pero el derecho a la privacidad y protección de datos no había sido abordado ni mencionado específicamente. En consecuencia, una resolución judicial de 2001 incluye la invasión a la privacidad junto con la difamación en conformidad a la ley civil. También es relevante una resolución del 2000 (NPCS 2000) que especifica que incursión en responsabilidad civil hay si se infringe a través de internet los derechos legítimos de otra persona constituyendo un daño. Según el artículo 120 de la Ley Civil, permite a los demandantes reclamar una indemnización

[50] Constitución de la República Popular de China de 1982

[51] Principios Generales de la Ley Civil China 1986

por daño moral, el cese de la infracción, una disculpa pública y la corrección de las declaraciones difamatorias para restablecer la reputación y erradicar los efectos nocivos[52].

Ley de responsabilidad civil 2010

El derecho a la privacidad ha sido protegido directamente desde que la ley de responsabilidad civil entró en vigor el 1 de julio de 2010[53].

a) ***El artículo 2 de esta ley protege el derecho a la intimidad,*** entre otros derechos e intereses de carácter civil. Sin embargo, la ley no proporciona una definición de privacidad, ni está diseñada para proteger los datos personales o el derecho al olvido. «Los que infrinjan los derechos e intereses civiles estarán sujetos a la responsabilidad por daños y perjuicios de conformidad con la ley, donde la *privacidad* está incluida en la lista de derechos e intereses civiles protegidos».
b) ***El artículo 36 recoge el procedimiento de «notificación y supresión» para los ISP.*** Estipula claramente que «un proveedor de servicios de Internet (ISP) será responsable de forma conjunta y solidaria por los daños cometidos por el usuario/s de su servicio de Internet si el proveedor de servicios de internet (ISP) no sigue los procedimientos de *notificación y supresión* que brindan protección para este. Para disfrutar de la protección, una vez que una víctima de agravio tiene un servidor para el ISP con respecto a los agravios o cuando el ISP tiene conocimiento del contenido ilícito, el ISP debe cumplir con las reglas esenciales de responder de manera oportuna y debe tomar las medidas necesarias para eliminar o desvincular el contenido dañino»
c) ***Artículo 15: Recursos jurídicos para las víctimas***. Incluye el cese de información y la erradicación de efectos nocivos. Si un ISP no sigue los procedimientos de *notificación y supresión* estipulados en el artículo 36 y se considera responsable por la invasión a la privacidad, el perjudicado puede acogerse al artículo 15 para exigir que el ISP elimine, bloquee o desvincule el contenido perjudicial.

Ni la ley de responsabilidad civil extracontractual ni la resolución judicial de 2014 aclaran si el significado de «ISP» incluye o no a los motores de búsqueda.

[52] Ning Yan, M. (2105) Protecting the Right to be Forgotten: Is Mainland China Ready. European Data Protection Law Review, pág 258

[53] Ley de Responsabilidad China de 2010

Interpretación judicial (2014) del CCP:

El Partido Comunista de China emitió una interpretación judicial en octubre de 2014 sobre las actuaciones en internet que infringen los derechos personales para proporcionar orientación a los tribunales de China en sus resoluciones.

a) De los *artículos 6 y 9* se puede concluir que, (i) el término «ISP» posiblemente también incluya motores de búsqueda; (ii) los motores de búsqueda, aunque no editan ni modifican la información en la red, sí seleccionan, organizan, clasifican o incluso recomiendan resultados de búsqueda; (iii) los motores de búsqueda pueden ser tratados de manera diferente a otros ISP debido a la naturaleza de sus servicios. Pero la Interpretación Judicial 2014 no estipula claramente las responsabilidades de los motores de búsqueda.
b) El *artículo 12* «proporciona una mayor protección y más clara contra un daño derivado de la divulgación de datos personales en internet, pero no ofrece una protección completa de los datos personales con relación a la recopilación, el uso y el almacenamiento, etc. Un ISP eliminará el contenido ilícito de la siguiente manera: (i) siguiendo voluntariamente los procedimientos de notificación y supresión establecidos por el artículo 36 de la Ley de responsabilidad extracontractual o (ii) cumpliendo con las órdenes judiciales sobre los hallazgos de contenido por parte del tribunal que el contenido de internet en cuestión viole el artículo 12 de la interpretación Judicial 2014»

Sin embargo, sigue sin estar claro si los motores de búsqueda están obligados a bloquear o eliminar el contenido en cuestión.

Derecho público

El *artículo 42.6* de la Ley de Sanciones Administrativos del Orden Público, en adelante LAPO, castiga ciertos actos como la divulgación de datos privados de otra persona. La policía puede multar o detener, sin un tribunal de primera instancia, a los usuarios de Internet que violen la privacidad de otras personas en la red. La difusión de contenido ilegal puede generar advertencias, multas, suspensiones o revocaciones de las licencias de ISP. El personal de administración del ISP puede ser considerado personalmente responsable por los delitos cometidos. Según el artículo 7 de la Sentencia NPCSC de 2000, una vez que se detecta información ilegal y dañina en internet, los ISP deben

detener la transmisión e informar a las autoridades. Es aplicable a todos los ISP, incluidos los motores de búsqueda.

Este método puede ser más eficaz que la interposición de acciones civiles por los ciudadanos.

Resolución 2012 NPCSC

Regula la *recolección, uso, divulgación y almacenamiento* de información electrónica con el fin de reforzar la protección de la información electrónica relativa a los datos personales y la privacidad[54].

(i)*El artículo 5* rige el deber de los ISP de proteger la privacidad en línea y datos personales, de tal forma que deben detener y eliminar la transmisión de información prohibida, mantener un registro y denunciarlo a las autoridades. (ii) *El artículo 8* especifica el derecho a solicitar la acción del ISP, es decir, que borre o tome las medidas necesarias para detener la difusión, siempre y cuando se trate de datos reveladores de identidad o que causen daño. (iii) *El artículo 11* enumera una serie de sanciones como: «advertencias, multas, confiscación del producto, revocación de la licencia, cancelación del registro y cierre de los sitios Web. El personal de ISP a cargo puede ser expulsados por infringir la ley. También pueden incurrir en sanciones civiles». Esto se combina con el borrado de dichos datos. Los perjudicados puede ejercer, bajo esta directiva, su *derecho a desindexar*.

«Las regulaciones rigen principalmente a los operadores de telecomunicaciones e ISP en su recopilación y uso de datos personales de sus clientes y no otorga a los clientes el derecho de acceder o borrar sus datos personales».

Directrices 2013

Establecen estándares que deben seguir los controladores con relación a la recopilación, procesamiento, transferencia y borrado de datos personales.

Por ejemplo, el *artículo 5.5.1* establece que: (a) el controlador de datos debe eliminar los datos personales si se ha solicitado de forma legítima por un usuario; y (b) el controlador de datos debería recurrir a medidas apropiadas de almacenamiento y bloqueo si la

[54] Resolución del NPCSC sobre el fortalecimiento de la protección de la información de la red (promulgada y en vigor desde el 28 de diciembre de 2012)

eliminación afectara la recopilación de pruebas por parte de los organismos encargados de hacer cumplir la ley.

Podemos entender que un sujeto tiene derecho a solicitar el borrado de sus datos personales, lo cual, aparentemente, también se aplica a los datos personales mostrados como resultados por los motores de búsqueda[55].

Ley de ciberseguridad 2017

La nueva Ley de ciberseguridad china, en adelante CSL, promulgada el 7 de noviembre de 2016, entró en vigor el 1 de junio de 2017. Caben destacar los estrictos requisitos de la Ley, el lenguaje ambiguo y la falta de claridad en cuanto al plan de implementación. La Administración del Ciberespacio China, en adelante ACC, modificó el lenguaje empleado en ciertas partes de la Ley y retrasó la implementación de las provisiones transfronterizas de localización de datos hasta el final de 2018[56].

La agencia oficial de noticias Xinhua publicó que la ley se aprueba con el fin de «controlar, defender y gestionar los riesgos de ciberseguridad y las amenazas que procedan de dentro del país o del extranjero, protegiendo la infraestructura de información clave de ataques, intrusiones, alteraciones y daños». No obstante, la ley termina, a su vez, con los derechos y libertades de los ciudadanos chinos en Internet, prohíbe el anonimato y el uso de pseudónimos, obliga a los usuarios a dar su nombre real, exige a las redes sociales y servicios online que pidan el nombre real de los usuarios y sanciona a todos aquellas personas que critiquen al Gobierno[57].

i. Datos personales

La ACC aclaró que los *datos importantes* serán evaluados como datos importantes desde la perspectiva del estado, en lugar de la perspectiva de una empresa o individuo.

[55] Tecnología de seguridad de la información - Directrices sobre protección de datos personales de los sistemas de información de los servicios públicos y comerciales (promulgadas por la Administración General de Supervisión de la Calidad, Inspección y Cuarentena; y la Administración de Normalización de la República Popular China, 5 de noviembre de 2012, en vigor desde el 1 de febrero de 2013.

[56] Mariscal, S. (2016) China prohíbe el anonimato en internet con una nueva ley de ciberseguridad

[57] 20minutos (2017) China pone en marcha una ley de ciberseguridad que obliga a almacenar datos en su territorio

En el borrador de las Directrices para la evaluación de la seguridad de las transferencias transfronterizas publicada el 27 de mayo de 2017, datos importantes se define ampliamente como datos que pueden «influir o perjudicar al gobierno, el estado, las fuerzas armadas, la economía, la cultura, la sociedad, la tecnología, la información, etc., así como otros asuntos de seguridad nacional». Los departamentos pertinentes del gobierno tendrán la responsabilidad de clarificar los detalles de lo que se considerará como *datos importantes* dentro de su industria[58].

ii. Obligaciones de los operadores de infraestructuras de información crítica y operadores de red.

Esta ley sí impone ciertas obligaciones a los operadores de infraestructuras de información crítica, en adelante CIIs y operadores de red.

En términos generales podríamos decir que cumplen con estas funciones: (i) Localización de datos, (ii) Restricciones a las transferencias de datos transfronterizas, (iii) Cumplimiento y certificación de medidas de seguridad, (iv) Verificaciones de identidad del *mundo físico*, (v) Detener la divulgación pública ilegal de información transmitida por los usuarios, (vi) Aplicación por la ACC[59].

Podemos encontrar las obligaciones impuestas en estos artículos:

- Artículo 43: Cuando una persona descubre que los operadores han violado las disposiciones legales en materia de protección de datos, tienen el derecho de solicitar a los operadores de la red que eliminen / bloqueen su información personal[60].
- Artículo 50 estipula que, a fin de resguardar la seguridad nacional y el orden público, y responder a importantes incidentes de seguridad social, el Consejo de Estado, o los gobiernos de las provincias, regiones autónomas y municipalidades

[58]Chipman, A. (2018) La nueva Ley de ciberseguridad china: se anuncian aclaraciones y retraso en la ejecución. China Briefing

[59] Zhang,J. (2015) China legaliza el gran cortafuegos: Nueva ley de seguridad infórmatica codificará la censura y los bloqueos. GlobalVoices

[60] Artículo 43 de la Ley de Ciberseguridad China 2017.

con la aprobación del Consejo de Estado, pueden adoptar medidas temporales sobre la comunicación por internet dentro de ciertas regiones, como restringirla[61].

- Artículo 40, obliga a los proveedores y plataformas de servicios de internet a vigilar activamente toda actividad de los usuarios y borrar los contenidos que estén prohibidos por ley a fin de prevenir que se difunda tal información[62].
- Artículo 57, establece de manera explícita que el no prevenir la difusión de información ilegal será sancionado con advertencias, multas e, incluso, órdenes de clausura[63].
- Artículo 23, Las autoridades pueden, además, obtener la ayuda de operadores de red con motivo de la seguridad nacional y la detección de delitos[64].
- Artículo 31, se puede consolidar el poder de la dirección central de la Administración del Ciberespacio para administrar, coordinar y supervisar los asuntos del ciberespacio, desde vigilar y censurar los contenidos web hasta evaluar y autorizar el almacenamiento y transferencia al exterior de la información personal de los ciudadanos chinos[65].
- El artículo 20 establece que «los operadores de red deberán solicitar a los usuarios que brinden la información real de su identidad al firmar acuerdos de servicios para asegurar la rastreabilidad de sus actividades y contenidos de internet. Si los usuarios no brindan los datos reales, los operadores de red deberán negarles los servicios solicitados»[66].
- Las cláusulas 34-36 rigen los deberes de los ISP en su recopilación, uso y almacenamiento de datos personales de los ciudadanos[67].
- La cláusula 37 estipula los derechos de cancelación, indicando que, «si un ciudadano encuentra que un ISP ha recopilado o utilizado sus datos personales en

[61] Artículo 50 de la Ley de Ciberseguridad China 2017.

[62] Artículo 40 de la Ley de Ciberseguridad China 2017.

[63] Artículo 57 de la Ley de Ciberseguridad China 2017.

[64] Artículo 23 de la Ley de Ciberseguridad China 2017.

[65] Artículo 31 de la Ley de Ciberseguridad China 2017.

[66] Artículo 20 de la Ley de Ciberseguridad China 2017.

[67] Artículos del 34 al 36 de la Ley de Ciberseguridad China 2017.

violación de las leyes y regulaciones o el acuerdo entre el ciudadano y el ISP, el ciudadano tiene el derecho de solicitar el borrado de los datos personales»[68].

Derecho al olvido en China

En mayo de 2016, los tribunales chinos de Pekín determinaron que sus ciudadanos no tienen derecho al olvido cuando un juez dictaminó a favor de Baidu en una demanda por la eliminación de los resultados de la búsqueda, y fue el primer caso sobre el *derecho al olvido* que se presentó ante un tribunal en China. Ren argumentó que al publicar los resultados de la búsqueda, Baidu había violado su derecho al nombre y a la reputación, ambos protegidos por la ley china. Debido a estas protecciones, Ren creía que tenía derecho al olvido y a eliminar los resultados de la búsqueda. El tribunal falló en contra de Ren, alegando que su nombre es una colección de caracteres comunes, y que los resultados de la búsqueda fueron extraídos de palabras relevantes y de alta frecuencia que el motor de búsqueda encontró automáticamente[69].

Wei Yongzheng, profesor jubilado de la Academia de Ciencias Sociales de Shanghai y experto en derecho de los medios de comunicación, dijo a Sixth Tone que China tiene algo parecido al *derecho de supresión.* «Si los ciudadanos descubren que se revela su identidad personal, se divulga información privada, o si se encuentra en Internet otra información que invade sus derechos legales, tienen derecho a solicitar al proveedor del servicio de red que borre la información pertinente»

[68] Artículo 37 de la Ley de Ciberseguridad China 2017.

[69] Jubb, N. (2016) China no tiene derecho al olvido. Sixth Tone

4. SUPUESTO PRÁCTICO

4.1 Google Spain (C-131/12) TJUE

4.1.1 Hechos

El litigio fue planteado por la Audiencia Nacional, a raíz de una denuncia interpuesta ante la Agencia Española de Protección de Datos (AEPD) por un ciudadano español llamado Mario Costeja González, que denunció que un periódico nacional había publicado dos anuncios relativos a una subasta de inmuebles relacionada con un embargo ocasionado por una deuda contraída con la Seguridad Social hace 17 años. Esta deuda se resolvió en su momento y perdió su relevancia. Efectuando así su derecho a solicitar que Google elimine u oculte su información personal, con relación a los procedimientos de esta deuda, mostrada en los resultados de búsqueda al introducir su nombre[70].

4.1.2 Fundamento

Tras analizar varios artículos y la sentencia podemos sacar varios puntos en claro[71]. Esta Sentencia trae como causa la cuestión prejudicial de interpretación al TJUE planteada por la Sala de lo contencioso-administrativo de la Audiencia Nacional (Auto, Secc 1a, 27-02-12, Rec 725/2010), en la que suscitaba diferentes dudas en torno a la correcta interpretación y aplicación que debería de recibir el derecho de cancelación de datos personales que apareciesen en los listados de un motor de búsqueda.

Por lo tanto, al hablar del derecho de cancelación, nos estamos refiriendo al llamado *derecho al olvido*.

1. Primeramente, la sentencia reconoce la sujeción de Google a la normativa europea, y en concreto a la española, por tener un establecimiento abierto en España.

2. Nos encontramos con una colisión de derechos, ya que el derecho al olvido está limitado como veíamos anteriormente. Esto significa que, por un lado, debemos

[70] Sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317

[71] Córdoba, D. (2014) El "derecho al olvido" tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Revista de Jurisprudencia; Martínez, JM. (2016) La aplicación del derecho al olvido en España tras la STJUE, Google contra AEPD y Mario Costeja

proteger los derechos fundamentales como el de respeto a su vida privada y derecho a la protección de sus datos personales del afectado Mario Costeja González; y por el otro, nos limita el derecho a la libertad de expresión del editor y derecho a la información. Esto último quiere decir que, la eliminación de los datos o su desvinculación de la lista de resultados podría afectar a los derechos de las personas interesadas en acceder a esta información. El Tribunal afirma que es necesario buscar cierto equilibrio entre ambos derechos colisionados. Este equilibrio puede depender en casos particulares de «la naturaleza de la información de que se trate, de lo delicada que ésta sea para la vida privada de la persona de que se trate y del interés del público en disponer de esa información, que puede variar, en particular, en función del papel que esa persona desempeñe en la vida pública». Aún así, el Tribunal señala que, por regla general, prevalecen los derechos de la persona afectada sobre los derechos de los internautas.

3. Otorga la responsabilidad del tratamiento a los motores de búsqueda, por lo que se reconoce el derecho a la cancelación y supresión de los datos personales en cuestión por haber sido suministrada por los motores de búsqueda al considerar que esta información «puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo».

4. El TJUE considera que este derecho puede ejercitarse frente al motor de búsqueda sin solicitar previamente la cancelación al editor. En caso de que el responsable del tratamiento no acceda a lo solicitado, la persona afectada podrá acudir a las

autoridades (Tribunales) con el fin de que estos mismos lleven a cabo las comprobaciones precisas y ordenen al responsable que adopte las medidas necesarias.

5. El Abogado general señala que los «procedimientos de detección y retirada» recogidos en la Directiva 2000/31/CE, sobre el comercio electrónico -EDL 2000/87907-, están relacionados con los contenidos ilegales, pero en el marco del presente asunto nos enfrentamos a una solicitud de eliminación de información legítima y legal que se ha hecho pública[72].

   El TJUE señala que, «con el tiempo, incluso un tratamiento inicialmente lícito de datos exactos puede llegar a ser incompatible con la Directiva cuando, habida cuenta de todas las circunstancias que caractericen cada caso, esos datos se revelen inadecuados, no pertinentes o excesivos desde el punto de vista de los fines para los que fueron tratados y del tiempo transcurrido».

   En este caso la publicación del procedimiento de embargo de Mario Costeja González era totalmente lícita, pero pasados 17 años y con la deuda resuelta, no es oportuno que esta información siga estando visible en la red si le está causando perjuicios, mala imagen y afectando a su reputación. Por lo tanto, esta información que en principio era lícita, a devenido ilícita por su impertinencia, largo transcurso en el tiempo y factor perjudicial.

4.1.3 Conclusiones

En resumen, nos encontramos en una situación en la que se quieren eliminar unos datos personales en Google Spain, empresa que ofrece servicios en todo el mundo, pero al tener establecimiento en España se encuentra dentro del ámbito de aplicación de la (i) normativa europea. Se le otorga la (ii) responsabilidad al motor de búsqueda y no al editor porque se considera fundamental el trabajo del motor para la difusión de estos datos, y es realmente esta difusión la que causa el daño. Los datos en cuestión es información legítima y legal, pero llegan a la conclusión que puede (iii) devenir ilegal por el largo transcurso del tiempo convirtiéndose esta información en inadecuada, no pertinente y excesiva. Por último, nos encontramos con una (iv) colisión entre los derechos a la

[72] Tribunal de Justicia de la Unión Europea. Comunicado de Prensa Nº 2/19. Conclusiones del Abogado General en el asunto C – 507/17

libertad de expresión y acceso a la información, y los derechos fundamentales del afectado Mario Costeja González, lo cual debe solucionarse, según el Tribunal, con una ponderación de derechos. Aún así los derechos fundamentales del afectado, por regla general, siempre prevalecen ante el derecho a la información y libertad de expresión.

Esta sentencia confirmó que los usuarios tienen un nuevo derecho a *desindexar*, es decir, eliminar de la lista de resultados unos enlaces a páginas web, con datos personales controvertidos, a los que se redirige tras efectuar una búsqueda con su nombre.

Gracias a este caso se han sentado unas bases para el desarrollo legal y jurisprudencial del derecho al olvido, como manifestación del derecho de oposición y cancelación de datos personales en Internet.

A raíz de esto, se han producido multitud de solicitudes de eliminación de datos a los principales buscadores de Internet, en especial Google, los cuales se resuelven aplicando los criterios sentados por esta sentencia del TJUE.

El problema fue que el Tribunal no abordó el alcance territorial de las medidas relativas a la supresión de datos personales. La sentencia -EDJ 2014/67782- razona al respecto que «(...) habida cuenta de la facilidad con que la información publicada en un sitio de Internet puede ser copiada en otros sitios y de que los responsables de su publicación no están siempre sujetos al Derecho de la Unión, no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet».

Deja claro que la «decisión de cancelación o supresión de tales datos frente al buscador no presupone que los mismos sean eliminados con carácter previo o simultáneamente de la página web en la que han sido publicados, por lo que la supresión de los datos dependerá de los derechos que invoque la persona o entidad frente a la que se ejercita, pues no tendrán la misma intensidad ni idéntica protección».

Es decir, gracias a la sentencia de Google Spain disfrutamos de un nuevo derecho a desindexar, pero esta desindexación conlleva la eliminación de la dirección web de una lista de resultados, no la eliminación de esta página web, sus datos, o la publicación de

estos datos en otras páginas web u otras partes del mundo. Lo que significa que la información sigue existiendo.

Consecuentemente surgen unas cuestiones sin resolver, ¿No deberían estas medidas tener un alcance a nivel mundial para que sea totalmente efectivo?; Si hablamos de un estado miembro, ¿debe alcanzar a todos los miembros de la Unión, o solo el país en cuestión? ¿Puede existir algún efecto extra transfronterizo?...

No existe respuesta por parte de tribunales a estas respuestas, pero actualmente están siendo discutidas en el caso c-507/17 que analizaré a continuación.

4.2 Google/CNIL (C-507/17) TJUE

4.2.1 Hechos

Este asunto tuvo su origen, en una resolución de 21 de mayo de 2015 de la presidenta de la autoridad francesa de protección de datos, la *Commision nationale de l'informatique et des libertés*, en adelante CNIL, una persona física al hacer una búsqueda con su nombre en Google, le dirigía a unas páginas de internet que no consideraba adecuadas[73]. Esta persona solicitó a Google la supresión respecto de todas las extensiones de dominio de su motor de búsqueda.

Google se negó a atenerse a este requerimiento y se limitó a suprimir los vínculos en cuestión exclusivamente de los resultados mostrados como respuesta a las búsquedas efectuadas desde los nombres de dominio correspondientes a las extensiones de su buscador en los Estados miembros de la Unión Europea.

Por otra parte, la CNIL consideró insuficiente la propuesta complementaria denominada de «bloqueo geográfico» presentada por Google tras la expiración del plazo de requerimiento, que consistía en eliminar la posibilidad de acceder desde una dirección IP (Internet Protocol) que se presuma esté localizada en el Estado de residencia de la persona interesada a los resultados controvertidos obtenidos como consecuencia de una búsqueda

[73] Sentencia de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU:C:2014:317.

realizada a partir de su nombre, independientemente de la extensión del motor de búsqueda solicitada por el internauta[74].

Tras constatar que Google no se había atenido a dicho requerimiento en el plazo establecido, la CNIL, mediante resolución de 10 de marzo de 2016, le impuso una sanción, que se hizo pública, de 100.000 euros.

Mediante demanda presentada ante el *Conseil d'État* francés, órgano que actúa como Tribunal Supremo de lo Contencioso-Administrativo en ese país, Google solicitó la anulación de esta resolución.

4.2.2 Cuestiones prejudiciales

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 2014sobre la base de las disposiciones de los artículos 12, letra b), y 14, letra a), de la Directiva de 24 de octubre de 1995 [75], 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?»

   Por lo tanto, tal y como aclara Diego Córdoba, «la pregunta es si el derecho al olvido previsto en la legislación europea sobre protección de datos implica la obligación del responsable del buscador de retirar los enlaces controvertidos (en las búsquedas realizadas a partir del nombre del solicitante) de los resultados de todas las versiones de su buscador en el mundo, de tal manera que los vínculos controvertidos dejen de mostrarse en todo el mundo»[76].

[74] Coex International Trade (2019) El alcance del derecho al olvido debe limitarse al ámbito de la Unión Europea

[75] 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 (DO 1995, L 281, p. 31).

[76] Córdoba, D. (2014) El "derecho al olvido" tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Revista de Jurisprudencia

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?»

   Por lo tanto, tal y como aclara Diego Córdoba, «el Conseil d'État plantea si el responsable del buscador solamente está obligado a suprimir los vínculos controvertidos en la versión del buscador bajo el nombre de dominio correspondiente al Estado en el que se considera que se ha efectuado la solicitud de retirada o bajo los nombres de dominio del buscador que corresponden a las extensiones nacionales del conjunto de los Estados miembros de la Unión».

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?»

   Por lo tanto, tal y como aclara Diego Córdoba «Plantea si el responsable del buscador debe aplicar medidas de geolocalización para que los enlaces controvertidos no se muestren cuando se acceda al buscador desde una dirección IP localizada en el Estado

de residencia del beneficiario del derecho al olvido o en cualquiera de los Estados de la UE».

Este asunto todavía no está resuelto, sigue pendiente de la sentencia del Tribunal. Veamos las diferentes posturas que se discuten[77]:

1. El Abogado General defiende que «la desindexación (*déréférencement)* a la que han de proceder los gestores de motores de búsqueda ante el ejercicio del derecho al olvido se limita a la Unión Europea, pues las disposiciones del Derecho de la Unión no deben interpretarse de forma tan amplia que produzcan efectos más allá de las fronteras territoriales de los Estados miembros».

   Rechaza la aplicación de las medidas de supresión tengan un alcance mundial, de tal forma que no se pueda acceder a dicha información desde ninguna parte del mundo.

a) Aún así, el abogado general entiende la posible existencia de excepciones por las cuales sí pueda obligarse al motor de búsqueda la realización de una desindexación o una medida en base al derecho al olvido a escala mundial.

b) La desindexación a escala mundial aparte de ser prácticamente imposible llevarla a cabo, acarrearía una serie de dificultades y conflictos[78].

   i) Anteriormente, en el caso Google Spain, mencionábamos la ponderación necesaria para poder equilibrar la confrontación del derecho a acceder a la información y el derecho fundamental del olvido. La Unión Europea no tiene la capacidad para realizar esta ponderación a escala mundial ya que el (1) interés del público en acceder a la información variará obligatoriamente según su localización geográfica, por ejemplo, de un tercer Estado a otro. Esta

[77] Tribunal de Justicia de la Unión Europea. Comunicado de Prensa Nº 2/19. Conclusiones del Abogado General en el asunto C – 507/17. Google / CNIL, de 10 de enero de 2019

[78] Padova, Y. (2019) ¿Es el derecho al olvido universal, regional o "glocal"? International Privacy Law, Volumen 0, Artículo 1.

ponderación se subordina a la importante (2) exigencia de vínculos de conexión suficiente con la Unión Europea para poder limitar el ejercicio del derecho al olvido ante autoridades europeas.

ii) En caso de poder llevar a cabo esta desindexación mundial, lo cual conlleva impedir el acceso a cierta información a personas de terceros Estados, se produciría el mismo caso recíprocamente. Estarían capacitados, en consecuencia, estos terceros Estados a bloquear el acceso a la información que ellos consideren a personas de Estados miembros.

iii) Otra de las razones sería el criterio de que «el legislador de un territorio no debe regular el contenido de la red en todo el mundo, precisamente por el alcance global de esta y la necesidad de *respetar* la coexistencia de una pluralidad de ordenamientos jurídicos a nivel mundial» (apartado 61 conclusiones sentencia)

iv) Daría lugar a conflictos muy relevantes con relación a decidir la licitud o ilicitud de los resultados que un buscador establecido en un tercer Estado muestra a un usuario.

v) Que un tribunal pueda tener competencia con alcance mundial no implica que las medidas que adopte deban tenerla. Incluso al intentar adoptarlas, puede que las normas de ley aplicable le impongan que aplique normas de otros ordenamientos jurídicos.

2. El Abogado General (i) sí considera que deban tomarse medidas para garantizar la eficacia de la actuación, «una vez establecido el derecho a la desindexación en la Unión, el (ii) gestor de un motor de búsqueda debe tomar todas las medidas a su disposición, incluida la del *bloqueo geográfico*, para garantizar una desindexación eficaz y completa en el territorio de la Unión Europea desde una dirección IP que se presuma esté localizada en uno de los Estados miembros, con independencia del nombre de dominio empleado por el internauta que efectúa la búsqueda». (apartado 74)

3. Hemos comentado que según el Abogado General «no deben interpretarse de forma tan amplia que produzcan efectos más allá de las fronteras territoriales de los Estados miembros» pero realmente sí se está considerando que puedan producir efectos con límites razonables. No en base a bloquear el acceso a personas que se encuentren en terceros Estados, sino, que estos terceros Estados puedan quedar sometidos a la legislación europea en el caso de que una empresa establecida en un tercer estado preste servicios de búsqueda a la Unión Europea, y, por tanto, si ciertos datos personales perjudiciales quedan sometidos al derecho al olvido, el tercer estado en cuestión también quedará obligado pero solo en relación a la información que proporciona a los Estados miembros.

   Ha llegado a comparase, aunque sin éxito, esta situación donde la legislación europea produce consecuencias extraterritoriales con los casos de aplicación de la legislación europea de marcas a los actos de comercialización de productos a través de internet en el extranjero, pero dirigido a consumidores dentro de la Unión (ejemplo, sentencia *L'Oréal* de 12 de julio de 2011)[79]

4.2.3 Conclusión

Gracias a los servicios que proporcionan los motores de búsqueda, la difusión de información por internet es masiva y llega a cada rincón del mundo. Por ello es evidente que el rechazo al alcance mundial del derecho al olvido, previsto en la legislación europea, puede impedir la eficacia del derecho fundamental a la protección de datos. Ya que sería tan fácil como realizar la búsqueda a través de quien se encuentre en cualquiera de esos (i) terceros Estados para poder llegar a conocer la información, o incluso, desde el propio territorio *cancelado* pero simplemente desde (ii) otro buscador, el cual no ha sufrido una desindexación[80].

Sin embargo, como hemos podido analizar, existen varias dificultades a la hora de intentar establecer un alcance mundial como que: el interés público varia dependiendo de los Estados; los Estados miembros sufrirían también un bloqueo de acceso a información que

[79] L'Oréal de 12 de julio de 2011. C-324/09. ECLI:EU: C:2011:474

[80] Alcance territorial del derecho al olvido: las conclusiones en el asunto Google/CNIL

los terceros Estados considerasen, ya que sería prácticamente imposible que todos los Estados adoptaran una regulación común sobre qué información se considera adecuada para compartir o no; y la necesidad del respeto a una pluralidad de ordenamientos jurídicos.

Por ello, aparte de que todos los Estados de la unión estén bajo una misma regulación, se propone un alcance limitado a conductas (desde terceros Estados) que producen consecuencias en el territorio de la Unión.

También se debe tomar en consideración la obtención de datos a través de otros buscadores diferentes al que se le solicita la cancelación, ya que por mucho que se lleve a cabo una desindexación en Google, va a seguir siendo accesible, aparte de a través de Google en terceros Estados como decíamos anteriormente a no ser que existan limitaciones, desde la propia Unión pero a través de otros buscadores como Mozilla Firefox, Bing, Yahoo, Youtube, Yandex, Baidu, Ask, Aol, Ecosia, DuckduckGo, Yippy, etc.

Destacaría estos dos puntos, tanto la accesibilidad (i) desde terceros Estados, como la accesibilidad a la información a través de (ii) buscadores diferentes al demandado, puesto que, si no se encuentra una manera de poder limitar estas actuaciones, no estaríamos respetando la tutela efectiva del derecho fundamental a la protección de datos.

4.3 Aplicación de los casos en EE. UU. y en China

Una vez explicadas las principales características de la forma que tiene Europa, Estados Unidos y China de regular la privacidad de datos, ¿Qué habría pasado si las cuestiones planteadas en los casos anteriores hubieran sucedido, en Estados Unidos o en China, en vez de en Europa?

Situémonos en el supuesto de que un estadounidense o un chino hubiera solicitado la eliminación de datos personales legales en la red justificando que están obsoletos y no son de interés público pero que su visibilidad le está causando un perjuicio.

Estados Unidos

Como vimos anteriormente, cada estado en los EE. UU. regula de forma diferente la privacidad de datos, pero ninguno de ellos tiene reconocido un *derecho al olvido*.

a) Lo más parecido lo encontramos en California donde sí existe el *derecho de supresión* pero solo empleado a menores y sobre información publicada por ellos mismos, por lo que en este caso no tendría efecto.
b) En los EE. UU. también se discute la confrontación de los derechos fundamentales de las personas con respecto a su privacidad frente al derecho de libertad de expresión y acceso a la información recogido en la Primera Enmienda. Se han dado una serie de casos de la Corte Suprema similares al de Google Spain como, por ejemplo: Cox Broadcasting v. Cohn, 420 U.S. 469 (1975), Smith v. Daily Mail, 443 U.S. 97 (1979), Florida Star v. BJF, 491 U.S. 524 (1989), y Bartnicki v. Vopper 532 U.S. 514 (2001). Estos casos junto con jurisprudencia apoyan que será difícilmente sancionada penal o civilmente la publicación de información incluso siendo falsa o difamatoria. En nuestro supuesto la información es totalmente verdadera, por lo que, basándonos en lo anterior, no se reconocería el derecho a eliminarlo.
c) Además, la Ley de Decencia en las Comunicaciones prohíbe las reclamaciones contra los motores de búsqueda basadas en su vinculación con material supuestamente ilícito, incluyendo tanto la solicitud de eliminación como las medidas cautelares. Los proveedores de servicios de internet podrían eliminar voluntariamente los enlaces si se presenta una orden que declare la ilicitud del contenido, pero los tribunales no les obligan a hacerlo.

Por lo tanto, si es tan complicado que se falle a favor de afectados por difamación, mucho más complicado será resolver a favor cuando: la información en cuestión es legal, verdad, el perjudicado no es menor de edad ni publicó él esta información, y además está prohibido reclamar a los motores de búsqueda.

Por último, con relación al alcance territorial, en el caso de que se reconociera en algún estado, sería muy complicado que pudiera tener efecto en otros Estados ya que como hemos visto, cada uno se regula de manera diferente. Además de que consideran que este alcance podría ir en contra de la Constitución de los Estados Unidos.

China

Si analizamos el supuesto en China debemos partir de la consideración de que todo funciona en base al interés del Estado.

a) Como hemos visto anteriormente el concepto de *datos personales* según la ACC y Medidas para la evaluación de la seguridad de las transferencias transfronterizas como los que pueden «influir o perjudicar al gobierno, el estado, las fuerzas armadas, la economía, la cultura, la sociedad, la tecnología, la información, etc., así como otros asuntos de seguridad nacional».
b) En China no se respeta el derecho a la libertad de expresión ni acceso a la información ya que tienen toda la red, sistemas informáticos de empresas que contengan datos y los medios de comunicación totalmente controlados y censurados. El Estado decide que información se pública y lleva un control absoluto de todos los datos privados de los ciudadanos. Incluso la nueva ley de ciberseguridad 2017 «prohíbe el anonimato y el uso de pseudónimos, obliga a los usuarios a dar su nombre real, exige a las redes sociales y servicios online que pidan el nombre real de los usuarios y sanciona a todos aquellas personas que critiquen al Gobierno».
c) Según la LAOP la difusión de contenido ilegal puede generar advertencias, multas, suspensiones o revocaciones de las licencias de ISP. En nuestro caso la información no era ilegal por lo que no aplicaría.
d) Sin embargo, el artículo 5.5.1 de las Directrices de 2013, da a entender que un sujeto tiene derecho a solicitar el borrado o desvinculación de sus datos personales, lo cual, aparentemente, también se aplica a los datos personales mostrados como resultados por los motores de búsqueda.
e) La resolución 2012 NPCSC, rige el deber de los ISP de proteger los datos personales en internet y que elimine o tome las medidas necesarias para detener la difusión ilegal de estos datos si está causando daño. (artículos 5, 8 y 11).
f) Está reconocido el derecho a la reputación de las personas (honor), por lo que si consideramos este caso como una violación al honor podría ejercitarse acción civil. Otra cuestión es si los Tribunales lo reconocerían como tal.

Por lo tanto, con este último punto podemos entender que los ciudadanos tendrían un derecho parecido al de olvido pero sin estar reconocido como tal. La regulación China solo en este aspecto puede acercarse más a la europea en su *proteccionismo*. Aunque en nuestro supuesto, la información y forma de publicación era totalmente legal, por lo que

sería más complicada su supresión. Por otro lado, como también hemos visto, el gobierno tiene un control absoluto de toda la información que se emite y recibe, incluidos los datos privados de sus ciudadanos, por lo que, lo procesa y censura (en China) en base a su propio interés, aunque tenga que pasar por encima a los derechos fundamentales de las personas.

5. CONCLUSIONES

En este trabajo he querido realizar un análisis comparativo de las diferentes regulaciones en materia de protección de datos, de una manera general en cuanto a las características y de otra un poco más específica en términos del derecho al olvido, y más aún en el marco europeo.

He comenzado definiendo los conceptos de los derechos más relevantes en esta materia debido a que son los que se han reconocido hace relativamente poco de manera oficial en Europa y entre los cuales ha surgido controversia. Por ejemplo, lo que se entiende por *datos personales*, *derecho de oposición al tratamiento*, el *derecho de supresión*, el *derecho a desindexar* que no es la completa eliminación sino solo una desvinculación, *el derecho a la libertad de expresión y acceso a la información* entre otros.

Hemos podido discutir los diferentes puntos de vista en cuanto al reconocimiento de un *derecho al olvido*. Por un lado, es necesario defender los derechos fundamentales de las personas como lo es el derecho a la protección de datos y a la vida privada; y por otro lado, si este derecho se reconoce, puede violar, en cierta medida, el derecho a la libertad de expresión y acceso a información ya que estaríamos *censurando* a los ciudadanos determinada información. Este tema se soluciona haciendo una ponderación de estos derechos según las circunstancias, lo que significa que se lleva a cabo una optimización de derechos.

La Unión Europea tiene la regulación más proteccionista en comparación con los Estados Unidos y China. Hace un año entró en vigor el RGPD, el cual ha sido un gran avance tanto para la seguridad de los ciudadanos de los Estados miembros, como para influenciar al resto del mundo en esta materia. Podemos decir que el régimen de protección de datos ha experimentado una evolución desde ser un mero instrumento regulador, a una política de derechos fundamentales de la UE plenamente desarrollada.

China puede acercarse a ese carácter proteccionista en ciertos aspectos, pero es el territorio más controlador, debido a que sobrepone los intereses del estado a los derechos fundamentales de sus propios ciudadanos, debido a que viola de una manera exorbitante los derechos a la libertad de expresión y acceso a la información a través de la censura de

internet y medios de comunicación. Estados Unidos tampoco reconoce un derecho al olvido al considerarlo contrario al orden público.

Por último, con relación a los conocidos casos de *Google Spain* y *Google/ CNIL*, hemos podido ver como ha nacido este nuevo derecho a eliminar ciertos datos o vínculos de la red si causan daño y ya no son de importancia para el conocimiento público. Pero si esta información ha sido publicada en otro de tantos buscadores o millones de páginas web, no se podrá cumplir la tutela efectiva del derecho ya que esa información siempre podrá ser localizada.

Por todo esto podríamos concluir que:

«Dios perdona y olvida, pero la red nunca olvida»

BIBLIOGRAFÍA

- **Referencias jurisprudenciales**

- Artículo 29 Directriz del Grupo de Trabajo 4/2007 sobre datos personales, 20 de junio de 2007.

- Conseil d´État. Caso: C – 507/17 (CNIL).

- HUNTINX, P. (2015) Dictamen de la Comisión. Disponible en <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiyzLz9gq3hAhVQxIUKHYHgAYQFjALegQIBBAC&url=http%3A%2F%2Fwww.madrid.org%2Frlma_web%2Fhtml%2Fweb%2FDescarga.icm%3FidLegislacion%3D2731%26idDocumento%3D1&usg=AOvVaw0YnDTevoWlX-e00tCUjzjJ> [consulta: 17 marzo 2019].

- Orden Ejecutiva de la Casa Blanca (2017) Mejorando la Seguridad Pública en el Interior de los Estados Unidos, Nº 13768, 25 enero [en línea] disponible en <https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/> [consulta: 19 de marzo 2019].

- Orden Ejecutiva de la Casa Blanca (2017) Memorándum de Orientación de la Política de Privacidad, Nº 1, 25 abril [en línea] disponible en <https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf > [consulta: 19 de marzo 2019].

- Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea (2007/C 306/C1).

- Tribunal de Justicia de la Unión Europea. Comunicado de Prensa Nº 2/19. Conclusiones del Abogado General en el asunto C – 507/17. Google / CNIL, de 10 de enero de 2019.

- Tribunal de Justicia. Caso: C-131/12 – Google Spain, sentencia de 13 de mayo de 2014.

- Tribunal de los Estados Unidos para el Distrito Este de Pensilvania. Caso: Gorman vs. Steinborn, Nº 2:14-cv-00890-NS, sentencia de 20 d mayo de 2015.

- Tribunal Supremo de Estados Unidos. Caso: Katz vs. Estados Unidos, 389 U.S. 347, sentencia de 18 de diciembre de 1967.

- **Referencias doctrinales**

- BYGRAVE, LEE A. (2014) Data Privacy Law, an International Perspective, págs. 53 – 116. Oxford University Press.

- DE TERWANGNE, C. (2012) Internet Privacy and the Right to be forgotten/Right to Oblivion, págs. 109-121.

- KUNER, C. (2017) The internet and the global Reach of EU Law, págs. 52-85

- LYNSKEY, O. (2015) The Foundations of EU Data Protection Law, págs. 15 – 45.

- NIEVES, M. (2011) El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego, págs. 280 – 289. (tesis doctoral) Huelva

- NING YAN, M. (2105) Protecting the Right to be Forgotten: Is Mainland China Ready. European Data Protection Law Review, págs. 190 – 205.

- PADOVA, Y. (2019) ¿Es el derecho al olvido universal, regional o "glocal"? International Privacy Law, Volumen 0, Artículo 1.

- WALKER, R. (2012) The Right to be forgotten, pág. 257. 64 Hastings Law Journal.

- **Artículos periodísticos**

- 20MINUTOS (2017) China pone en marcha una ley de ciberseguridad que obliga a almacenar datos en su territorio [en línea] disponible en <https://www.20minutos.es/noticia/3052493/0/china-pone-marcha-ley-ciberseguridad-obliga-almacenar-datos-territorio/> [consulta: 22 de marzo 2019].

- ALDAMA, Z. (2017) El gran salto atrás de China: el bloqueo del internet sin censura que preocupa a los activistas. El diario [en línea] disponible en <https://www.eldiario.es/desalambre/salto-China-bloqueo-acceso-Internet_0_668433334.html> [consulta: 26 de marzo 2019].

- ASENSIO, P. (2019) Alcance territorial del derecho al olvido: las conclusiones del asunto Google/CNIL [en línea] disponible en <http://pedrodemiguelasensio.blogspot.com/2019/01/alcance-territorial-del-derecho-al.html> [consulta: 16 de marzo 2019].

- CHIPMAN, A. (2018) La nueva Ley de ciberseguridad china: se anuncian aclaraciones y retraso en la ejecución. China Briefing [en línea] disponible en <https://www.china-briefing.com/news/la-nueva-ley-de-ciberseguridad-china-se-anuncian-aclaraciones-y-retraso-en-la-ejecucion/> [consulta: 26 de marzo 2019].

- CLICK DATOS (2016) Diferencias entre el derecho de supresión de datos y el derecho al olvido [en línea] disponible en <https://clickdatos.es/diferencias-entre-el-derecho-de-supresion-de-datos-y-derecho-al-olvido/> [consulta: 14 de marzo 2019].

- COEX INTERNATIONAL TRADE (2019) El alcance del derecho al olvido debe limitarse al ámbito de la Unión Europea [en línea] disponible en <http://www.coexonline.es/el-alcance-del-derecho-al-olvido-debe-limitarse-al-ambito-de-la-union-europea/> [consulta: 16 de marzo 2019].

- COMISIÓN FEDERAL DE COMERCIO (1998) Informe para el Congreso sobre la Privacidad en internet [en línea] disponible en <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> [consulta: 15 de marzo 2019].

- CÓRDOBA, D. (2014) El "derecho al olvido" tras la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014. Revista de Jurisprudencia [en línea], Nº 1. Disponible en < https://elderecho.com/el-derecho-al-olvido-tras-la-sentencia-del-tribunal-de-justicia-de-la-union-europea-de-13-de-mayo-de-2014>[consulta:15 marzo 2019].

- GOLDMAN, E. (2013) La nueva ley de supresión de California debe ser eliminada. Forbes [en línea] disponible en <https://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased/#2007a2e77a33> [consulta: 27 de marzo 2019].

- GRUPO ÁTICO 34 (2018). Derecho al olvido en el RGPD. Blog de Protección de Datos para Empresas y Autónomos [blog] 20 septiembre. Disponible en < https://protecciondatos-lopd.com/empresas/derecho-olvido-rgpd/> [consulta: 18 marzo 2019].

- HEILWEIL, R. (2018) Como de cerca está el derecho al olvido en América [en línea] disponible en < https://www.forbes.com/sites/rebeccaheilweil1/2018/03/04/how-close-is-an-american-right-to-be-forgotten/#765202db626e> [consulta: 27 de marzo 2019].

- HENDEL, J. (2012) Por qué los periodistas no tienen que temer al derecho al olvido en Europa. The Atlantic [en línea] disponible en <https://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/ > [consulta: 15 de marzo 2019].

- IBM KNOWLEDGE CENTER (2017) Informe de la Ley de Privacidad de 1974 [en línea] disponible< https://www.ibm.com/support/knowledgecenter/es/SSW2NF_9.0.1/com.ibm.ase.help.doc/topics/r_privacy_act_1974_report.html> [consulta: 24 marzo 2019].

- JUBB, N. (2016) China no tiene derecho al olvido. Sixth Tone [en línea] disponible en <http://www.sixthtone.com/news/chinese-have-no-right-be-forgotten-court-rules> [consulta: 26 de marzo 2019].

- KEVIN, L. (2014) El derecho al olvido. Media Law Resources Center [en línea] disponible en < http://www.medialaw.org/component/k2/item/3994-the-right-to-be-forgotten> [consulta: 15 de marzo 2019].

- MANIACS (2018) ¿Qué son las Autoridades de Protección de Datos (APD)? [en línea] disponible en < https://www.lopdencastellon.com/que-son-las-autoridades-de-proteccion-de-datos-dpa/> [consulta: 25 marzo 2019].

- MARISCAL, S. (2016) China prohíbe el anonimato en internet con una nueva ley de ciberseguridad [en línea] disponible en <https://www.audea.com/es/china-aprueba-una-polemica-ley-de-ciberseguridad/> [consulta: 26 de marzo 2019].

- MARTÍNEZ, A. (2019) El Supremo obliga a Google a garantizar el derecho al olvido en noticias "erróneas o inexactas". ABC [en línea] disponible en <https://www.abc.es/tecnologia/redes/abci-supremo-obliga-google-garantizar-derecho-olvido-noticias-erroneas-o-inexactas-201901161916_noticia.html> [consulta: 22 de marzo 2019].

- MARTÍNEZ, JM. (2016) La aplicación del derecho al olvido en España tras la STJUE, Google contra AEPD y Mario Costeja. [en línea] disponible en <https://www.redalyc.org/html/4275/427551159004/> [consulta 19 marzo 2019]

- NATTRASS, S. (2017) Orden Ejecutiva de eliminación de la Ley de protección de la Privacidad para los canadienses. Norton Rose Fulbright [en línea] disponible en <https://www.nortonrosefulbright.com/en/knowledge/publications/01bc866e/executive-order-removes-us-iprivacy-acti-protection-for-canadians> [consulta: 27 de marzo 2019].

- PANDA SECURITY (2017) La nueva ley de ciberseguridad china que afectará al resto del mundo [en línea] disponible en <https://www.pandasecurity.com/spain/mediacenter/noticias/china-cyber-security-law /> [consulta: 25 de marzo 2019].

- PURTOVA, N. (2008) The Law of Everything. Broad concept of personal data and future of EU data protection Law, págs. 40 – 81, [en línea] disponible en < https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> [consulta: 19 marzo 2019].

- RAMÍREZ, D. (2017) Ciberseguridad en China. Instituto Español de Estudios Estratégicos [en línea] disponible en <http://www.ieee.es/en/Galerias/fichero/docs_informativos/2017/DIEEEI012017_CyberChina_DRM.pdf> [consulta: 26 de marzo 2019].

- REDONDO, T. (2019) Protección de datos en Estados Unidos: ¿Cómo afecta a tu negocio? Mailjet [blog] 1 febrero. [en línea] disponible en <https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/> [consulta: 27 marzo 2019].

- REEDSMITH (2018) La ley de ciberseguridad China [en línea] disponible en <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=2ahUKEwiC37r_3KrhAhWDzoUKHVVZA6AQFjAGegQIABAC&url=https%3A%2F%2Fwww.reedsmith.com%2F%2Fmedia%2Ffiles%2Fperspectives%2F2018%2Fchinas-cybersecurity-law-002.pdf&usg=AOvVaw00S9ZVyoTtdqjLqJI38C9U> [consulta: 26 de marzo 2019].

- ROSEN, J. (2012) The Right to be Forgotten. Stanford Law Review [en línea] disponible en <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/> [consulta: 22 marzo 2019].

- VELASCO, J. (2017). Derecho de Acceso, Rectificación, Cancelación y Oposición. Big Data ISDE [en línea]. Disponible en

< https://www.casosreales.es/bigdata/ejemplos/Ficha%20de%20Nuevas%20Tecnolog%C3%ADas.pdf> [consulta: 15 marzo 2019].

- VIDAL, M. (2017) La polémica ley de ciberseguridad entra en vigor en China. El País [en línea] disponible en <https://elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.html> [consulta: 26 de marzo 2019].