Daniel Ángel García Tercero

LOS DATOS PERSONALES EN LAS COMUNICACIONES ELECTRÓNICAS

TRABAJO DE FIN DE GRADO

Dirigido por Rosa Barceló Compte

Grado en Derecho

UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2016

“No se trata de tener fe en la tecnología, se trata de tener fe en la gente, porque sabemos que si les das las herramientas adecuadas, las personas son suficientemente inteligentes, para hacer cosas increíbles con ellas”

Steve Jobs

Resumen: En el presente trabajo de fin de grado abordaremos la protección de datos mediante el enfoque de las comunicaciones electrónicas. La tecnología incide de forma global en nuestro catálogo de derechos. Mientras nos comunicamos, proporcionamos información sobre cuentas bancarias, billetes de avión, posición geográfica, etc. Valoraremos por qué es tan importante esa información que generamos, de qué forma está regulada y analizaremos los logros y retos en materia de privacidad.

Palabras clave: Privacidad - Protección de datos – comunicaciones – Seguridad - Derechos Fundamentales de Tercera Generación

Resum: En el present treball de fi de grau, tractarem la protecció de dades per mitjà de l'enfocament de les comunicacions electròniques. La tecnologia incideix de manera global en el nostre catàleg de drets. Mentre ens comuniquem, proporcionem informació sobre comptes bancaris, bitllets d'avió, posició geogràfica, etc. Valorarem per què és tan important aquesta informació que generem, de quina forma està regulada i analitzarem els èxits i reptes en matèria de privacitat.

Paraules clau: Privacitat - Protecció de dades – Comunicacions – Seguretat - Drets Fundamentals de Tercera Generació

Abstract: In this final degree assignment, we deal with the data protection, focusing on online communications. Technology affects our rights in a global way. In our communications, we facilitate information about bank accounts, plane tickets, geographical location, etc. We will evaluate how important the information we generate is, how it is regulated and we will analyze the achievements and challenges in protecting our rights.

Key words: Privacy - Data protection – Communications – Security - Third generation human rights

ÍNDICE

AGRADECIMIENTOS

Agradecimientos a Rosa Barceló Compte quien me ha orientado durante toda la labor de investigación y me ha brindado buen consejo.

Este Trabajo de Fin de Grado, plasma y culmina una larga trayectoria. Sería del todo inexcusable no apreciar el hecho de que todo el equipo de docentes de la *Universitat Rovira i Virgili* a través de sus enseñanzas en estos años también han hecho posible su elaboración.

ÍNDICE DE ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
ART	Artículo
CC.AA	Comunidades Autónomas
CE	Constitución Española
CGPJ	Consejo General del Poder Judicial
CNMV	Comisión Nacional del Mercado de Valores
DNI	Documento Nacional de Identidad
DOC	Documento
DOGC	Diario Oficial de la Generalitat de Cataluña
EAC	Estatuto de Autonomía de Cataluña
ED.	Edición
EEUU	Estados Unidos
ENISA	*European Unión Agency for Network and Information Security*
FBI	*Federal Bureau of Investigation*
FJ	Fundamento Jurídico
IP	*Internet Protocol*
LOPD	Ley Orgánica de Protección de Datos
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal
LSSI	Ley de Servicios de la Sociedad de la Información
NÚM.	Número
OB. CIT.	Obra ya citada
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONU	Organización de Naciones Unidas
PIB	Producto Interior Bruto
RD	Real Decreto
STC	Sentencia Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
VS	Versus

INTRODUCCIÓN

En la aldea global que vivimos el derecho no puede obviar la nueva realidad de internet, este avance tecnológico está configurando un nuevo entorno socioeconómico. Las nuevas tecnologías ya no lo son, están sucediendo ahora y llegan a todo. Medio siglo atrás sería impensable emprender un proyecto de análisis de la privacidad en las comunicaciones electrónicas.

Algunas entidades de crédito empiezan a apostar por la banca digital, la contratación electrónica está triunfando, el manejo estratégico de los datos está generando cuantiosísimas ganancias a las empresas. La Comisión Nacional del Mercado de Valores calcula que ocho de cada diez hogares tiene internet. El comercio electrónico superó en España la cifra de los 4.400 millones de euros en el primer trimestre de 2015. Según la actividad mundial en internet en 2016 en tan solo un minuto se envían 150 millones de correos electrónicos y 21 millones de mensajes de WhatsApp.

En la sociedad de la información se generan millones de datos personales cada día. La preocupación por la privacidad está en auge. En los últimos años, el estado debe trabajar y progresar para que no se vea alterada su gobernanza y debe velar para que toda la información que se maneja esté protegida. Las empresas son muy conscientes ya de la importancia de conservar sus datos seguros y del valor que tiene su información. Con campañas como las de "empleado seguro", las compañías más importantes de nuestro país conciencian y educan a sus trabajadores para que sean desconfiados a la hora de tratar la información que manejan.

La compañía WhatsApp acaba de anunciar en abril de 2016 que las conversaciones entre sus usuarios pasan a ser seguras y encriptadas, según dicen, ni la propia compañía podrá tener acceso a esas conversaciones. Muy posiblemente esta medida que ha tomado la empresa, que ahora forma parte del grupo de Facebook, sea preventiva para evitar controversias como las que ha protagonizado Apple, cuando fue requerida por el FBI en el caso de San Bernardino, California. Consiguiendo así que en el hipotético caso de que las autoridades soliciten a la empresa cualquier tipo de conversación de un usuario, la popular aplicación de mensajería instantánea se ampare señalando que no puede entregarlas porque esa conversación estará totalmente cifrada. Sucesos como

estos han abierto un debate social en el que los ciudadanos se preguntan qué ocurre con la privacidad y la seguridad.

Nos estamos sumergiendo en una sociedad ultra compleja. La globalización, el movimiento de personas, los avances de la tecnología están revolucionando la forma en que vivimos, nos comunicamos, aprendemos y trabajamos. En el trascurso de esta obra, comprenderemos de qué forma afecta el avance de la tecnología y especialmente de las comunicaciones a nuestro ordenamiento jurídico. Conoceremos también la realidad de ese flujo de interacciones o datos personales que transmitimos a través de las comunicaciones electrónicas. ¿Son seguros nuestros datos cuando nos comunicamos?

Todos conocemos las advertencias legales[1] que son tan usuales al pie de los correos electrónicos, pues bien, estas advertencias se fomentaron con el fin de eludir cualquier tipo de responsabilidad de profesionales que enviaran un correo electrónico a un destinatario equivocado. La utilidad de estas clausulas es dudosa, muy posiblemente llamen a la prudencia o el sentido común del destinatario. En última instancia, para el caso de que el receptor incurriera en algún supuesto ilícito susceptible de sanción, esta se produciría gracias a la LOPD o al CP por revelación de secretos y no por haber emitido un aviso legal en el correo electrónico.

El mayor reto de este proyecto de investigación es sin duda el de centrar dos objetos de estudio distintos, por un lado la protección de datos y por otro las comunicaciones electrónicas. Esto sumado a la amplitud de internet hacen que resulte arduo precisar el contenido y límites del proyecto. Otro desafío, es el referente a asuntos técnicos o de ingeniería informática, palabras tan desafinadas para un jurista, como por ejemplo, *proxys*, *servidores*, *cloudcomputing* o *bigdata*.

Haremos un estudio de la evolución y orígenes de la privacidad para así conocer las razones por las que la regulación de la protección de datos ha llegado a materializarse en la que hoy conocemos. Daremos las claves respecto a los retos y futuro de la

[1] AVISO LEGAL: "Esta información es privada y confidencial y está dirigida únicamente a su destinatario. Si usted no es el destinatario original de este mensaje y por este medio pudo acceder a dicha información, por favor, elimine el mensaje".

privacidad en las comunicaciones teniendo en cuenta todas las novedades y sucesos que están teniendo relevancia en 2016 y los acaecidos en últimos años, para hacer que este estudio sea lo más actual y preciso posible. La metodología empleada durante el trabajo ha consistido en la investigación de la información teórica extraída de informes de organismos oficiales, artículos de prensa, revistas y libros específicos sobre la materia.

Aunque parezca que la privacidad es una tendencia nueva, ya a principio del milenio empezaron a proliferar cuantiosas obras sobre protección de datos. Este trabajo de fin de grado es novedoso, por dos motivos, no fueron tantos los autores que abordaron el tema específico de los datos personales en las comunicaciones y segundo, porque se aparta del corte conservador del derecho, lo cual no es intencionado, sino más bien una consecuencia de la temática que aquí se trata.

El trabajo se divide en tres capítulos, en el primero trazamos la evolución histórica de las normas de protección de datos y de las comunicaciones, también hacemos una reflexión sobre el panorama legislativo actual e introducimos la figura del *compliance* como herramienta eficaz para cumplir las exigencias normativas. En el segundo, profundizamos un poco más sobre la esencia de la protección de datos, fijándonos en entender que son estos datos y por qué son tan valiosos, más allá de un concepto ambiguo informático. En el tercer capítulo, confluimos las dos temáticas que nos interesan: la privacidad y las comunicaciones de internet. Y por último, valoraremos el debate que gira en torno a la privacidad y la seguridad.

Con ánimo de ser exhaustivos hemos analizado también la repercusión de la tecnología en nuestro catálogo de derechos fundamentales. Se trata de lo que conocemos como derechos de tercera generación, dentro de los cuales podríamos incorporar el derecho a internet y el derecho a la protección de datos. Veremos que encaje tienen en nuestro ordenamiento jurídico, si son contemplados adecuadamente o por el contrario, debemos adaptar nuestra constitución.

CAPITULO I. MARCO NORMATIVO SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES

1. Evolución legislativa

1.1. Europa

Analizando la evolución en materia de privacidad hemos constatado que existe un marco de derecho comparado muy amplio; Europa y sus estados miembros han tenido una actividad legislativa realmente intensa. Podríamos decir que Suecia y Alemania fueron países pioneros, la primera ley regional de protección de datos europea fue aprobada por el Land de Hesse en 1970 y la primera ley nacional en la materia fue en Suecia en 1973.

HERNÁNDEZ[2] entiende a este respecto que la "*protección de datos personales es uno de los Derechos Fundamentales de nuevo cuño, conocido como derechos de tercera generación, y a su vez de uno de los principios fundamentales de la declaración universal de los Derechos del hombre de 10 de diciembre de 1948, en su art. 12*[3]. " A nuestro parecer aventurarse a entender que los redactores del art. 12 de dicha declaración podían llegar a defender la privacidad o la protección puede ser precipitado. Sin embargo en la actualidad, a través de una interpretación moderna de dicho precepto, a raíz de la evolución de los derechos a la intimidad podemos sostener que ahí se acoge sin género de dudas la protección de los datos personales. Tampoco descartamos la posibilidad de que la Declaración de los Derechos Humanos y del Hombre lo acabe integrando de forma expresa.

---

[2] HERNÁNDEZ GARCÍA-BERRIO, TERESA. *Informática y libertades: La protección de datos personales y su regulación en Francia y España.* 1a. ed. Murcia: Servicio de publicaciones de la Universidad de Murcia, 2004. p. 498.

[3] *Artículo 12 de la Declaración de los Derechos Humanos del Hombre de 1948.* Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

ORDOÑEZ[4] desde su amplia perspectiva de magistrado miembro de la red de expertos de derecho europeo del CGPJ sostiene que "*de manera simplificada el derecho fundamental a la protección de datos personales se ha desarrollado en los últimos 30 años: primero, como respuesta a Microsoft en los años 80 y 90 del siglo XX, y luego a Google en lo que va del siglo XXI*". Se trata de un punto de vista que consideramos muy acertado teniendo en cuenta la influencia de estas dos grandes empresas, quienes han sido protagonistas y encargadas de impulsar la era digital.

Considera también que este nuevo derecho fundamental surgía de la amenaza que suponía la facilidad del tratamiento automatizado de la información. Este peligro en los últimos años ha derivado en una disponibilidad de infinidad de datos de nuestra vida que con tanta facilidad se pueden hallar y emplear en internet.

La creación legislativa en materia de protección de datos en la UE se ha producido de forma poco ordenada. La previsión general la encontramos esencialmente en los tratados constitutivos de la UE, Tratado de Lisboa, Carta de Derechos Fundamentales de la Unión y en la Directiva 95/46.

En el año 1967, en el seno del Consejo de Europa, se constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona. Su trabajo dio como fruto la Resolución 68/509/CE sobre los *"derechos humanos y los nuevos logros científicos y técnicos"*.[5] A partir de la resolución, se siguieron estudiando las relaciones entre la informática y la intimidad. De ahí que poco más tarde, en 1973[6] y 1974[7], el Comité de Ministros del

[4] ORDÓÑEZ SOLÍS, DAVID. *La protección judicial de los derechos en internet en la jurisprudencia europea.* 1ª. ed. Madrid: Derecho de las nuevas tecnologías, 2014. 144 pp.

[5] RODRÍGUEZ nos relata de una forma muy acertada cómo surgió la conciencia europea sobre la protección de la privacidad. DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Manual de derecho informático.*10ª. ed. Pamplona: Aranzadi, 2008. 528 pp.

[6] Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

[7] Según HEREDERO «*la idea de una Directiva de protección de datos aparece por primera vez en 1974».* HEREDERO HIGUERAS, MANUEL. *La directiva comunitaria de Protección de datos de Carácter Personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa*

Consejo de Europa advirtiera a los Gobiernos de sus estados miembros que existía una problemática tanto en el sector público como privado del uso fraudulento de los datos personales. En este orden, en 1980[8] la OCDE emitió una serie de recomendaciones sobre la circulación internacional de datos personales y la protección de la intimidad. El consejo europeo consideraba lo siguiente:

> *Aunque las leyes y políticas nacionales pueden diferir, los países miembros tienen un interés común en proteger la privacidad y las libertades individuales, así como en reconciliar los valores fundamentales pero contradictorios como la privacidad y el libre flujo de información; El tratamiento automático y los flujos transfronterizos de datos personales crean nuevas formas de relaciones entre los países y requieren la elaboración de normas y prácticas compatibles; Los flujos transfronterizos de datos personales contribuyen al desarrollo socioeconómico; La legislación local relativa a la protección de la privacidad y los flujos transfronterizos de personal pueden obstaculizar esos flujos transfronterizos; Deciden fomentar el libre flujo de información entre los Países Miembros y evitar la creación de obstáculos injustificados para el desarrollo de las relaciones socioeconómicas entre los Países Miembros.*

De las consideraciones de la OCDE, se desprende la importancia que se le otorgaba a la armonización, en materia de políticas entre países, para vencer el obstáculo de las fronteras en un fenómeno de carácter internacional. Otro detalle que nos gustaría destacar es la importancia que Europa concedía a la protección de la privacidad en el flujo de información como uno de los puntos clave de las relaciones socioeconómicas entre países.

El año 1981 debiera ser nuestro punto de referencia en materia de protección de datos, en Europa también, la mayoría de autores así lo entienden. Pues fue la fecha de adopción en Estrasburgo del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal,

---

a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. 1ª ed. Navarra: Aranzadi, p. 384.

[8] Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales "directrices de privacidad" fueron adoptadas como una recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Se hicieron efectivas el 23 de septiembre de 1980.

Convenio 108[9]. Ya en el seno europeo se intuyó el potencial peligro que suponían las tecnologías en detrimento de la intimidad personal. Resulta muy aclaratorio prestar atención al contenido del preámbulo del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal:

> *Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras; Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos.*

Aquí el Consejo no se refiere tanto a los temas de cooperación entre países sino que advierte sobre el reconocimiento de valor fundamental, derecho humano o libertad fundamental que debe tener la información personal. También matiza el hecho de que hay una contraposición a la vida privada, por lo que, implícitamente reconoce también el derecho a la libre circulación de la información entre pueblos como expresión de la libertad de información.

Casi coincidiendo en el tiempo, veía la luz en Estados Unidos, la llamada ley de Privacidad[10], publicada en 31 de diciembre de 1974, la cual ha sufrido diversas actualizaciones[11].

---

[9] Convenio Nº 108 Del Consejo de Europa, de 28 de Enero de 1981. Para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo). (BOE núm. 274 de 15-11-1985)

[10] Para saber más acerca de la regulación de Protección de datos Americana, ya que es un tema de candente actualidad en comparación con Europa, véase: ROSEMARY P JAY. Data Protection and Privacy: United States. London: Law Business Research, 2014. 191-198 pp. 2051–1280;

El año 1995 el Parlamento Europeo y el Consejo aprobaron la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva es fundamental a nivel europeo en cuanto a protección de datos se refiere. Su objetivo es el de crear un marco que regule el equilibrio entre la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE. Solicita a los Estados la creación de organismos nacionales independientes para la supervisión del tratamiento de datos.[12] La directiva 95/46/CE[13] se produjo mucho antes de ni siquiera prever los riesgos actuales a raíz del uso masivo de internet. No obstante, es considerada como una pieza clave en cuanto a derechos de la UE en internet.

Poco después en 1997,[14] nació la Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad, en el sector de las telecomunicaciones. Con el objetivo de armonizar las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad.

The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for remedies for EU citizens. Estudio Realizado para el departamento de derechos civiles y constitucionales de la UE. 2015

[11] Considera RODRIGUEZ que *«esta ley de protección de datos no protege los datos de carácter personal más que de forma indirecta y que, precisamente, es este el problema que encuentra en discusión en la actualidad debido al desequilibrio existente cuando se realizan transferencias internacionales de datos de ciudadanos de la Unión Europea a otros países, debido a que se puede perder el nivel de protección adecuado y deseado».* DAVARA RODRIGUEZ, MIGUEL ANGEL. ob. cit.

[12] En este sentido ORDOÑEZ considera que la regulación por la UE de internet no se entiende sin esta adopción de 1995, sin tener conciencia de lo que significaría internet, de la Directiva 95/46/CE. ORDOÑEZ SOLÍS, DAVID. ob. Cit. p.25.

[13] Para saber más acerca de la directiva. Véase: HEREDERO HIGUERAS, MANUEL. Ob. Cit. p. 384.

[14] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

El año 2000 es clave para comprender la problemática de la transferencia de datos pues fue cuando se llegó a un acuerdo[15] entre la UE y EEUU, denominado "puerto seguro", con el objetivo de controlar la transmisión de datos de Europa a Estados Unidos. El problema surge porque en EEUU los principios de puerto seguro son solamente un sistema voluntario[16] que supone que cualquier empresa o entidad americana que afirme respetar los principios de puerto seguro tendría derecho a recibir datos personales de la UE.

El 18 de diciembre de ese mismo año entró en vigor la carta de los Derechos Fundamentales de la Unión Europea. Esta, es de suma importancia respecto al tema que nos atañe a causa del art. 7, que proclama el respeto a la vida privada y familiar y el art. 8[17] que defiende de forma expresa la protección de datos de carácter personal. Respecto a la carta es preciso recordar que en 2009 con la entrada en vigor del Tratado de Lisboa, la Carta adquirió el mismo carácter jurídico vinculante que los Tratados.

En 2002, se incorpora la directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas[18], substituyendo así a su predecesora de 1997, con el fin de regular el sector de las comunicaciones electrónicas. Dicha norma incluye previsiones en cuanto a la conservación de datos a efectos de vigilancia policial, envío de mensajes no solicitados

---

[15] ÁLVAREZ CARO, MARÍA, et al. *Hacia un acuerdo "Safe Harbour" renovado para la transferencia internacional de datos entre EE.UU y la UE"*. Informe. Inédito, Instituto de Derecho Europeo e Integración Regional de la Universidad Complutense, 2015.

[16] Víctor Drummond cree que *«el ámbito europeo ha sido más conservador que los Estados Unidos, pues Europa tiene una mayor protección de la privacidad, también respecto a otros países».* DRUMMOND, VÍCTOR. *Internet, Privacidad y Datos Personales.* 1ª. ed. Madrid: Ed. Reus, 2004. 181 p.

[17] *Artículo 8. Protección de datos de carácter personal (Carta de derechos fundamentales de la UE)*

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[18] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de la comunicaciones electrónicas.

"cookies" y la inclusión de datos personales en las guías públicas. En 2009, a través de la directiva 2009/136/CE se realizó una actualización.

En 2006, se aprobó la Directiva 2006/24 CE[19] con el objeto de regular la conservación de determinados datos generados o tratados por los mismos para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves[20]. Se adoptó en respuesta a los atentados terroristas del 11 de setiembre de 2001, en la ciudad de Nueva York; del 11M de Madrid o del 7 junio de 2005 en Londres y básicamente establecía medidas para que las autoridades competentes de los países miembros pudieran acceder a los datos conservados por cualquier entidad[21].

Su consecuencia fue una merma de los derechos fundamentales, así lo reconoció STJUE de 8 de abril de 2014[22]. Esta sentencia conocida como *Digital Rights* anuló esta Directiva por ser contraria al derecho a la vida privada, proclamado en el articulo 7 y al derecho a la protección de datos personales del artículo 8, de la carta de los derechos fundamentales de la Unión. Resulta interesante el contenido de la sentencia europea ya que los miembros de la curia abordan de una forma muy amplia la injerencia en los datos personales, en aras del interés general.

En 2013, nació el reglamento N. 611/2013[23] el cual contiene normas sobre la notificación de casos de violación de datos personales por parte de los proveedores de

[19] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, por contravenir la Carta de Derechos Fundamentales de la Unión Europea.

[20] VILASSAU ofrece un estudio amplio en base a la dualidad seguridad vs privacidad a raiz del debate que suscitó la directiva. VILASSAU, MONICA. La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. Privacidad. *Revista de Internet, Derecho y Política,* UOC, 2006, nº2, p. 15

[21] Véase: La justicia europea anula la norma que obliga a operadores a conservar datos de telecomunicaciones: La directiva constituye "una injerencia de gran magnitud y especial gravedad" en los derechos fundamentales. *Periodico Europa Press*. Bruselas 8 de abril de 2014.

[22] Sentencias del Tribunal de Justicia de la Unión Europea de los asuntos C-293/12 y C-594/12.

[23] Reglamento (UE) n.º 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva

servicios de comunicaciones en caso de pérdida, robo u otro incidente que comprometa la seguridad de los datos personales de sus clientes.

El derecho a ser protegido en sus datos personales goza de pleno reconocimiento legislativo en la actualidad en las democracias occidentales de los Estados miembros de la UE. Hoy en día la privacidad lo que incluye el derecho a la vida privada y el derecho a la protección de datos personales, es el derecho fundamental protagonista en Internet, y está provocando un reajuste en los derechos fundamentales.

Para conocer la actualidad de la protección de datos en Europa debemos prestar atención al pasado mes de octubre de 2015, pues el TJUE[24] tomó una decisión que está causando mucho revuelo. Se ha concluido lo que conocíamos como puerto seguro, ha desaparecido la base legal por la que se enviaban datos de Europa a Estados Unidos, la cual venía desde el año 2000 como comentamos a priori. La sentencia afecta en gran medida a sectores de grandes empresas del mundo digital, Facebook, Google, Twitter, cuyas fórmulas de negocio residen en la explotación de datos que obtienen de sus usuarios.

Las agencias de protección de datos europeas están coordinadas para imponer multas a las empresas que transfieran datos personales de sus clientes europeos basándose en el protocolo de Puerto Seguro.

El 2 de febrero de 2016, a través de nota de prensa, la Comisión Europea anunció que se estaba renegociando con Estados Unidos un nuevo marco de transmisión internacional de datos, con el objetivo de sustituir al que fuera anulado por el TJUE.[25] En nuestra

---

2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas [DOUE L 173, de 26-VI-2013].

[24] Tribunal de Justicia de la Unión Europea. A través de comunicado de prensa nº 117/15 En Luxemburgo, 6 de octubre de 2015. Sentencia en el asunto C-362/14 Maximillian Schrems/Data Protection Commissioner: El Tribunal de Justicia declara inválida la Decisión de la Comisión que declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos.

[25] Nota de prensa de la Comisión Europea 2 febrero de 2016; Noticia del Periódico 20 minutos: Acuerdo UE-EE UU para el nuevo 'safe harbour': el 'privacy shield' entraría en vigor en tres meses. 2 de febrero de 2016.

opinión, la agilidad por la comisión para remontar dicho acuerdo debe venir motivada por la importancia que tienen estos movimientos de datos, para los gigantes de internet, tales como Google, Dropbox, Facebook, pues resulta imprescindible para los intereses económicos de las empresas tecnológicas.

El 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en referencia al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en adelante RGPD, que entrará en vigor el 25 de mayo de 2018. El nuevo texto proclama que las personas físicas deben tener el control sobre sus propios datos. Se afirma en el considerando sexto que la recogida y tratamiento de datos personales ha aumentado de forma significativa y reconoce que las empresas privadas y las autoridades públicas utilizan datos personales en una escala sin precedentes. También expresa su preocupación sobre la necesidad de facilitar la circulación de datos con terceros países.

En palabras de ORDOÑEZ[26] *«Probablemente lo más significativo de la propuesta de la Comisión Europea respecto de Internet sea la consagración expresa del denominado "derecho al olvido"*. Lo que supone la posibilidad para el ciudadano de eliminar el rastro de datos personales referentes a su persona que se hallen en internet. Recordemos la sentencia GOOGLE SPAIN de 2014[27], que seguro el legislador europeo habrá tenido en cuenta.

Por último, decir que estudiando las normas de derecho internacional privado por las que se rigen los países miembros de Europa podremos observar que no existen todavía convenios multilaterales en disciplina de protección de datos y tampoco bilaterales para el caso de España. Actualmente, contamos con muchas normas de origen institucional

[26] ORDOÑEZ SOLÍS, DAVID. ob. cit. p.27.

[27] El 13 de mayo de 2014 se publicó la sentencia del Tribunal de Justicia de la Unión Europea («TJUE») dando respuesta, a una serie de cuestiones prejudiciales remitidas por la Audiencia Nacional española que enfrentó a la Agencia Española de Protección de Datos («AEPD») y a Google Spain. El TJUE vino a reconocer "el derecho al olvido".
Véase: ÁLVAREZ CECILIA, RIGAUDIAS. *Sentencia Google Spain y Derecho al Olvido.* Actualidad Jurídica de Uría Menéndez, 2014, pp. 110-118.

entendiendo por tales las procedentes de la Unión Europea, que se canalizan a través de Reglamentos y Directivas. A nuestro parecer dado que la información se mueve en un mundo cada vez más moderno en que las comunicaciones electrónicas son en gran medida internacionales es preciso que Europa siga trabajando para conseguir asumir normas de cooperación y acuerdos con otros países en aras de una mejor seguridad para los ciudadanos.

1.1.2. España

Antes de entrar a analizar cuál ha sido la actividad del legislador español en cuanto a protección de datos fijaremos nuestro punto de partida en la Constitución, concretamente en el artículo 18. En este precepto el constituyente garantiza el secreto de las comunicaciones y en su apartado cuarto recoge el concepto de informática. En el capítulo octavo analizaremos con más profundidad el alcance constitucional de la protección de datos.

En cuanto al desarrollo legislativo en España, el primer eslabón fue la Ley 5/1992 Orgánica sobre la regulación del tratamiento automatizado de datos, en adelante LORTAD, que se encargó de impulsar la Agencia Española de Protección de datos. Su vigencia fue breve a causa de la directiva comunitaria 95/46/CE, donde se exigía que la legislación de los países no debía prever solo el tratamiento automatizado de datos sino también el manual. Cabe decir que no fue difícil para España acoger los requerimientos europeos porque ya disponía de una legislación preexistente en materia de protección de datos. España optó por redactar una ley completamente nueva en lugar de modificar y adaptar la legislación en materia de protección de datos que existía en aquel momento. Por ello, aparece la Ley Orgánica de Protección de Datos[28], en adelante LOPD que atendería las exigencias de la directiva.

Estas leyes orgánicas de protección de datos, tanto LORTAD como LOPD, surgen como establecen en su art. 1 con el objetivo[29] de:

[28] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm. 298 de 14 de Diciembre de 1999.

[29] Sobre los límites de desarrollo legislativo fijados por el TC. Véase la STC 290/2000.

Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar. Así pues podemos decir que el derecho de la protección de datos se ha desarrollado a través de las dos Leyes orgánicas antes señaladas.

Junto a las leyes de protección de datos se ha elaborado en España la normativa de desarrollo y aplicación de estas, entre las que destaca la norma de desarrollo con la cual se creó la AEPD. De esta normativa de desarrollo hay que señalar que la misma surgió como desarrollo de la LORTAD. Fue en 1999 cuando se creó el RD 994/1999 que desarrolla la LORTAD, y no será hasta el año 2007 que se promulgue el reglamento que desarrolla la nueva LOPTD[30].

Además de la normativa específica sobre protección de datos personales, en determinados sectores junto a la LOPD y sus normas de desarrollo, el legislador ha dejado abierta la posibilidad de regulaciones sectoriales optándose así como el resto de países europeos por un sistema mixto de regulación de protección de datos personales en el que la Ley general no deroga toda la normativa sectorial precedente, quedando como norma general subsidiaria[31].

[30] Sobre la ley protección de la LOPD, véase: APARICIO SALOM, JAVIER. *Estudio sobre la Ley la Protección de Datos*. 4ª. ed. Madrid: Aranzadi, 2013. 464 pp.

[31] Ley Orgánica 6/2001, de 21 de diciembre, de Universidades modificada por Ley Orgánica 4/2007, de 12 de abril (Art. 57, 62 y DA 21); Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia; Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (*Artículo 333 y Disposición adicional vigésima sexta);* Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público; Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica Esquema Nacional de Seguridad; Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los servicios públicos; Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones; Ley 59/2003, de 19 de diciembre, de firma electrónica; Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y de Comercio Electrónico.

En materia de comunicaciones, las leyes básicas de interés son la Ley 9/2014[32] general de telecomunicaciones, la ley 56/2007[33] de medidas de impulso de la sociedad y la información, la ley 25/2007[34] de conservación de datos, la ley 34/2002[35] de servicios de la sociedad de la información y del comercio electrónico y el texto refundido de los consumidores[36].

Según el preámbulo de la nueva ley general de telecomunicaciones 9/2014:

> *La Agenda Digital para Europa, principal instrumento para el cumplimiento de los objetivos de la Estrategia Europa 2020, persigue que para 2020 todos los europeos tengan la posibilidad de acceder a conexiones de banda ancha a una velocidad como mínimo de 30 Mbps, y que, al menos, un 50 % de los hogares europeos estén abonados a conexiones de banda ancha superiores a 100 Mbps.*

Como vemos España está trabajando para que el acceso a internet sea universal, atajando lo que conocemos como brecha digital. Estos objetivos quedaron incorporados a la agenda digital española, aprobada por el Gobierno en febrero de 2013.

Nuestra legislación nacional cuenta con dos normas de desarrollo destacables: el RD 889/2009 por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas y el RD 424/2005 relativo a las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

---

[32] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. (Texto consolidado. Última modificación: sin modificaciones).

[33] Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. Última modificación: 28 de diciembre de 2013).

[34] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (Última modificación: 10 de mayo de 2014).

[35]Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (Última modificación: 10 de mayo de 2014).

[36] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

España, en calidad de país miembro, va observando y atendiendo las instrucciones de Europa en materia de protección de datos. Recordemos que el Derecho Comunitario tiene primacía sobre el nacional. Por tanto, el legislador español deberá atender y cumplir las actualizaciones que incorpore el nuevo reglamento de la Unión Europea. Una vez entre en vigor este nuevo reglamento y conozcamos el texto definitivo parece difícil que coexista íntegramente con las normas internas españolas, deberán ser los jueces los que en última instancia valoren dicha compatibilidad.

Nuestro pronóstico es que a causa de las nuevas exigencias que impondrá el nuevo marco legal europeo, la LOPD deberá renovarse: llegado el caso no sabemos si se optará por adaptarla o por derogarla e incorporar una completamente nueva. Esto dependerá del grado de compatibilidad que se produzca entre nuestro ordenamiento y el Reglamento.

A raíz del fallo del TJUE de 2015 la AEPD ha prohibido a las plataformas tecnológicas[37], como *DropBox* o *Google Drive*, que realicen transferencias de datos de ciudadanos europeos a otros países, sin su consentimiento. El plazo que concedió finalizó el pasado 29 de enero de 2016. Por el momento, la Agencia Española no ha sancionado a nadie todavía, la solución de requerimiento de autorización no parece muy efectiva.

Hemos advertido que para conseguir una protección efectiva de los ciudadanos se requiere una gran inversión por parte del gobierno, por lo que topamos también con los límites de los Presupuestos Generales del Estado. Entendemos que el parlamento español debe ser prudente en las garantías o los niveles de protección que otorga en esta materia sobre todo en el contexto actual de depresión económica.

[37] Respecto a la actuación de la AEPD, véase: CRESPO VITORIQUE, ISABELA. Asunto Safe Harbor La Agencia Española de Protección de Datos da el primer paso en relación con las transferencias internacionales de datos a Estados Unidos. *Gómez-Acebo & Pombo,* 2016, p.1.; El TJUE declara inválida la Decisión de la Comisión que declara el nivel adecuado de protección del Puerto Seguro. *Nota de prensa de la AEPD*. Madrid. 6 de octubre de 2015; V.MORENO. Guía para entender el laberinto legal del Puerto Seguro. *Periódico Expansión.* Octubre de 2015.

El estado debería velar por el correcto cumplimiento de la normativa en esta materia y por la diligencia de los responsables del tratamiento de datos de una forma similar a como lo viene haciendo en materia laboral o tributaria. La AEPD dispone de funcionarios que ejercen la función de inspección a tenor del art. 40 de la LOPD. Debe trabajarse paulatinamente para que el inspector de protección de datos sea considerado como un homólogo al inspector de hacienda o de trabajo lo que supondría un gran avance y creemos que acabará materializándose en los próximos años a medida que la vulnerabilidad de la información personal sea cada vez más pública y notoria.

1.1.3. Cataluña

En una perspectiva de comparación entre los países miembros ARENAS[38], al referirse a la situación de la normativa de protección de datos en España destaca que "*aparte del legislador central en España, tenemos que mencionar el importante papel que ha jugado el legislador autonómico en esta materia*". Debido a que tanto la LORTAD como la LOPD establecían la posibilidad de que las CC.AA. pudieran crear y mantener sus propios registros de ficheros, así como de una autoridad de control encargada de los mismos, las comunidades autónomas entendieron que la ley tenía una habilitación para elaborar normas autonómicas en materia y se aprobaron diversas leyes sobre protección de datos personales

En el año 2002 el Parlamento de Cataluña aprobó la Ley de la Agencia Catalana de Protección de Datos. Esta misma norma establecía la obligación de que el Gobierno catalán aprobara el estatuto de la agencia catalana de protección de datos en el plazo de 3 meses desde la promulgación del cuerpo legislativo.

Como decíamos anteriormente, la ley de la Agencia Catalana de Protección de Datos surge de la previsión contenida en el art. 41 de la LOPD de 1999 que establecía la posibilidad de creación de órganos correspondientes a la autoridad de la administración estatal, por parte de las comunidades autónomas. Cataluña fue la segunda comunidad autónoma por detrás solo de Madrid, quien lo hiciera en 1995, en crear su propia Agencia, si bien esta última desaparecería años más tarde. En 2003 entró en vigor el

[38] ARENAS RAMIRO, MÓNICA. *La protección de los datos personales de la Unión Europea.* Revista Jurídica de Castilla y León, 2008, nº 16, pp. 113-168.

Decreto 48/2003[39], que aprobaba el Estatuto de la Agencia Catalana de Protección de Datos.

La aprobación del Estatuto de autonomía de 2006 supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos y reforzó el papel de la autoridad de control en materia de protección de datos, ya que, por una parte, clarificó y amplió su ámbito de actuación y, por otra, reforzó su independencia al establecer su designación parlamentaria.

El EAC en su art. 31[40] proclama el derecho a la protección de datos personales y el art. 156 detalla cual es la competencia ejecutiva en materia de protección de datos de carácter personal que, respetando las garantías de los derechos fundamentales en esta materia junto con estas exigencias derivadas del Estatuto de autonomía y otras mejoras técnicas necesarias, el año 2010 se publicó la Ley 32/2010[41] de 1 de octubre, de la Autoridad Catalana de Protección de Datos[42], que todavía sigue en vigor, la cual vino a derogar la anterior Ley Catalana de Protección de Datos de 2002. Incorporó además a la legislación vigente en Cataluña otras modificaciones, como la propia denominación de la autoridad.

1.2. Cooperación internacional para ofrecer más seguridad en un entorno digital global.

Durante la Edad Media los comerciantes que viajaban alrededor de los países en sus mercados, plazas y puertos advirtieron que precisaban de unas reglas consensuadas

[39] Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. (DOGC núm. 3835, de 04.03.2003).

[40] *Artículo 31 EAC. Derecho a la protección de los datos personales***.** Todas las personas tienen derecho a la protección de los datos personales contenidos en los ficheros que son competencia de la Generalitat y el derecho a acceder a los mismos, a su examen y a obtener su corrección. Una autoridad independiente, designada por el Parlamento, debe velar por el respeto de estos derechos en los términos que establecen las leyes.

[41] Promulgada el 1 de octubre de 2010 (Diario Oficial de la Generalitat de Cataluña, núm. 5731, del 8 de octubre de 2010).

[42] Para más información acerca de la autoridad de protección de datos de Cataluña, véase: Informe 6/2015 de la Sindicatura de Cuentas, publicado en junio de 2015. Disponible en la web: www.sindicatura.cat

comunes para generar confianza y seguridad en el tráfico internacional. La costumbre acabó desarrollando la *Lex Mercatoria*.

En la era de de internet y las comunicaciones, los agentes de la sociedad de la información afrontan un entorno incierto a causa de las diferentes regulaciones que existen según los países. Requieren también para generar confianza y seguridad en el trafico de la sociedad de la información fijar unas reglas esenciales comunes para sus participantes. El conflicto normativo va en detrimento del proceso abierto y global de la Sociedad de la Información, al igual que les ocurría a los comerciantes hace cientos de años. Los principios que rigen el entorno digital deben ofrecer seguridad y certeza para que los participantes tengan la suficiente confianza, al igual que las costumbres lo hacían entre los sujetos mercantiles.

Actualmente la protección en cuanto al tratamiento de la información personal se enfrenta a graves obstáculos, por la falta de armonización entre países y jurisdiccionales que dificultan la aplicación efectiva de todos los derechos legales sustanciales en el entorno de la red. Por ello, el acceso, distribución y uso de la información requieren de unas reglas que aporten confianza, seguridad y la justicia en el siglo XXI del mundo digital compuesto por ciudadanos, empresas y gobiernos.

HEIDELBERG[43], profesor de derecho de la Fordham University Law School especializado en derecho de las nuevas tecnologías, ciberseguridad y propiedad intelectual, introdujo la idea de la *lex informática*[44] como proceso que debía obedecer a la formación de políticas comunes que tutelen la sociedad de la información y la tecnología. Considera en esencia que el conjunto de reglas previstas para acoger el tráfico de información que genera la tecnología y las comunicaciones deben formar una

[43] REIDENBERG R, JOEL. *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 1998. 76-553 pp.

[44] OLIVERA L, NOEMÍ. *Estado de la cuestión en la relación entre derecho e informát*ica. Derecho y nuevas tecnologías: Universidad de la Plata, 2009. 505 a 517 pp. ; FRANCO LEGUÍZAMO, CAMILO ARMANDO. De la Lex Mercatoria a la Lex Constructions. *Revista emercatoria*, 2007 nº6, pp 14-15. ; Rodriguez Puerto, Manuel J. La regulación de Internet y la teoría jurídica. Revista Dialnet, 2007, 441-464 pp. Articulo elaborado dentro del Proyecto I+D del Ministerio de Educación y Ciencia Libertad y nuevas tecnologías: regulación jurídica (SEJ2004-06124).

lex informática la cual debe ser comprendida y acogida por los gobiernos de manera consciente.

Problemas internacionales precisan de soluciones igualmente globales. Comprobaremos la necesidad de una formas de actuación armonizada con la ayuda de algunos ejemplos. Empresas como *Microsoft, Facebook*, *Dropbox*, que ofrecen el mismo servicio a sus usuarios se someten a distintas regulaciones. Pensemos en un nacional español que interactúa mediante servicios de mensajería instantánea con otro de California, este con un panameño y este último con un finlandés mediante WhatsApp. Imaginemos otro caso en que se produce una compraventa a través de PayPal, Amazon o WallaPop, siendo el vendedor europeo y el comprador asiático. En los dos ejemplos citados, comunicación y comercio electrónico, estaríamos otorgando una protección distinta a la información generada por los sujetos intervinientes.

Al hilo de esto último, cabe hacer referencia al asunto del acuerdo *"safe harbour"* entre Estados Unidos y Europa, pues en síntesis todo el debate gira en torno la diferente tutela que otorgan los distintos ordenamientos jurídicos a los datos que generan las operaciones que conllevan un traspaso internacional de datos. Sucede, como decíamos, que el conflicto normativo se contrapone al proceso abierto y global que se ve inmersa la sociedad de la información en que vivimos.

A nuestro juicio la labor de fijar unas normas de comportamiento comunes entre países va a ser una tarea complicada por las diferencias jurídicas, políticas y sociales entre estados. Por ejemplo, entre Estados Unidos y Europa nos topamos ante un problema añadido que supone las desigualdades entre los principios y valores que rigen ambos ordenamientos jurídicos. La seguridad de estado en el país americano, prima siempre sin discusión frente al derecho a la intimidad, y en cambio en Europa el concepto de seguridad de estado tiene unos límites más estrictos.

1.3. Importancia del *compliance* en el cumplimiento de la normativa en materia de protección de datos

En los últimos años se está extendiendo el concepto de *compliance* empresarial, considerado como una herramienta útil de prevención de conflictos. Lo hace a través de una cultura de cumplimiento y responsabilidad. En España se ha visto impulsada por la reciente modificación de la Ley Orgánica del Código Penal[45], que vino a actualizar el régimen de responsabilidad penal de las personas jurídicas.

La expresión *compliance* o cumplimiento normativo tiene como objetivo evitar aquel riesgo legal, pérdida económica o de reputación que puede sufrir una persona física o jurídica como consecuencia de su falta de cumplimiento de las leyes.

A nuestro juicio en el mundo de protección de datos el *compliance* también pasará a ser una pieza clave para el cumplimiento de la legislación por parte de las empresas. Motivado por una finalidad doble, debido a las exigencias de las regulaciones y para evitar mala reputación de la entidad. Especialmente se extenderá cuando entre en vigor en 2018 el nuevo reglamento de la Unión Europea, Nº 2016/679 una de las novedades que se esperaba, suponía la obligación de crear la figura de un delegado de protección, finalmente solo será preciso para algunos casos. Esta nueva figura se encargará de velar por el cumplimiento legal en el seno de las entidades.

Respecto al incumplimiento del reglamento de protección de datos, se estipula que el responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de una infracción durante el tratamiento.

Este nuevo reglamento también insta a los Estados Miembros a la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de la regulación en materia de protección de datos, teniendo en cuenta las necesidades especificas de las pequeñas y medianas empresas.

[45] En materia de compliance, véase: BEGOÑA, GONZALEZ Y MORAL, Mª TERESA. Responsabilidad Penal de Personas Jurídica y *Corporate Compliance*. *Fundesem Business School, Cuatrecasas Goncalves Pereira,* 2015. pp.1-4.

Como podemos observar tanto la responsabilidad derivada por daños, como la creación de mecanismos de certificación constituyen dos elementos suficientes para motivar a las empresas que tratan información personal a cumplir de forma estricta las previsiones legales.

En este sentido SALDAÑA[46] haciendo referencia al asesoramiento jurídico del responsable del tratamiento expone que *«la aplicación de los controles preventivos en un mismo cliente al mismo tiempo permite detectar los riesgos operativos incluso antes de que se produzcan».* Como vemos también apuesta por el compliance, y añade que la protección de datos dentro de la operativa global de la compañía como un gran activo a tener en cuenta por cualquier organización.

Por otro lado según GALLEGO[47] en España cumplir los requisitos impuestos por las leyes de protección de datos es complicado porque considera que la AEPD vigila continuamente la actividad de las empresas, especialmente en el sector de bancos, seguros, telecomunicaciones y comercio electrónico.

Sin embargo, es aconsejable porque la AEPD dispone de un régimen sancionador fijado en la LOPD mediante el cual impone multas pecuniarias periódicas, que oscilan entre los 900 y los 600.000 euros dependiendo de la gravedad. Con arreglo a Ley de Servicios de la Información además pueden imponerse sanciones que consisten en dar publicidad a la infracción en el BOE, en dos periódicos de difusión que coincida con el ámbito de difusión o en la página de inicio del sitio de internet del prestador. Esto último es más eficaz como herramienta coercitiva ya que supone un riesgo de mala reputación para la empresa infractora.

[46] SALDAÑA, JORDI. Capitulo XIII. El asesoramiento jurídico al responsable del tratamiento. Llacer Matacas, María Rosa. *Protección de Datos Personales en la Sociedad de la Información y Vigilancia.* 1ª ed. Madrid: Kluwer, La Ley grupo Wolters, 2011. 380 pp.

[47] F. GALLEGO, GONZALO. Data protection compliance in Spain Mission impossible*? Hogal Hovells,* 2015, nº 1, p. 16.

CAPITULO II. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

2.1. Evolución del concepto de protección de datos

La actual LOPD en su artículo 3 define los datos de carácter personal como *"cualquier información concerniente a personas físicas identificadas o identificables"*. Esto supone que cuando nos referimos a datos personales, no solo estamos utilizando un concepto vago e indeterminado relacionado con la informática. Sobre este respecto MARTINEZ[48] puntualiza que puede atribuirse la naturaleza de dato personal a una imagen, a un sonido, a un número de teléfono o como ha señalado la AEPD a una dirección IP o correo electrónico.

El nuevo RGPD de 27 de abril de 2016 mantiene el concepto de datos personales y amplia el concepto de "el interesado" que lo considera como aquella persona física identificable cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Aunque ahora concibamos nuestros datos personales en términos digitales no siempre fueron así. RUIZ[49] a través de un enfoque histórico nos explica en qué consistían los datos personales tradicionales. Este autor describe los datos personales tradicionales, como aquellos básicos que según el Código Civil identificaban a las personas físicas, tales como, el nombre y los apellidos. A posteriori se fueron añadiendo informaciones adicionales como la del domicilio, DNI, estado civil o cualquier otro dato que ofreciera más información acerca de la situación social y económica.

[48] MARTÍNEZ MARTÍNEZ, RICARD. El derecho fundamental a la protección de datos. Benjamin R. Barber, et al. *Internet, Derecho y Política: Las transformaciones del Derecho y la Política en 15 artículos.* Barcelona: Editorial UOC, 2009. pp. 141-166.

[49] RUIZ CARRILLO, ANTONIO. *La protección de los datos de carácter personal.* Editorial Bosch, Barcelona. 2000. 1ª ed. pp. 20-27.

Nos parece un buen punto de partida, pues gracias a este enfoque afrontamos con mayor perspectiva cómo ha evolucionado la información personal de los ciudadanos de acuerdo a las nuevas dinámicas sociales y económicas. Ha cambiado la forma en que nos comunicamos, pero también, ahora es distinta la información que generamos. Pues todos aquellos datos clásicos no aportaban ningún indicio sobre la personalidad, el carácter o estilo de vida.

2.2. El valor de nuestros datos

La información es poder. Como consecuencia del avance de la tecnología, esos datos tradicionales se han convertido en una auténtica fuente de compleja información personal. Meglena Kuneva , comisionada europea de los consumidores, en marzo de 2009, dijo lo siguiente: *"Los datos personales son el petróleo nuevo de Internet y la nueva moneda del mundo digital"* .

En este apartado trataremos de comprender por qué es tan valiosa toda la información que generamos, mientras configuramos nuestros perfiles digitales. Varios analistas han descrito a nuestros datos como, el petróleo del S. XXI.[50] Pensemos en el beneficio económico que genera para las empresas el conocer el comportamiento de los ciudadanos de cara al mercado. Se trata de un punto sobre el cual no habíamos reparado atención al inicio del trabajo, y significa que los datos no solo afectan a la esfera de la intimidad sino también tienen incidencia en materia económica y fiscal. Supone que a la luz del valor que están adquiriendo los datos, estos deben ser cuantificados económicamente de alguna forma.

No sabemos cuánto tardarán estas nuevas iniciativas en el ámbito tributario en España o en Europa, pero la comercialización de datos debe conllevar nuevas obligaciones fiscales por su valoración. De igual forma si las empresas generan un gran almacenamiento de datos personales y estos son de alto valor, debe existir la manera de contabilizar ese activo intangible. En Estados Unidos ya hay un debate en torno a esto.

[50] LUZI, MICHELE, et al. *Personal Data: The emergence of a new asset class*. World Economic Forum, in colaboration with Bain & Company, Inc. 2011; COOPER, TIM, et al. Guarding and growing personal data value, 2015. pp. 35.

El famoso periódico *Wall Street Journal*[51] en el contexto de la salida a bolsa de Facebook presentó una cuantificación individualizada de su valor y mostraba los siguientes datos:

> *"Los resultados muestran que usted es un valor aproximado de $ 81 para Facebook. Sus amistades valen $ 0,62 cada una, y su página de perfil podría ser valorada en $ 1.800. Facebook con casi mil millones de usuarios se ha convertido en la mayor fuerza de trabajo no remunerado de la historia".*

En otra noticia el *New York Times*[52], comentaba iniciativas para ayudar a los usuarios a poner precio a sus datos personales:

> *"La información de los consumidores es de miles de millones en su conjunto, pero individualmente, los bits de datos valen prácticamente nada. Un estudio realizado por JP Morgan Chase mostró el año pasado que un usuario único valía $ 4 a Facebook y $ 24 a Google. Otros miraban recientes presentaciones de Facebook con la Comisión de Valores y se coloca el valor de un usuario tan alto como $ 120."*

El concepto *Big Data*[53], surgió como actividad consistente en analizar cantidades enormes de datos para identificar los patrones de consumo y así crear nuevas oportunidades de negocio. La importancia de nuestros datos personales para las empresas radica sobre todo en la capacidad que tienen estos de convertirse en beneficios económicos.

PEREZ LUÑO[54] considera que la dificultad está en garantizar una protección a algo que evoluciona de una forma constante y la necesidad de hallar una fórmula que evite el monopolio de la información.

---

[51] To Facebook You're Worth $80.95. *Wall Street Journal.* 3 Mayo de 2012.

[52] BRUSTEIN JOSHUA. Start-Ups Seek to Help Users Put a Price on Their Personal Data. *New York Times*. 12 de febrero de 2012.

[53] Noticias: ARRIETA, ELENA. ¿Aún hablas de 'big data'? Estás obsoleto. Periódico Expansión. 9 de febrero de 2016; La moda del big data ¿En que consiste en realidad? *Periódico El economista.* José Carlos López López. 27 de febrero de 2014.

[54] PÉREZ LUÑO, ANTONIO ENRIQUE. *Informática y libertad: comentario al articulo 18.4 de la constitución española*. Revista de Estudios Políticos N. 24 noviembre-diciembre, 1981.

2.3. El derecho fundamental a la protección de datos y a la libertad de las comunicaciones

Al margen de la recopilación y evolución histórica que habíamos trazado en el plano legislativo, es preciso mediante un enfoque constitucional, comprobar cuál ha sido la previsión del constituyente en estos aspectos. La CE de 1978 ya recogía expresamente el término informática, por tanto, el constituyente español ya tenía una posible perspectiva de lo que sería la revolución tecnológica y sus peligros, seguramente también influido la tendencia internacional. Pues recordemos que Europa ya había emitido varias resoluciones y recomendaciones[55], alertando de la lesividad de la informática sobre los derechos fundamentales. Debemos señalar en favor del constituyente español que lejos de lo que puediera parecer, la previsión constitucional de la protección de datos y de la libertad en las comunicaciones tiene pleno acogimiento en nuestros días.

Considera FERNÁNDEZ[56] que mediante la configuración de los derechos fundamentales podremos afrontar la evolución que la sociedad impone, para proteger al individuo de las amenazas de la sociedad de la información.

Por otra parte, ORDOÑEZ[57] entiende que *«en España no había un objetivo claro de la doctrina respecto a la protección de datos, ni la población tenía conciencia del concepto de privacidad».* A nuestro juicio esto es comprensible, pues la sociedad todavía no era tan sofisticada como ahora, en ese momento era lógico que los ciudadanos no vieran amenazados sus datos personales ni sus comunicaciones. Tampoco se tenía tanta información como en el presente y los usuarios con acceso a la red eran una minoría privilegiada. Pensemos que no fue hasta años más tarde en que

[55] Cfr. pp 9-10, Capítulo I.

[56] FERNÁNDEZ RODRÍGUEZ, JOSÉ JULIO. *Secreto e Intervención de las comunicaciones e internet.* Madrid: Thomson Civitas, 2004. p.41.

[57] ORDOÑEZ considera que por aquel entonces en España no existía una doctrina clara y decidida en un sentido determinado, ni la conciencia social reaccionaba al termino de protección de datos, ni, mucho menos, había un poso de formación y conocimiento sobre el que se ha dado en llamar "derecho de la privacidad" que se ha incorporado a la lista de los denominados "derechos fundamentales de tercera generación". ORDOÑEZ SOLÍS, DAVID. Ob cit.p.22.

triunfaría la era digital en España, la cual podemos fijar en 1995, con la llegada de la telefonía móvil y de internet a los hogares españoles.

Si analizamos nuestra Constitución no indica en ningún momento que la privacidad sea un derecho fundamental, sin embargo es el Tribunal Constitucional en su STC 292/2000 quien le otorga ese carácter. En este sentido también se pronuncia PÉREZ[58] que *«entiende el derecho a la protección de datos como un derecho fundamental de creación jurisprudencial».* Por tanto, gracias a la tarea interpretativa[59] y la experiencia del Tribunal Constitucional no ha sido necesaria la modificación del texto constitucional para otorgar a la protección de datos un rango de derecho fundamental.

El art. 18[60] es sin duda el que más circunstancias comparte con la protección de datos. Analizaremos este artículo a través de sus dos vertientes más trascendentes para nuestro estudio. Esto es, a través de las comunicaciones y de la protección de datos por otro lado.

El secreto de las comunicaciones, ha venido perfilándose por la jurisprudencia del Tribunal Constitucional. En la STC 132/2002[61] el Alto Tribunal ya constató que el avance tecnológico de la sociedad suponía la necesidad de un cambio de mentalidad y entendía la comunicación como *"un instrumento de desarrollo cultural, científico y tecnológico colectivo"*. Siguiendo la jurisprudencia[62] del Tribunal Constitucional, el 18.3 de la CE consagra la libertad de las comunicaciones y garantiza su secreto, sea cual fuere la forma de interceptación, mientras dure el proceso de comunicación, en el marco

[58] MÉNDEZ PÉREZ, JESÚS MARÍA. *La protección de datos de carácter personal como derecho fundamental autónomo*. Informe, Inédito. Derecho constitucional III, Universidad de Murcia, 2014.

[59] Sentencia 254/1993, de 20 de julio de 1993 del Tribunal Constitucional. Recurso de Amparo núm 1827/1990.

[60] PERALES ASCENSIÓN, ELVIRA. *Sinopsis de la constitución española.* Informe, Inédito, Universidad Carlos III, 2003.

[61] *"En una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo"* (STC 132/2002, de 20 de mayo).

[62] Véase: STC 114/1984, SSTC 114/1984, 49/1999, 70/2002, 184/2003, 281/2006, SSTC 123/2002, 56/2003, 230/2007.

de comunicaciones indirectas, es decir, que empleen medios técnicos[63], y frente a terceros ajenos a la comunicación.

URBANO[64] mediante una interpretación moderna del artículo 18 entiende que no protege la privacidad como tal sino un derecho diferente, el de la libertad de comunicación, esto es, el derecho a transmitir un mensaje a otro y a recibir su respuesta sin interferencia de terceros, sobre cualquier soporte técnico. Al hilo de la versatilidad de la constitución que comentábamos, esta es de tal magnitud que nos ha permitido proteger en unos inicios el derecho clásico a la inviolabilidad del secreto postal y que con el avance de las nuevas tecnologías se ampare de la misma forma las comunicaciones mediante correo electrónico.

Respecto a la protección de datos, ya en su redacción el constituyente tuvo el acierto de advertir el uso de los datos personales, por lo que la nuestra fue una de las primeras constituciones en tener este nivel de protección. El Tribunal constitucional interpretó que el derecho de la protección de datos debía considerarse como un derecho independiente, si bien es cierto, que precisaba que este estaba íntimamente ligado al derecho a la intimidad.[65] En este sentido, vinculaba de forma directa a los poderes públicos al afirmar que no requería de desarrollo normativo.

En concreto, la STC 94/1988 de 24 de mayo en su FJ 4 señaló que, *"el art. 18 faculta a los ciudadanos para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención* . En el mismo sentido matiza el alto tribunal el objetivo de la protección de datos, en la STC 292/2000 de 30 de noviembre FJ 6 al afirmar lo siguiente:

---

[63] Si bien es cierto que el art. 18.3 atribuye garantías a las comunicaciones postales, telegráficas o telefónicas, cabe entender igualmente cualquier tipo de comunicación de correo electrónico, chat u otro medio, tal y como dice Elvira Perales, siempre que se efectúen mediante algún artificio instrumental o técnico, pues la presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional del precepto; en consecuencia, el levantamiento del secreto por uno de los intervinientes no se consideraría violación del artículo 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad (STC 114/1984).

[64] URBANO CASTRILLO, EDUARDO. *El derecho al secreto de las comunicaciones.* Madrid: La Ley grupo Wolsters Kluwer. 1ª ed. 2011. pp. 19-23.

[65] Véase SSTC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre.

"Tal derecho persigue garantizar a las personas un poder de control sobre sus datos personales, sobre su uso y su destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".

Este derecho se halla estrechamente vinculado con la libertad ideológica que consagra el art. 16 CE[66]. Pues el almacenamiento y uso de datos puede suponer un riesgo para la libertad ideológica, sobretodo, con un uso distinto o fraudulento sin conocimiento del interesado y también a través de intromisiones indebidas[67] a ficheros ajenos. Ofreciendo garantías de protección de datos se consigue una defensa doble, la de los fines de las bases de datos, su cancelación y el conocimiento de terceros; y la protección de la ideología, religión o creencias que consagra el art. 16.2 CE.

Recordemos también que los derechos del art. 18 CE se encuentran en el rango de derechos protegidos por reserva de ley orgánica del art. 81 CE y que vinculan a todos los poderes públicos a tenor del art. 53. CE y tutelados en última ratio a través de la tutela del Tribunal Constitucional mediante recurso de amparo que dispone el art. 53.2 CE.

[66] SSTC 11/98, de 13 de enero; 44 y 45/1999, de 22 de marzo, entre otras, en relación con la libertad sindical.

[67] STC 144/1999, de 22 de julio, en torno a una indebida utilización por parte de una Junta Electoral de Zona de datos incluidos en el Registro Central de Penados y Rebeldes.

CAPITULO III. LA PROTECCION DE DATOS EN LAS COMUNICACIONES ELECTRONICAS

3.1. Internet y la tercera generación de derechos

Internet es una de las tecnologías de la información y comunicación, que últimamente son conocidas como las (TIC). La cuestión es que lejos de considerarse un mero avance tecnológico, está suponiendo una transformación económica y social. Estamos seguros de que en nuestro presente año 2016, se ha convertido en una herramienta imprescindible en innumerables ámbitos de nuestras vidas.

En palabras de José Carbonell,[68]

> *"Internet es el tejido de nuestras vidas. Si la tecnología de información es el equivalente histórico de lo que supuso la electricidad en la era industrial, en nuestra era podríamos comparar internet con la red eléctrica y el motor eléctrico, dada su capacidad para distribuir el poder de la información por todos los ámbitos de la actividad humana"*

CASTELLS[69] defiende que internet afecta a la forma en que nos comunicamos y a la forma en que se organizan las empresas y gobiernos. Por eso, de la misma manera que ocurre con los datos personales, su importancia radica en su repercusión calculada en términos económicos. Pero no solo eso, internet es una revolución social y cultural.

La economía digital cada vez está más conectada, hasta tal punto que según un informe[70] de Naciones Unidas se considera ya, que hay una clara correlación entre las capacidades de un país para desarrollar economía digital[71] y su renta per cápita. Sin embargo, es difícil cuantificar el valor que generan los bienes y servicios intangibles. El consumo privado es el sector que más aporta al PIB, y este es más alto en los países

[68] CARBONELL, JOSÉ Y CARBONELL, MIGUEL. Capitulo II. El acceso a internet como derecho humano. Vega Gómez, Juan. *Temas selectos de Derecho Internacional Privado y de Derechos Humanos.* 1ª. ed. México. D.F: Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas, 2014. pp. 19-39.

[69] CASTELLS, MANUEL. *La galaxia Internet. Reflexiones sobre internet, empresa y sociedad.* Barcelona, Editorial de Bolsillo, 2003, p.15.

[70] PÉREZ, RICARDO Y CIMOLI, MARIO, et al. *La nueva revolución digital: de la internet del consumo a la internet de la producción*. Informe. Inédito, Naciones Unidas-CEPAL, 2015.

[71] A través del índice de disponibilidad de red: Networked Readiness Index.

desarrollados o emergentes. El consumo ligado a las redes sociales, comunicaciones y comercio electrónico supone una actividad más fácil para los usuarios. Por otro lado, la planificación del impacto de internet es más elevada en países económicamente avanzados en los que la inversión privada y el gasto público comporta una mayor adopción tecnológica por las empresas y gobiernos.

3.2. El derecho fundamental de acceso a internet

El Tribunal Supremo alemán el 24 de enero de 2013[72] consideraba que en las sociedades desarrolladas internet se trataba de algo esencial para la vida. Como hemos visto anteriormente[73] se está comprobando que los países que tienen más desarrollado su entorno digital cuentan con un PIB más elevado.

Dada la importancia que está adquiriendo internet en nuestra sociedad nos lleva a reflexionar acerca de si debe ser considerado como un derecho fundamental. Llegado el caso también habría que decidir cuál sería su contenido y limites. Se trataría de un derecho surgido del cosmopolitismo, de los conocidos como derechos de tercera generación.

Una de las repercusiones del triunfo de internet recae sobre su encaje constitucional. A este respecto, la declaración Universal de Derechos Humanos en su articulo 12[74] reconoce el derecho a "tomar parte libremente de la vida cultural de la comunidad" y a "participar del progreso científico".

[72] Sentencia del Tribunal Supremo Federal alemán, dictada el 24 de enero de 2013 por la sección tercera de su sala de lo civil (III ZR 98/12).

[73] Véase Capitulo 3, "Internet y la tercera generación de derechos".

[74] *Articulo 12 de la Declaración Universal de Derechos Humanos.* Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de el resulten.

El relator especial en la promoción y protección del Derecho a la Libertad de Opinión y Expresión de las Naciones Unidas Frank la Rue[75] considera que en "cuanto medio por el que puede ejercerse el derecho a la libertad de expresión. Internet solo puede responder a su finalidad si los Estados asumen ser un instrumento tecnológico al que solo podrá acceder una determinada élite, con lo cual se perpetuará la brecha digital, generando la desigualdad y la exclusión."

Recordemos que algunos países como China, Egipto, Irán o Corea del Norte han limitado el acceso a internet de los ciudadanos. Por este motivo la ONU, mediante su relator La Rue, ha declarado la importancia de que se considere internet como un medio para ejercer el derecho a la libertad de expresión, y consideran que eso solo se podrá llevar a cabo si los países asumen mayores compromisos.

El derecho de acceso a internet no es la única reivindicación en cuanto a derechos humanos modernos, el derecho a la paz, consumidores, medio ambiente. Son lo que conocemos como la tercera generación de derechos. En Reino Unido se ha acuñado el concepto "contaminación de libertades" para describir la erosión y degradación que vulnera a los derechos fundamentales frente a las nuevas tecnologías. A este respecto considera GARCÍA SAN MIGUEL[76] que esta pretensión de derechos se sitúa en un contexto en que la informática ha pasado a ser símbolo emblemático de nuestra cultura.

En la Cumbre mundial sobre la sociedad de la información Ginebra 2003 -2005[77] se centraron en los mecanismos de financiación destinados a colmar la brecha digital, en la gobernanza de Internet, y en general todos los desafíos de las TIC.

La mesa redonda del Consejo de Derechos Humanos sobre la promoción y la protección de la libertad de expresión en Internet[78] expresó su preocupación respecto a la

---

[75] Consejo de Derechos Humanos, Tema 3. De la Agenda. Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Frank La Rue. GE.11-13204 (S)

[76] GARCÍA SAN MIGUEL, LUIS, et al. *Estudios sobre el derecho a la intimidad.* Madrid: Tecnos. 1992. p. 37.

[77] Documento: WSIS-05/TUNIS/DOC/6 (Rev.1)-S. 28 de junio de 2006. Texto Original en ingles.

[78] Consejo de Derechos Humanos 21º período de sesiones Temas 2 y 3 de la agenda Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General Promoción y protección de todos los derechos humanos, civiles,

privacidad del contenido online y sobre la existencia de programas informáticos de vigilancia. También se refirieron a las limitaciones que podía suponer el hecho de que Internet supusiera una barrera fundamental para el ejercicio del derecho a la libertad de expresión en internet. Ya que consideraban que el acceso a internet se refería tanto a su contenido como a la infraestructura, apremiando a reducir la brecha digital entre los países del mundo. Llegando a considerar Internet como una herramienta indispensable, que favorece el crecimiento y el progreso de la sociedad en su conjunto.

Pasamos ahora a plantearnos la situación de internet como derecho fundamental en nuestro ordenamiento jurídico, y si es necesaria su integración. En España, no han existido hasta el momento pronunciamientos sobre el carácter de derecho fundamental del acceso a internet, salvo la declaración de derechos de internet del Senado español de 1999. Sí que es posible encontrar en las últimas redacciones de algunos Estatutos de Autonomía un reconocimiento al derecho de acceso a internet por parte de los ciudadanos. Art. 34 del Estatuto de Autonomía de Andalucía, art. 53.1 del Estatuto de Autonomía de Cataluña y 7.6 del de Extremadura, art. 19.2 de Estatuto de Comunidad Valenciana.

LUCENA[79] entiende que el problema del acceso al patrimonio digital de internet y su integración como derecho está relacionado con el art. 9.2[80] de la CE. Según esta teoría conllevaría que internet representa un instrumento para el ejercicio de los derechos de la ciudadanía y desarrollo de su persona. Por lo que, la imposibilidad de su acceso comportaría riesgo de exclusión social, que incide en el plano de la igualdad.

---

políticos, económicos, sociales y culturales, incluido el derecho al desarrollo. 2 de Julio de 2012. Original: Inglés.

[79] LUCENA CID, ISABEL VICTORIA. *El derecho de acceso a internet y el Fortalecimiento de la democracia.* 2014. Universidad Pablo de Olavide. Revista Internacional de Pensamiento Político. Vol. 9. pp. 383-398.

[80] Art. 9.2 CE: "corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social".

A nuestro juicio el artículo 20[81] de la Constitución española, acoge perfectamente la tecnología de internet. Su apartado primero proclama el derecho: a) a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción, b) a la producción y creación literaria, artística, científica y técnica, c) a la libertad de cátedra, y d) a comunicar o recibir libremente información veraz por cualquier medio de difusión.

Más allá de debates técnicos acerca de cuál sería la mejor delimitación conceptual y más acertada para encajar internet en nuestra carta magna. Lo cierto es que gracias a clausulas abiertas que estableció el constituyente no es necesario especificar a qué tipo de tecnología le estamos otorgando un derecho. La inclusión de internet en nuestra constitución comportaría que nuestra carta magna fuera más moderna y reconoceríamos expresamente un fenómeno social que tiene una importancia innegable. Sin embargo, si cada vez que hubiese un avance tecnológico con magnitudes socioeconómicas tan importantes tuviéramos que reformar nuestro marco constitucional para incluir ese nuevo concepto, correríamos el riesgo de desnaturalizar nuestro catálogo de derechos de la CE.

Otra opción es la inclusión del derecho de acceso a internet como principio rector de la política social y económica, tal como sucede con otro derecho de tercera generación que es el de medio ambiente. Insistimos en que el debate es puramente conceptual, pues con la formula abierta de nuestra constitución ya se entiende que acoge la tecnología de internet.

3.3. Algunos datos estadísticos sobre los servicios de comunicaciones electrónicas

La utilidad de un sistema de comunicaciones electrónico, comporta el hecho de que se pueda transferir información electrónica entre distintos lugares. Por ello, podemos decir

[81] Sobre el articulo 20 de la CE véase: NUÑEZ MARTINEZ, MARÍA ACRACIA. *El Tribunal Constitucional y las libertades del articulo 20 de la constitución española*. Revista de Derecho de la UNED, 2008. núm. 3. pp. 289-317.

que: *"las comunicaciones electrónicas son la transmisión, recepción y procesamiento de información entre dos o más lugares, mediante circuitos electrónicos"* [82]

La directiva 2002/58/CE relativa al tratamiento de la protección de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas entiende por comunicación: *"cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público".*

La realidad actual de que los servicios electrónicos y la tecnología constituyen un elemento casi esencial en nuestro desarrollo diario a nivel personal y de negocios es algo innegable. Sin embargo, hemos querido contrastarlo, comprobar que efectivamente esa sensación es cierta. Lo haremos a través de estudios de consumo y del Instituto Nacional de Estadística. Evidenciaremos la trascendencia de las comunicaciones electrónicas desde la óptica de cuatro sectores que son a mi juicio determinantes en una sociedad moderna: los hogares, las empresas, los bancos y la administración.

La finalidad de determinar la magnitud de la implantación de los servicios de comunicaciones electrónicas a través de cifras es doble: por un lado, para conocer cuántos son los sujetos intervinientes y por otro, para comprender la necesidad del análisis en profundidad de las comunicaciones electrónicas en relación con su necesaria salvaguarda de los datos personales. Este apartado es alentador porque de alguna manera legitima toda la obra.

Es algo que ya intuíamos, si bien lo constata la COMISIÓN NACIONAL DEL MERCADO DE VALORES[83]. Ocho de cada diez hogares tiene internet, según el Panel de Hogares del CNMC correspondientes al primer semestre de 2015. En cuanto a

[82] Definición obtenida del libro: TOMASI, WAYNE. *Sistemas de comunicaciones electrónicas.* 4ª edición. DeVry Institute of Technology Phoenix, Arizona. p. 1.

[83] Nota de Prensa de la Comisión Nacional del Marcado de Valores. Resultados obtenidos a través del Panel de Hogares, a través de encuestas del primer trimestre de 2015. [En línea] [Fecha de consulta: 15 de marzo de 2016] 2015 [Acceso gratuito]: *http://www.cnmc.es/Portals/0/Ficheros/notasdeprensa/2015/TELECOS_AUDIOVISUAL/PanelHogares/20151204_Panel6_telecos_rev.pdf;*

servicios móviles, en el primer semestre de 2015 el 90,5 % de los individuos disfrutaron de algún tipo de servicio de telefonía móvil, 4 puntos más respecto al primer semestre de 2014. Otro dato que nos parece relevante, es el de la reducción en el gasto de mensajes de texto y de llamadas de voz, un 60% y un 46,6 % respectivamente. La banda ancha móvil continuó durante el primer trimestre de 2014 con su expansión. [84]

Una vez analizados los hábitos de consumo relativos a internet de los hogares, pasamos a analizar los de las empresas[85], lo haremos a través de la encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas del primer trimestre de 2015. El 98,4% de las empresas españolas de 10 o más empleados dispone de conexión a Internet en el primer trimestre de 2015. Siete de cada 10 tienen página web. El 93,0% de las empresas de 10 o más empleados interactuó a través de Internet con las Administraciones Públicas durante 2014.

Según la Ley General de Telecomunicaciones, aunque la explotación de redes de comunicaciones electrónicas se realice en régimen de libertad de competencia, el art. 2 de este cuerpo legislativo impone a los interesados la notificación previa al Registro de operadores. Por lo que respecta a las condiciones para la explotación de redes y la prestación de servicios de comunicaciones electrónicas se establece el régimen de derechos de los operadores, las condiciones que deben cumplir y las obligaciones de suministro de la información.

---

[84] Informe por la Comisión Nacional del Mercado de Valores sobre los consumos y gastos de los hogares españoles en los servicios de comunicaciones electrónicas, del primer semestre de 2014. ESTAD/CNMC/0003/15. [En línea] marzo de 2015 [Fecha de consulta: 16 de marzo de 2016] [Acceso gratuito]:*http://www.cnmc.es/Portals/0/Ficheros/Telecomunicaciones/Informes/20150318_Informe_Consumos_y_gastos_12014.pdf ;* Informe de la situación económico digital de BBVA. [En línea] julio de 2015 [Fecha de consulta: 16 de marzo de 2016] [Acceso gratuito] Disponible en: *https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion_Economia_digital_jul-ago15-Cap1.pdf*

[85] Para conocer el uso de las TIC según los sectores empresariales, véase el Informe realizado por la Subsecretaria de Industria, energía y turismo: Sector electrónica y TIC. [En línea] abril de 2015 [Fecha de consulta: 16 de marzo de 2016] [Acceso gratuito]: *http://www.minetur.gob.es/esES/IndicadoresyEstadisticas/Presentaciones%20sectoriales/Electronica%20y%20TIC.pdf*

La LGT define la red de comunicaciones electrónicas como los sistemas de transmisión, y cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan y demás recursos que permitan el transporte de señales mediante cables, con inclusión de las redes de satélites, redes terrestres fijas y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la redifusión sonora y televisiva.

Respecto al servicio de comunicaciones electrónicas, según la misma ley, este se configura como el prestado por lo general a cambio de una remuneración que consisten su totalidad o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos.

La sociedad espera poder conectarse en cualquier sitio en cualquier momento. Por ese motivo, los usuarios de estas comunicaciones también deben demandar que estos servicios sean seguros. La Unión Europea ha dotado una agencia encargada de la seguridad de redes, (ENISA)[86]. Este organismo tiene la función de asesorar y coordinar las medidas adoptadas por la Comisión y países de la Unión para dar seguridad a sus redes. En 2014 publicó un informe[87] relevante para la materia objeto de investigación: El informe cuyo título traducido al castellano es "Adquisiciones seguras para unas comunicaciones electrónicas seguras", subrayaba la creciente dependencia de los proveedores con respecto a los productos y los servicios subcontratados de TIC, y que analiza los riesgos de seguridad que implica esta evolución.

La guía de adquisición segura de TIC para proveedores de comunicaciones electrónicas recomienda a los Estados miembros que se sensibilicen sobre los riesgos de seguridad relacionados con la adquisición de productos y la externalización de servicios de TIC. Asímismo, se anima a vendedores y proveedores a desarrollar un enfoque colaborativo

[86] ENISA. La agencia Europea de Seguridad e Información y la Red. Dispone de página web. https://www.enisa.europa.eu/

[87] KARSBERG, CHRISTOFFER. *Secure ICT Procurement in Electronic Communications. Analysis and recommendations for procuring ICT securely in the Electronic Communications Sector.* European Union Agency for Network and Information Security, 2014. 40 pp.

en lo referente a la elaboración de los requisitos de seguridad, el intercambio de información sobre vulnerabilidades y amenazas a la seguridad, y la reducción de los incidentes.

La directiva 2002/58/CE, respecto a la seguridad en la red establece dos obligaciones para los prestadores de servicios: la primera, consiste en la adopción de medidas técnicas y adecuadas para preservar la seguridad de sus servicios; y la segunda, constituye un derecho de información para el usuario que consiste en que éste deberá ser informado en caso de que exista un riesgo particular de violación de la seguridad en la red.

Las administraciones públicas y las empresas están recurriendo a modernas medidas tecnológicas y procedimientos de gestión de seguridad. Una de las medidas más efectivas que están empleando las empresas al margen de otras muchas tareas preventivas es el de cifrado de datos, especialistas informáticos y abogados recomiendan este sistema.[88]

3.4. Los datos personales en las comunicaciones electrónicas

Como decíamos al inicio del trabajo uno de los mayores retos era el de establecer una conexión entre la protección de datos y las comunicaciones. DAVARA[89] justifica esta conexión por causa de la capacidad de generar datos personales por parte de las nuevas empresas de telecomunicaciones, así como de la facilidad de almacenarlos y transmitirlos. Respecto a la forma de abordar este tema VELEIRO[90] sostiene que debemos abordarlo desde un doble prisma: el tratamiento de los datos que obren en poder de los operadores relativos al tráfico y la prestación de servicios avanzados en telefonía.

Para tener una mejor visión de la privacidad en las comunicaciones citaremos brevemente la legislación europea y española relativa a esta materia. A nivel europeo es

[88] ABANLEX. *Segundo informe sobre la necesidad legal de cifrar información y datos personales.* Informe. Inédito, Abanlex, Despacho de abogados Especializado en tecnología de protección de datos, 2015.

[89] DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *XVII Encuentros sobre informática y derecho.* 2002,2003. Madrid: Universidad Pontifica de Comillas. p.103.

[90] VELEIRO REBOREDO, BELÉN. ob cit. p.84.

destacable la Directiva 95/46[91], relativa a la protección de datos personales y a la libre circulación de datos. En cuanto a la protección específica de la privacidad en el sector de las telecomunicaciones hay que atender a lo dispuesto en la Directiva 97/66/CE[92]. Por otro lado la Directiva 2002/58/CE[93], garantiza el derecho a la intimidad y la protección de datos personales en el sector de las telecomunicaciones.

En España, respecto al derecho a la protección de datos el art. 18 de la CE y la LO 1/1982. En cuanto a la regulación en materia de comunicaciones por vía electrónica, sería la LSSI y la LGT. En materia de protección de datos debemos atender lo dispuesto en la LOPD y el RD 1702/2007. Y por último las responsabilidades que se puedan dirimir en el ámbito penal, se desprenderán de lo dispuesto en el capítulo primero del título décimo del código penal, art. 197.

En el plano legislativo procesal COTINO[94] aboga por la readecuación del secreto de las comunicaciones a las comunicaciones electrónicas y la imperiosa necesidad de la acción legislativa. Entiende que es preciso que el secreto de las comunicaciones también sea aplicable a los datos de tráfico y geolocalización.

El concepto de privacidad simplemente se ha expandido, pues aunque no haya variado el significado, las nuevas tecnologías y el progreso de la sociedad ha añadido nuevos elementos susceptibles de ser íntimos que en una sociedad analógica no estaban en riesgo. CAMPUZANO[95] entiende que no es que los nuevos medios electrónicos hayan modificado el concepto de privacidad, lo que sucede es que han cambiado las formas en que se ponen en peligro nuestros datos.

---

[91] La Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[92] Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

[93] Directiva 2002/58/CE del parlamento europeo y del consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)

[94] COTINO HUESO, LORENZO. Derechos humanos, internet y TICs". Rey Martínez, Fernando. *Los derechos humanos en España, un balance crítico.* Valencia: Tirant lo Blanch, 2015, pp. 418-480.

[95] CAMPUZANO TOMÉ, HERMINIA. *Vida privada y datos personales.* Tecnos. 2000. p. 69.

BALLESTEROS[96] reconoce también la complejidad de la privacidad en el ámbito de las comunicaciones, cuando afirma que es el desafío más evidente de la sociedad tecnológica. A este reto que el autor nos plantea, debemos añadir el hecho de que muchos de los prestadores de servicios de la información utilizan servidores que se encuentran ubicados en Estados Unidos, estado en el cual sabemos, cuentan con una regulación de la privacidad distinta.

Como vemos tanto en la gestión de datos de tráfico telefónico como los relativos a la ubicación por parte del prestador de servicios de comunicaciones, se recalca la necesidad de ese consentimiento previo que deriva de la LOPD. Sucede que el usuario no es consciente de la información que quien le presta los servicios maneja o bien y que asume la imposición de la obligación de ceder sus datos para la promoción comercial, como expone el art. 6 de la Directiva 2002/58/CE.

La directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, define los datos de tráfico como: *"cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"*. Se emiten datos de tráfico cuando escribes un correo electrónico o lo recibes, cuando envías contenidos por aplicaciones de mensajería instantánea o cuando accedes a páginas web. La directiva, en su artículo 9, establece la obligación de eliminarse o de hacerse anónimos los datos de tráfico surgidos de las comunicaciones electrónicas cuando ya no sean necesarios a efectos de la transmisión de una comunicación. Tan solo se permite tratar los datos de tráfico necesarios a efectos de la facturación de los abonados.

También se establece una segunda excepción, en previsión de los datos almacenados por motivo de las contrataciones a distancia. Últimamente es muy común que los ciudadanos contraten servicios, seguros de automóvil o de hogar, telefonía por vía electrónica o telefónico. Por este motivo se permiten las grabaciones legalmente autorizadas de comunicaciones y de datos de tráfico asociados a ellas cuando se lleven a

[96] BALLESTEROS MOFFA, LUIS ANGEL. *La privacidad electrónica: Internet en el centro de protección*. Tirant Monografías, 2005, Valencia. p.139.

cabo en el marco de una práctica comercial lícita con el fin de aportar pruebas de una transacción comercial.

Los datos de localización son cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio. Pensemos en la cantidad de aplicaciones que tenemos en nuestro teléfono móvil que solicitan el acceso a los datos de localización para poderlas instalar en nuestros dispositivos (Instagram, Facebook, Aplicaciones de Deporte, etc) y sobre las cuales nosotros lo autorizamos.

La directiva 2002/58/CE los regula separadamente, aunque de una forma muy similar a los datos de tránsito. A tenor de esta norma, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesario para la prestación de un servicio con valor añadido. El consentimiento deberá consistir en informar al usuario sobre los datos que serán tratados, su finalidad, duración y transmisión a terceros. De igual forma el usuario siempre deberá tener la posibilidad de mediante un procedimiento sencillo y gratuito rechazar temporalmente el tratamiento de tales datos.

Respecto a la confidencialidad de las comunicaciones esta directiva es clara y proclama en su art. 5 que los estados miembros garantizarán la confidencialidad de las comunicaciones realizadas mediante las redes públicas de telecomunicación, prohibiendo expresamente la *"escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados"*. Sin embargo hace aquí una excepción *"salvo cuando esté autorizada legalmente"*. Y con esto se refiere a aquellas limitaciones que constituyan una medida necesaria para proteger la seguridad nacional, defensa, seguridad pública, prevención, investigación, detección, persecución de delitos o la utilización no autorizada del sistema de telecomunicación. Esta excepcionalidad la abordaremos en más profundidad en el último capítulo.

3.5. Marketing

3.5.1. Cookies

Se trata de un dispositivo que se descarga en el terminal de un usuario con la finalidad de almacenar datos, que irán siendo actualizados y finalmente podrán ser recuperados por la entidad responsable.[97] Son tecnologías destinadas para almacenar y obtener luego datos de cualquier terminal ya sea un ordenador, teléfono móvil o Tablet. Pensemos por ejemplo en un servicio a través de una página web o una aplicación móvil, o comercio electrónico o un servicio bancario. La finalidad es sencilla, los prestadores de servicios web las emplean alegando que su objetivo es mejorar la experiencia de los usuarios. DRUMMOND interpreta que para abordar el conflicto de las cookies debemos hacerlo a través de tres fases, la primera sería la recogida de datos, la segunda el almacenamiento y la última consistiría en la utilización de estos datos.

Su regulación se encuentra recogida en la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSI)[98]. No obstante, cuando la instalación de una *cookie* suponga una utilización de datos personales implicará necesariamente que el responsable del tratamiento cumpla con las exigencias adicionales sobre la normativa de protección de datos personales.

Nos aporta mucha luz un informe del gabinete jurídico de la Agencia de Protección de Datos[99] en respuesta a una consulta planteada por un prestador de servicios de información en referencia a la obtención del consentimiento del usuario en materia de cookies. Nos recuerda la AEPD que el art. 22 de la LSSI permite a los prestadores de servicios el uso de *cookies* siempre que se haya obtenido el consentimiento de los

[97] Agencia Española de Protección de Datos. Guía sobre el uso de las Cookies. [En línea] 1ª ed. [Fecha de consulta: [3 de abril de 2016] [Acceso gratuito]: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

[98] Ley 34/2002 de Servicios de la Sociedad de la Información (a consecuencia de la transposición de la Directiva 31/2000/CE) como por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos. Entrada en vigor el 10 de mayo de 2014.

[99] GABINETE JURÍDICO, et al. *Informe 0011/2014*. Informe. Inédito, Agencia Española de Protección de Datos, 2014.

usuarios de forma clara y completa. Por este motivo para dar cumplimiento al consentimiento informado es imprescindible que el prestador desarrolle un sistema en que se asegure que el usuario es consciente del destino de sus datos y la injerencia en su privacidad. Este requisito ha venido exigiéndose a raíz de la trasposición de la Directiva 2009/136/CE que actualizaba la anterior Directiva de Privacidad 2002/58/CE.

En este sentido también se incluyó en el régimen sancionador de la LSSI el uso de *cookies* sin consentimiento del usuario en los términos del art. 22. El cual ha sido modificado por la Ley 9/2015 de Telecomunicaciones. Por este motivo, habremos podido observar que cada vez que accedemos a un aplicativo web de la índole que sea, se nos previene del uso de cookies y en ocasiones no nos permite avanzar hasta que aceptemos el uso de estos o incluso se emplean formulas más elaboradas como "si usted continúa navegando en esta página significará que entiende y acepta las condiciones de esta web"

El incumplimiento de la condición de que los usuarios hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre , de protección de datos de carácter personal. La LSSI lo considera una infracción grave y sanciona esta conducta con una multa de 30.000 a 150.000 euros y la posibilidad de publicar la sanción en el BOE, en dos periódicos de difusión que coincida con el ámbito de difusión o en la página de inicio del sitio de internet del prestador.

En el grupo de trabajo[100] creado sobre la recomendación de mejores prácticas de EASA/IAB se expone de forma detallada porqué se introdujo la condición del consentimiento informado. En esencia, venían a decir que era consecuencia de la creciente preocupación de los ciudadanos y autoridades por el rápido aumento de las posibilidades técnicas que permiten seguir el comportamiento de navegación de las personas en internet de manera continuada y en distintos sitios de la red. También preocupaba al grupo de trabajo que las medidas para proteger la vida privada no iban parejas a la evolución de las medidas para atacarla, en este sentido también consideraban que los ciudadanos no eran conscientes de el uso de las *cookies*. Este

[100] Dictamen 16/2011 sobre la recomendación de mejores prácticas de EASA/IAB sobre publicidad comportamental en línea. Informe. Inédito, Grupo de Trabajo de Protección de Datos del art. 29, 2011.

desconocimiento y la creciente dependencia de los europeos a internet para actividades cotidianas

DRUMMOND[101] entiende que no hay violación de la privacidad en la fase de recopilación y almacenamiento en consecuencia está exento el prestador del servicio de responsabilidad, argumentando que se trata de un mecanismo informático que facilita la navegación. Sí que considera que puede vulnerarse la privacidad cuando se utilicen los datos personales por parte del prestador de servicios. Lo cual se agrava cuando se trata de empresas que se dedican al comercio electrónico. El usuario debe aportar mucha más información, todo ello junto con las otras informaciones que ha recopilado la web generan un perfil muy completo del usuario y pone al sitio web a un paso de la ilicitud por la tentación de comercializarlos.

8.5.2. Spam

La AEPD[102] define como Spam o "correo basura" todo tipo de comunicación no solicitada, realizada por vía electrónica. Esto es, cualquier mensaje no solicitado que normalmente persigue la comercialización por parte de alguna empresa[103]. Son varias las vías, llamadas, mensajes o correos electrónicos.

Ocurre en muchos casos, ya sea una compra online, la suscripción a una revista, el registro en una plataforma web o la instalación de cualquier programa o aplicación en que por defecto el prestador de servicio establece que el usuario consiente el envío de publicidad. Por este motivo, es preciso ser cautos a la hora de tratar el spam, pues en algunos casos somos nosotros mismos los que lo consentimos por no prestar la suficiente atención. La AEPD alerta de que los casos de Spam cada vez son más complicados de abordar por ser que los que lo generan contratan a informáticos para ocultar su verdadera identidad.

---

[101] DRUMMOND, VICTOR. Ob. cit. p. 118.

[102] Guía de Facua para enfrentar el Spam. [En línea] 1ª ed. Fecha de consulta: [12 de abril de 2016] [Acceso gratuito]: https://www.facua.org/es/guias/guia141.pdf

[103] Guía Para Lucha Contra el Spam. Agencia Española de Protección de Datos. [En línea] 1ª ed. Fecha de consulta: [12 de abril de 2016] [Acceso gratuito]: http://www.uv.es/siuv/cat/norm/luchaspam.pdf

A nivel europeo el artículo 13 de la Directiva 2002/58/CE solo autoriza la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.

Nuestra legislación nacional acogió este precepto mediante el art. 21 de la LSSI que prohíbe el envió de comunicaciones publicitarias por cualquier medio electrónico siempre que no hayan sido autorizadas o solicitadas y con la salvedad de que existiera una relación contractual previa en la que se hubiera obtenido de forma lícita los datos del destinatario y los empleara para el envió de comunicaciones comerciales referentes a productos de su empresa que fueran similares. Igual que sucede con las cookies, se considera una infracción grave y se sanciona esta conducta con una multa de 30.000 a 150.000 euros y la posibilidad de publicar la sanción en el BOE, en dos periódicos de difusión que coincida con el ámbito de difusión o en la página de inicio del sitio de internet del prestador.

En caso de que se prestara ese consentimiento, la LSSI establece que el usuario deberá tener la posibilidad de oponerse o revocar el tratamiento de sus datos mediante un procedimiento gratuito y sencillo. Es por ello, que en el momento en que percibamos que estamos recibiendo publicidad no deseada en nuestro correo electrónico y deseemos que no se siga produciendo, debemos contactar con el prestador de servicios y hacérselo constar.

Existe un debate suscitado en torno a esta cuestión, a juicio de DRUMMOND[104] debe abordarse estableciendo una ponderación entre la libertad de expresión o la privacidad del usuario. Este autor sostiene que el correo electrónico es un bien intangible amparado por el derecho de propiedad, sin embargo, afirma que la libertad de expresión debe ser plena siempre que no ofenda los principios fundamentales básicos. Nos ofrece una solución a través de la responsabilidad civil, como mecanismos de control. Considera que el spam debe controlarse para que el desarrollo tecnológico no se vea mermado.

[104] DRUMMOND, VICTOR. Ob. Cit. p.126.

CAPITULO IV. SEGURIDAD VS PRIVACIDAD

La eficacia de los sistemas de protección de privacidad de los individuos depende de los límites a los que estos sistemas se vean sometidos, tradicionalmente los gobiernos han venido justificando la restricción de estas garantías amparados en la seguridad nacional. Lo que nos conduce a un debate verdaderamente complejo propio de las sociedades cosmopolitas: ¿Debe prevalecer la privacidad de los individuos por encima de todo? O por el contrario, debemos defender que existen motivos que legitimen su intromisión.

FROSINI[105] considera que nuestras vidas corren el riesgo de hallarse sometidas a lo que ha llegado a calificar como un juicio universal permanente. Esto significa que a través del control electrónico de documentos personales, del manejo de datos fiscales, del comercio electrónico, pagos con tarjeta de crédito o mediante la reserva de billetes de transporte se pueden crear bancos de datos muy amplios. Estas informaciones dispersas si se concentran y organizan pueden generar un perfil digital muy exhaustivo.

En nuestra opinión ello conlleva una discusión, muy similar a la que pudo generarse a raíz de la implantación en la sociedad de los servicios de comunicación por voz, las llamadas telefónicas, la cual está ya superada. De forma muy resumida, la solución a la que se llegó fue la de permitir su intervención pero con límites legales exhaustivos. Solución que nos parece salomónica pues es razonable que ante la existencia de indicios de criminalidad se permita la intromisión en la vida privada del individuo. De lo contrario este debate no giraría en torno a la privacidad o seguridad, sino que sería más bien, privacidad o delincuencia. El problema podría venir cuando en un futuro no muy lejano el conocimiento de esos datos se emplee de una forma anterior, atemporal y pasemos a una cultura preventiva.

Como suele suceder, el legislador redacta los textos legislativos de acuerdo con su contexto, realidad social o el desarrollo de ese momento histórico. Uno de los sucesos acaecidos que ha marcado un punto obvio de inflexión en el fenómeno de la seguridad

[105] GARCÍA SAN MIGUEL, LUIS, et al. *Estudios sobre el derecho a la intimidad.* Madrid: Tecnos. 1992. pp 38 a 44.

nacional ha sido el atentado cometido el 11 de setiembre de 2001[106], su repercusión fue tal que los americanos se sitúan a la cabeza en políticas de vigilancia en aras de una mayor seguridad nacional.

Precisamente en Norteamérica están sucediendo casos actualmente muy mediáticos acerca de la cuestión que aquí tratamos. El caso Apple vs FBI[107] es un perfecto ejemplo de lo que supone la privacidad vs la seguridad nacional. Por un lado la empresa Apple que representa el triunfo del progreso, del consumo y la tecnología y por otro lado al FBI de los Estados Unidos que siempre ha apostado por la seguridad nacional. Ante el requerimiento de colaboración para desbloquear un *IPhone* del FBI, Apple se negó asegurando que esta ayuda supondría una merma de las libertades. No rompemos una lanza en favor de la compañía, pues seguro que formaba parte de su estrategia empresarial, pero lo cierto es que ha conseguido generar un debate en la ciudadanía sobre la importancia de la privacidad.

Otra de los gigantes de internet ha demandado en abril de 2016[108] al gobierno de Estados Unidos al considerar que es inconstitucional la prohibición de que las empresas tecnológicas no puedan informar a sus clientes cuando sus datos han sido revisados. En su demanda asegura que ha recibido 5.624 peticiones de información del gobierno en un año y medio. Como vemos en la sociedad de la información que vivimos el alcance de la privacidad tiene una importancia notable.

Centrándonos en nuestro entorno más próximo, en Europa este debate se vio reflejado de una forma muy evidente en la directiva 2006/24[109]. Esta se dispuso como consecuencia de los atentados terroristas de Londres surgida de la necesidad de adoptar cuanto antes medidas sobre conservación de datos de telecomunicaciones. Proclamaba

[106] COMISIÓN EUROPEA, DIRECCIÓN GENERAL. *Seguridad y Privacidad para el ciudadano en la Era digital posterior al 11 de setiembre: vision prospectiva.* Informe. Inédito, Institute for Prospective Techonological Studies, 2003.

[107] MENN, JOSEPH; FINKLE JIM. Privacy vs. Security at heart of Apple phone decrypt order. *Reuters.* Unites States. 18-04-2016.

[108] JIMÉNEZ CANO, ROSA. Microsoft demanda a Estados Unidos por las búsquedas secretas de datos de clientes. San Francisco. *El país.* 15 de abril de 2016.

[109] Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

que la conservación de datos se había acreditado como una herramienta de investigación por parte de las fuerzas y cuerpos de seguridad imprescindible para los estados en asuntos de delincuencia organizada y terrorismo. Esta directiva fue anulada finalmente por la sentencia *digital rights*. [110]

Después del duro golpe de los atentados de París y en Bélgica se está reflexionando en torno a la correcta graduación de la seguridad y la privacidad, ya que se ha constatado que los resultados no son los esperados, además de que los grupos terroristas están empleando formas muy avanzadas de comunicación mediante aplicaciones de cifrado. A este respecto, el comisario de migración y asuntos de Interior[111] ha dicho que los atentados terroristas registrados en nuestro suelo han hecho patente la amenaza que suponen para nuestra seguridad. Considera además que el intercambio de información es el nexo de unión en las redes terroristas. En nuestra opinión está justificado que para combatir un fenómeno tan devastador y peligroso como es el terrorismo se empleen todas las herramientas al alcance.

La Comisión Europea[112] reabre así el debate sobre el futuro marco relativo a unos sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad interior. Deducimos de sus declaraciones que se pretende mejorar el acceso a bases de datos comunes en aras de un mayor intercambio de información.

El 10 de marzo de 2016 la Organización para la Seguridad y la Cooperación en Europa, según decisión Nº 1202[113] alentaba a los estados de que dispusieran de una normativa

[110] Sentencias del Tribunal de Justicia de la Unión Europea en los asuntos acumulados C-293/12 y C-594/12.

[111] COMISIÓN EUROPEA, COMUNICADO DE PRENSA. Agenda Europea de Seguridad: Allanar el camino hacía una unión de la Seguridad. Bruselas, 20 de abril de 2016.

[112] COMISIÓN EUROPEA, COMUNICADO DE PRENSA. La Comisión lanza el debate sobre el futuro marco relativo a unos sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad interior. Bruselas, 6 de abril de 2016.

[113] ORGANIZACIÓN PARA LA SEGURIDAD Y LA COOPERACIÓN EN EUROPA. Consejo Permanente. 1092ª sesión plenaria Diario CP Nº 1092, punto 1 del orden del día. Decisión nº 1202 medidas de la OSCE para el fomento de la confianza destinadas a reducir los riesgos de conflicto dimanantes del uso de tecnologías de la información y la comunicación. 10 de marzo de 2016. Idioma original: Inglés.

nacional que fomentara la cooperación y el intercambio de información entre autoridades competentes, incluidas las fuerzas de orden público, a fin de luchar contra el uso de las TIC con fines terroristas o delictivos.

MORENO[114] señala que la universalidad de internet y de las redes comunicativas junto con todos los contenidos digitales, servicios en la nube y pautas de consumo ocio, implican un flujo muy intenso de datos personales, lo cual ofrece la posibilidad a los gobiernos y agencias de inteligencia de invadir la privacidad de millones de ciudadanos.

La sociedad de la información pone más en peligro que nunca la privacidad, esta constituye un bien jurídico que debe ser protegido de forma muy estricta. La directiva de protección de datos[115] de la Unión Europea prima la privacidad de las personas en todo caso, salvo cuando se justifique su intromisión en aras de la seguridad nacional. A mi parecer la previsión es acertada, la privacidad e intimidad de los individuos debe respetarse pero existen motivos que legitiman su intromisión, de lo contrario hablaríamos de privacidad o delincuencia.

Son dos las posiciones que pueden tomarse respecto a este planteamiento, la primera sería la voz de aquellos que defienden la no injerencia del estado sobre los ciudadanos, y la segunda, aquellos que proclaman la intervención total del estado como garante de la pacífica convivencia de los ciudadanos. La solución no es fácil pues el que defienda la postura de la privacidad, cuando vea acusada su seguridad cambiará de opinión y el que postule la máxima seguridad cuando perciba demasiado intrusismo se crispará.

Mediante un juicio de ponderación resulta innegable el hecho de que prevalecen los derechos de los ciudadanos como colectivo sobre los derechos de la esfera individual. Lo anterior no significa que la seguridad nacional pueda utilizarse como puerta trasera para justificar cualquier intromisión arbitraria. Es decir, cada injerencia en la privacidad debe ser adecuada, necesaria, proporcional y apropiada para una sociedad democrática.

[114] MORENO MUÑOZ, MIGUEL. Tensión entre Privacidad y Seguridad en el desarrollo de Internet. *Universidad de Granada. Dilemata año 6,* 2014, n.15, pp. 181-193.

[115] Véase: Capitulo II. Protección de Datos en las comunicaciones electrónicas.

CONCLUSIONES

Llegados a este punto, tras el desarrollo del contenido de este trabajo de fin de grado, nos hallamos en condiciones de establecer las siguientes conclusiones:

I. PRIMERA. *Derecho a la protección de datos.* La privacidad de los datos personales se desprende del concepto de intimidad; la tecnología ha provocado que la esfera personal de los individuos esté compuesta por más y nuevos elementos. El Tribunal Constitucional ha sido el encargado de configurar el derecho a la protección de datos para proteger la vida privada de las amenazas de la informática. De igual forma, entra en riesgo la libertad ideológica, desde el momento en que los datos que se generan aportan información sobre la ideología, religión o hábitos de vida. Los ciudadanos deben tener el control de los datos que desprenden, del mismo modo los encargados de su tratamiento están obligados a custodiarlos diligentemente puesto que son un bien jurídico protegido por nuestra Constitución.

II. SEGUNDA. *Derechos derivados de internet.* Es innegable el hecho de que internet es una herramienta comunicativa, cultural, económica y social, en auge y por ello todo aquel que no tenga acceso corre riesgo de exclusión,: es lo que se denomina como brecha digital. Los países deben garantizar este acceso del mismo modo que sucede con otros servicios básicos. El problema de esta garantía es de índole presupuestaria. En España, en virtud del art. 20 de la Constitución se reconoce el derecho de acceso a internet, aunque no de forma expresa. La necesidad de su inclusión legal es un debate puramente conceptual; los avances tecnológicos van a una velocidad incomparable con la del proceso legislativo, lo cual convierte en inviable la incorporación de tales avances. Alternativamente, la vía más factible es la que ha optado el legislador: la utilización de una fórmula legal abierta que abarca de una forma generalista cuantos avances acaezcan en aspectos tanto técnicos como científicos.

III. TERCERA. *Confidencialidad en las comunicaciones.* El secreto en las comunicaciones es una garantía de las libertades individuales. La regulación europea entiende el derecho a la protección de datos en las comunicaciones como un bien jurídico de vital importancia y de especial protección debido al

constante riesgo al cual está sometido a consecuencia de los avances tecnológicos. La confidencialidad de las comunicaciones no solo está amparada en la regulación de protección de datos y de las comunicaciones, también en el art. 18 de la CE y en el art. 197 del CP.

IV. CUARTA. *Los datos constituyen activos intangibles de las empresas.* La información que se genera no solo tiene valor por formar parte de la privacidad del individuo. Los perfiles digitales constituyen un activo intangible para las empresas, es por ello que deberemos reflexionar acerca de cuál será la forma de contabilizarlos.

V. QUINTA. *Cooperación internacional.* Las comunicaciones son una actividad global, por este motivo deben crearse marcos de cooperación comunes, para regular de una forma más efectiva este fenómeno. Un ejemplo fehaciente a tenor de lo expuesto es la transferencia internacional de datos. Europa debería trabajar en este sentido para conseguir los objetivos citados e iniciar cauces de negociación con otros países.

VI. SEXTA. *Privacidad vs Seguridad.* La regulación europea otorga un carácter confidencial a las comunicaciones electrónicas, bajo consentimiento del usuario, salvo que se trate de una medida necesaria proporcionada y apropiada en una sociedad democrática. Lo anterior no significa que dicha excepción pueda utilizarse como puerta trasera para justificar cualquier intromisión arbitraria. Es decir, cada injerencia en la privacidad debe ser adecuada, necesaria y proporcional.

VII. SÉPTIMA. *Nuevo Reglamento de Protección de datos.* La Unión Europea ha aprobado recientemente el nuevo reglamento 2016/679 de 27 de abril de 2016. Entrará en vigor el año 2018 y significará una gran actualización en materia de tratamiento de datos personales. Actualmente la regulación europea en materia de protección de datos solo se aplica a las empresas que tienen sede o establecimiento permanente en Europa, se trata de un punto de conexión poco práctico ya que la mayoría de las formas de comunicación que utilizamos en la actualidad provienen de empresas extranjeras. El nuevo Reglamento de la Unión

Europea incrementa notablemente su ámbito territorial y se aplicará también a los responsables del tratamiento de datos que no estén establecidos en la Unión Europea pero que oferten bienes o servicios dentro de sus fronteras.

BIBLIOGRAFÍA

APARICIO SALOM, JAVIER. *Estudio sobre la Ley la Protección de Datos*. 4ª. ed. Madrid: Aranzadi, 2013. 464 pp. 978-84-9014-926-3.

BALLESTEROS MOFFA, LUIS ANGEL. *La privacidad electrónica: Internet en el centro de protección.* Tirant Monografías, 2005, Valencia. p. 139

CAMPUZANO TOMÉ, HERMINIA. *Vida privada y datos personales.* Tecnos. 2000. p.69. 8430934766

CARBONELL, JOSÉ Y CARBONELL, MIGUEL. Capitulo II. El acceso a internet como derecho humano. Vega Gómez, Juan. *Temas selectos de Derecho Internacional Privado y de Derechos Humanos.* 1ª. ed. México. D.F: Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas, 2014. pp. 19-39. 978-607-02-54109.

CASTELLS, MANUEL. *La galaxia Internet. Reflexiones sobre internet, empresa y sociedad.* Barcelona, Editorial de Bolsillo, 2003, p.15.

COTINO HUESO, LORENZO. Derechos humanos, internet y TICs". Rey Martínez, Fernando. *Los derechos humanos en España, un balance crítico*. Valencia: Tirant lo Blanch, 2015, pp. 418-480

DAVARA RODRIGUEZ, MIGUEL ANGEL. *Manual de derecho informático.*10ª. ed. Pamplona: Aranzadi, 2008. 528 pp. 9788483558195

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *XVII Encuentros sobre informática y derecho.* 2002,2003. Madrid: Universidad Pontifica de Comillas. M-20.660-2003

FERNANDEZ RODRIGUEZ, JOSÉ JULIO. *Secreto e Intervención de las comunicaciones e internet.* Madrid: Thomson Civitas, 2004. p.41. 8447022463.

GARCÍA SAN MIGUEL, LUIS, et al. Estudios sobre el derecho a la intimidad. Madrid: Tecnos. 1992. p 37. 9788430922208.

HEREDERO HIGUERAS, MANUEL. *La directiva comunitaria de Protección de datos de Carácter Personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*

y a la libre circulación de esos datos. 1ª ed. Navarra: Aranzadi, p. 384. 8481935158.

HERNÁNDEZ GARCÍA-BERRIO, TERESA. *Informática y libertades: La protección de datos personales y su regulación en Francia y España.* 1a. ed. Murcia: Servicio de publicaciones de la Universidad de Murcia, 2004. p. 498.

MARTÍNEZ MARTÍNEZ, RICARD. El derecho fundamental a la protección de datos. Benjamin R. Barber, et al. *Internet, Derecho y Política: Las transformaciones del Derecho y la Política en 15 artículos.* Barcelona: Editorial UOC, 2009. 325 pp. 978-84-9788-789-2. pp. 141-166.

NUÑEZ MARTINEZ, MARÍA ACRACIA. *El Tribunal Constitucional y las libertades del articulo 20 de la constitución española*. Revista de Derecho de la UNED, 2008. núm. 3. pp. 289-317.

OLIVERA L, NOEMÍ. Estado de la cuestión en la relación entre derecho e informática. Derecho y nuevas tecnologías: Universidad de la Plata, 2009. pp.505 a 517.

ORDÓÑEZ SOLÍS, DAVID. *La protección judicial de los derechos en internet en la jurisprudencia europea.* 1ª. ed. Madrid: Derecho de las nuevas tecnologías, 2014. 144 pp. 978-84-290-1810-3.

REIDENBERG R, JOEL. Lex Informatica: The Formulation of Information Policy Rules through Technology, 1998. 76-553 pp.

RUIZ CARRILLO, ANTONIO. *La protección de los datos de carácter personal.* Editorial Bosch, Barcelona. 2000. 1ª ed. 84-7676-818-4 pp. 20-27.

SALDAÑA, JORDI. Capitulo XIII. El asesoramiento jurídico al responsable del tratamiento. Llacer Matacas, María Rosa. *Protección de Datos Personales en la Sociedad de la Información y Vigilancia.* 1ª ed. Madrid: Kluwer, La Ley grupo Wolters, 2011. 380 pp. 9788481268218.

TOMASI, WAYNE. Sistemas de comunicaciones electrónicas. 4ª edición. DeVry Institute of Technology Phoenix, Arizona. p. 1.

URBANO CASTRILLO, EDUARDO. *El derecho al secreto de las comunicaciones.* Madrid: La Ley grupo Wolsters Kluwer. 1ª ed. 2011. Pp. 19-23. 978-84-8126-829-4

ÁLVAREZ CECILIA, RIGAUDIAS. Sentencia Google Spain y Derecho al Olvido. *Actualidad Jurídica de Uría Menéndez,* 2014, pp. 110-118.

ARENAS RAMIRO, MÓNICA. La protección de los datos personales de la Unión Europea. *Revista Jurídica de Castilla y León, 2008*, nº 16, pp. 113-168.

BEGOÑA, GONZALEZ Y MORAL, Mª TERESA. Responsabilidad Penal de Personas Juridica y Corporate Compliance. *Fundesem Business School, Cuatrecasas Goncalves Pereira*, 2015.

CRESPO VITORIQUE, ISABELA. "Asunto Safe Harbor "La Agencia Española de Protección de Datos da el primer paso en relación con las transferencias internacionales de datos a Estados Unidos. *Gómez-Acebo & Pombo*, 2016.

F. GALLEGO, GONZALO. Data protection compliance in Spain Mission impossible? *Hogal Hovells,* 2015, nº1, p. 16.

FRANCO LEGUÍZAMO, CAMILO ARMANDO. De la Lex Mercatoria a la Lex Constructions. *Revista emercatoria,* 2007 nº6, pp 14-15.

MORENO MUÑOZ, MIGUEL. Tensión entre Privacidad y Seguridad en el desarrollo de Internet. Universidad de Granada. *Dilemata año 6,* 2014, n.15, pp.181-193.

PÉREZ LUÑO, ANTONIO ENRIQUE. Informática y libertad: comentario al articulo 18.4 de la constitución española. *Revista de Estudios Políticos* N. 24 noviembre-diciembre, 1981.

COOPER TIM, et al. Personal Data: The emergence of a new asset class. *World Economic Forum, in colaboration with Bain & Company.* 2011.

RODRIGUEZ PUERTO, MANUEL J. La regulación de Internet y la teoría jurídica. *Revista Dialnet,* 2007, pp. 441-464.

ROSEMARY P JAY. Data Protection and Privacy: United States. *London: Law Business Research*, 2014, 191-198, pp. 2051–1280.

ROSINI, VICTORIO. Informática y administración publica. *Revista de Administración Pública*, n. 105, 1994, p. 456.

VILASSAU, MONICA. La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. Privacidad. *Revista de Internet, Derecho y Política, UOC,* 2006, nº2, p. 15

ABANLEX. *Segundo informe sobre la necesidad legal de cifrar información y datos personales.* Informe. Inédito, Abanlex, Despacho de abogados Especializado en tecnología de protección de datos, 2015.

COMISIÓN EUROPEA, DIRECCIÓN GENERAL. *Seguridad y Privacidad para el ciudadano en la Era digital posterior al 11 de setiembre: vision prospectiva.* Informe. Inédito, Institute for Prospective Techonological Studies, 2003.

GABINETE JURÍDICO, et al. *Informe 0011/2014.* Informe. Inédito, Agencia Española de Protección de Datos, 2014.

MÉNDEZ PÉREZ, JESÚS MARÍA. *La protección de datos de carácter personal como derecho fundamental autónomo*. Informe, Inédito. Derecho constitucional III, Universidad de Murcia, 2014.

PERALES ASCENSIÓN, ELVIRA. *Sinopsis de la constitución española.* Informe, Inédito, Universidad Carlos III, 2003.

PÉREZ, RICARDO Y CIMOLI, MARIO, et al. *La nueva revolución digital: de la internet del consumo a la internet de la producción*. Informe. Inédito, Naciones Unidas-CEPAL, 2015

AEPD. El TJUE declara invalidad la Decisión de la Comisión que declara el nivel adecuado de protección de Puerto Seguro. *Nota de Prensa de la AEPD.* 6 de octubre de 2015

ARRIETA, ELENA. ¿Aún hablas de 'big data'? Estás obsoleto. *Periódico Expansión*. 9 de febrero de 2016.

BRUSTEIN JOSHUA. Start-Ups Seek to Help Users Put a Price on Their Personal Data. *New York Times.* 12 de febrero de 2012.

JIMÉNEZ CANO, ROSA. Microsoft demanda a Estados Unidos por las búsquedas secretas de datos de clientes. *El País.* San Francisco. 15 de febrero de 2016.

LÓPEZ LÓPEZ, JOSE CARLOS. La moda del big data ¿En que consiste en realidad? *Periódico El economista.* 27 de febrero de 2014.

MENN, JOSEPH; FINKLE JIM. Privacy vs. Security at heart of Apple phone decrypt order. *Reuters.* Unites States.18 de abril de 2016.

V.MORENO. Guía para entender el laberinto legal del Puerto Seguro. *Periódico Expansión.* Octubre de 2015.

WEBGRAFIA

Agencia Española de Protección de Datos. Guía sobre el uso de las Cookies. [En línea] 1ª ed. [Fecha de consulta: 3 de abril de 2016] [Acceso gratuito]: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

Guía de Facua para enfrentar el Spam. [En línea] 1ª ed. [Fecha de consulta: 12 de abril de 2016] [Acceso gratuito]: https://www.facua.org/es/guias/guia141.pdf

Guía Para Lucha Contra el Spam. Agencia Española de Protección de Datos. [En línea] 1ª ed. [Fecha de consulta: 12 de abril de 2016] [Acceso gratuito]: http://www.uv.es/siuv/cat/norm/luchaspam.pdf