Tesis de Doctorado
Derecho Internacional

EL DERECHO A LA PROTECCIÓN DE DATOS Y A LA PRIVACIDAD. UNA PERSPECTIVA COMPARADA ENTRE LA UNIÓN EUROPEA Y ESTADOS UNIDOS

Autor: Jorge Pérez Miras

Directora: Marycruz Arcos Vargas

2018

A mis hijas, por florecer en nuestra vida y recordarnos lo importante todos los días: el amor, la bondad y la alegría.

A mi mujer, por estar siempre ahí y no dejarme olvidar lo que merece la pena.

Nota de agradecimiento

Una tesis doctoral, llegado una edad, siendo padre de dos hijas inequívocamente inquietas, y trabajador con cierta responsabilidad, no puede realizarse, aún a tiempo parcial, sin la ayuda inestimable de los demás, de tu tribu primaria, y de los amigos y compañeros que acompañan tu vida de manera cariñosa, generosa y amable.
Es por ello, no ya de justicia, sino una necesidad, agradecer previamente aquí, ese esfuerzo anónimo (y anonimizado vista la temática de este trabajo), de esas personas que han formado parte de un esfuerzo menos individual (al igual que la sociedad en que vivimos) de lo que, en principio, se podría pensar.

Bajo su consentimiento procedo a dar aquí un sentido abrazo de gratitud a todas esas personas.

A Marycruz Arcos, mi directora de tesis y sherpa fundamental en el mundo académico. Sin sus consejos, siempre acertados, sin su *accuracy* en casi todos los temas y sugerencias propuestos, este trabajo no hubiera nunca llegado a puerto seguro. Igualmente, sus ánimos en los momentos complicados y su valía personal y humana merecen ser igualmente reconocidos. Al igual que su europeismo militante y sincero, aún en los instantes más oscuros. Gracias.

A mis *parents in law*, (por no llamarlos suegros y ser este un trabajo jurídico), por estar disponibles en el cuidado y caución de unas niñas no siempre risueñas, y, sobre todo, por ser un ejemplo permanente de trabajo, profesionalidad, decencia y elegancia personal en todos los ámbitos de su vida. Gracias.

A mi padre, por haber sabido transmitir una honradez liberal y una bondad personal a sus hijos, entre los que me incluyo, heredada, a su vez, de un familia sin reino, trabajadora y tenazmente mediterránea, que supo llevar con gran dignidad el ideal arrebatado. A él y todos ellos. Gracias.

A mi hermano, un brillante joven profesor de derecho constitucional, cuyos apuntes y recomendaciones han exigido lo mejor de mi torpe actitud, la de, quizá, su alumno más viejo. Su ayuda ha sido oportuna y valiosa. Y sobre todo, por ser una gran persona, un tío (en el sentido familiar y también con sus sobrinas) extraordinario y un profesional incansable. Gracias.

A mi madre, porque madre no hay más que una. Y a su (nuestra) familia porque hizo de una hija única la mujer más fuerte y amorosa que conozco. A ella y todos ellos. Gracias.

A mi mujer, porque sin ella nada (tampoco esta tesis) habría sido posible. Gracias.

A mis hijas, por hacerme levantarme por las mañanas (en todos los sentidos). En definitiva, por existir. Gracias.

Al resto de mi familia y a todos mis amigos. En imposible resumen, a todas las personas que han aportado su pequeño sedimento en este océano de vida. Gracias.

A todos os debo, en menor o mayor medida, quien y como soy, además de un sincero abrazo. Muchas gracias.

GLOSARIO DE ABREVIATURAS

ACT	*Autoridade Para As Condições do Trabalho*
AECG	Acuerdo Económico y Comercial Global
AEPD	Agencia Española de Protección de Datos
ALERTS	Automated Labor Employee Relations Tracking System
ADFUE	Agencia de Derechos Fundamentales de la Unión Europea
APD's	Agencias de Protección de Datos
APEC	*Asia-Pacific Economic Cooperation*
ATA	*Anti-Terrorism Act*
API	*Advance Passenger Information*
CALEA	Communications Assistance for Law Enforcement Act
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo de Derechos Humanos
CAN-SPAM	*Controlling the Assault of Non-Solicited Pornography and Marketing*
CPEA	Cross-border Privacy Enforcement Arrangement
CBPR	Cross Border Privacy Rules
CISA	*Cybersecurity Information Sharing Act*
CESE	Comité Económico y Social Europeo
CETA	*Comprehensive Economic and Trade Agreement*
CIA	*Central Intelligence Agency*
CoE	Consejo de Europa
CFPB	*Consumer Financial Protection Bureau*
CFR	*Code of Federal Regulations*
COPPA	*Children Online Privacy Protection Act*
CPO	*Chief Privacy Officer*
CRA's	*Credit Reporting Agencies*
CRA	*Consumer Reporting Agency*
CSIRT	*Computer Security Incident Response Team*
DIA	*Defense Intelligence Agency*
DPPA	*Driver's Privacy Protection Act*
ECPA	*Electronic Communications Privacy Act*
EEOC	*Equal Employment Opportunity Commission*
EE.UU.	Estados Unidos
ENISA	*European Union Agency for Network and Information Security*
EPIC	*Electronic Privacy Information Center*
FAA	*FISA Amendments Act*
FACTA	*Fair and Accurate Credit Transactions Act*
FBI	*Federal Bureau of Investigation*
FCA	*Federal Communications Act*
FCC	*Federal Communications Commission*
FCRA	*Fair Credit Reporting Act*
FERPA	*The Family Educational Rights and Privacy Act*
FDIC	*Federal Deposit Insurance Corporation*
FEADER	Fondo Europeo Agrícola de Desarrollo Rural
FEAGA	Fondo Europeo Agrícola de Garantía
FISA	*The Foreign Intelligence Surveillance Act*
FISC	*Foreign Intelligence Surveillance Court*
FOIA	*The Freedom of Information Act*

FTC	*Federal Trade Commission*
FRA	*Fundamental Rights Agency*
GLBA	*Gramm-Leach.Bliley Act*
HEW	*Department of Housing, Education and Welfare*
HIPAA	*Health Insurance Portability and Accountability Act*
ICR's	*Investigative Consumer Reports*
INS	*Immigration and Naturalization Service*
INR	*State Department`s Bureau and Research*
IRS	*Internal Revenue Service*
LIBE	*Civil Liberties, Justice and Home Affairs (Committee)*
MSPB	*Merit Systems Protection Board*
NIS	*Naval Investigative Service*
NSA	*National Security Agency*
NSL	*National Security Letters*
OCDE	Organización para la Cooperación y Desarrollo Económicos
ONU	Organización de Naciones Unidas
ORECE	Organismo de Reguladores Europeos de las Comunicaciones Electrónicas
PAMIA	*Privacy Act Modernization for the Information Age Act*
PII	*Personally Indentifiable Information*
PNR	*Passenger Name Record*
PPSC	*Privacy Protection Study Commission*
REPD	Reglamento Europeo de Protección de Datos
RFPA	*The Right to Financial Privacy Act*
SEPD	Supervisor Europeo de Protección de Datos
SNN	*Social Security Number*
TCPA	*Telephone Consumer Protection Act*
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJCE	Tribunal de Justicia de la Comunidad Europea
TJUE	Tribunal de Justicia de la Unión Europea
TTIP	*Transatlantic Trade and Investment Partnership*
TUE	Tratado de la Unión Europea
UE	Unión Europea
UIP	Unidad de Información sobre los Pasajeros
USC	*United States Code*
VPPA	*Video Privacy Protection Act*
VTSP	*Video Tape Service Provider*
WPSPDE	*Working Party on Security and Privacy in the Digital Economy*

ÍNDICE

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”

Edward Snowden

“Si después de yo morir quisieran escribir mi biografía, no hay nada más sencillo. Tiene sólo dos fechas, la de mi nacimiento y la de mi muerte. Entre una y otra todos los días son míos.”

Fernando Pessoa

¿A quién va usted a creer, a mí o a sus propios ojos?

Groucho Marx

PARTE I. INTRODUCCIÓN.

Trataremos en este trabajo de confrontar los dos grandes modelos de protección de la privacidad en el mundo. Por un lado el representado por Estados Unidos y su diversidad legislativa en la materia, que presenta una aproximación a la protección horizontal por materias de la misma; y por otro la bandera de la protección de datos como derecho fundamental y autónomo, representada por la Unión Europea, con su protección jurídica homogénea e influyente como modelo de referencia. Los dos grandes bloques del trabajo pretenden estudiar de manera pormenorizada los principales elementos de cada modelo, siendo el último bloque un análisis de la confluencia obligada de entendimiento entre ellos sobre la necesidad del flujo de datos mundial. Trataremos, al fin y al cabo, de arrojar luz sobre las diferencias, convergencias e influencias mutuas de estos dos principales modelos, pretendiendo algún ánimo conclusivo de carácter general que sirva de prisma de entendimiento de la privacidad a nivel global.

Para que nos sirva de antesala introductoria a este extenso trabajo hemos pensado explicar someramente la definición de los conceptos de privacidad y de protección de datos y tratar de delimitar sus contornos, con referencia al marco ofrecido a priori por los organismos internacionales que se han manifestado sobre el asunto, por una doble razón y utilidad: en primer lugar porque nos da una primera visión sobre su significado y naturaleza, además de anticiparnos su origen diferenciado en las dos orillas del Atlántico, marcando las piedras fundacionales del mismo tanto la Doctrina como la construcción jurisprudencial. En segundo lugar debido a que, tal y como veremos, esta concepción de derecho no surge exactamente de los tratados ni de las organizaciones internacionales, (que se han limitado a establecer marcos de actuación o de posible desarrollo jurídico, recomendaciones al fin o guías de buenas prácticas, - algunas de mayor importancia como las de la Organización para la Cooperación y Desarrollo Económicos, OCDE-), y que dejaremos aquí apuntadas para que nos sirvan de atención a ese marco y la comprobación de su trascendencia (en varias de las acepciones del término).

1. Sobre los conceptos de privacidad y de protección de datos

La privacidad es un concepto con múltiples aristas en su significado. La Doctrina, como veremos, tanto en Estados Unidos como en Europa, se ha esforzado en definir sus contornos y ha tratado de poner el foco de su definición desde la óptica de las distintas perspectivas a través de las cuáles la observaban y defendían.

La construcción filosófico-jurídica en torno a la privacidad ha sido abordada por estudios de gran calado y por numerosos filósofos y juristas, sociólogos y ensayistas políticos que conectan directamente con el fondo de la percepción de la persona y su dignidad, así como en su relación individual y grupal en la sociedad. Hanna Arendt, Stuart Mill, Foucault, Orwell y un largo etcétera se fijan en la importancia del concepto y su relación con el sujeto que lo sustenta.[1]

En Estados Unidos veremos que la privacidad y su derecho de protección se perfilan bien desde el punto de vista constitucional, bien desde el derecho mercantil, a través del desarrollo federal de normas de diversa índole material, e incluso desde el derecho contractual y de propiedad. Desde luego la única diferenciación clara en la normativa estadounidense es la que distingue el bloque de protección de la privacidad frente al Gobierno, del bloque que la protege frente a las entidades privadas, sin que ello suponga unidad aparente en el tratamiento de cada uno en su régimen jurídico respectivo.

En Europa las perspectivas doctrinales sobre la privacidad y la protección de datos parecen gozar de un mayor consenso, en parte por la tradición asimilada más cercana en el tiempo (sobre todo la genéricamente de postguerra y la de su desarrollo de autodeterminación informativa a partir de los años 70) en su consideración como derecho fundamental; y por otra parte por la propia construcción jurisprudencial que va modelando y afianzando su contenido desde la estructura judicial multinivel europea.[2]

[1] El panóptico de Focault o la condición humana de Arendt son clásicos de la filosofía del siglo XX donde se presta atención a la relación privacidad-individuo-sociedad. La novela 1984 de George Orwell puede ser la obra más conocida sobre la pérdida de la Privacidad individual como pérdida de dignidad humana en un medio totalitario de vigilancia. John Stuart Mill la vincula al concepto de Libertad individual y la no interferencia de la Sociedad en ella.

[2] Véase Albers (2014) sobre el carácter poliédrico y expansivo del concepto de protección de datos y el carácter multinivel de su regulación y protección.

La primigenia construcción del concepto de privacidad es americana y doctrinal, y la encontramos en el famoso artículo de Warren & Brandeis "The Right to Privacy" publicado en la Revista de la Universidad de Harvard en 1890, y del que nos ocupamos más adelante en este trabajo. La pretensión del nuevo derecho "a ser dejado en paz" ("The Right to be let alone")[3] será la punta de lanza del discurso jurídico de la privacidad para el futuro. Artículo que sirve de punto de partida e inspiración de esa privacidad jurídica no solo en Estados Unidos sino también en Europa.

Aprovechando esta referencia al artículo de Warren & Brandeis, que si bien americano tiene una fuerza fundadora iniciática del propio reconocimiento general de la privacidad, pasaremos ahora a diferenciar las dos percepciones que se vienen a dar, ya separadas desde su progresiva construcción, entre la privacidad americana y la protección de datos europea. Dos modelos conceptuales de regulación diferenciada que serán analizados a lo largo de este estudio y que, veremos, se influencian entre si, condenados a entenderse en un mundo globalizado.

Ahora bien, debemos no olvidar la realidad del problema al cuál nos acercamos con óptica jurídica desde este trabajo y que lo motiva, para no perderlo de vista. Así, López Aguilar (2015, 71 y ss.) nos sitúa oportunamente en la magnitud del asunto, afirmando que corren malos tiempos para la privacidad, planteándose desafíos enormes a las categorías clásicas del constitucionalismo y de la democracia, con el caso del espionaje masivo, sistemático y sostenido en el tiempo de la NSA estadounidense sobre las comunicaciones telefónicas y electrónicas de millones de ciudadanos europeos sin conexión alguna con el terrorismo, como paradigma. Y nos aclara, para evitar equívocos, que esas prácticas no tienen cobertura en ninguna normativa europea, ni por supuesto tampoco en ningún acuerdo bilateral suscrito hasta la fecha entre la UE y los EE.UU.

Ello es algo que hemos intentado deslindar en este trabajo: el dictado legal y sus garantías, que dista de manera enormemente preocupante de los hechos ilegales de vigilancia que se han podido conocer en este estado de "Gran Hermano Tecnológico" en que nos encontramos.

[3] (Warren & Brandeis, 1890)

1.1 Los fundamentos de la privacidad en América

Junto con el artículo referido de Warren & Brandeis, que sirve de impulso fundacional para la privacidad no solo americana sino con carácter general, podemos observar que ya en las aportaciones doctrinales posteriores en EE.UU. no se ha seguido una linea de delimitación clara de su derecho de protección, ni siquiera dentro de un solo ámbito del Derecho o disciplina jurídica. Y ni siquiera con un mismo enfoque sobre su naturaleza.
Así, como construcción doctrinal netamente americana y de controvertida repercusión (y de la que también nos ocuparemos más adelante), debemos empezar citando el artículo de William Prosser (1960) que distingue la protección de la privacidad en cuatro variantes sobre la base del derecho mercantil. La interpretación que Prosser hace del original de Warren & Brandeis, y su actualización a través del derecho a la responsabilidad civil por quiebra de la privacidad, sería contestado por alguna doctrina. Principalmente por Bloustein (1964), desde la otra costa del país, en la revista de Derecho de la Universidad de Nueva York, poniendo el foco en la pretensión de protección de la dignidad humana y de la personalidad individual como motivación principal de Warren & Brandeis.

Autores estadounidenses como Alan Westin en 1967[4] conciben la privacidad como una forma de control sobre la información personal (que enlazara el Tribunal Constitucional alemán en su concepto de autodeterminación informativa, como veremos). Otros autores[5] la ven como una forma de acceso circunscrito a uno mismo, al individuo. Y otros la conectan de manera reducida al concepto de intimidad, como concepto suficiente.[6]
Otros autores como Julie Cohen (2000, 1427) enlazan privacidad con el desarrollo de la autonomía individual y de la sociedad civil, que conecta con la concepción de Priscilla Regan (1995, 225), que la ve, con perspectiva europea, como un derecho individual y un valor social. Igualmente, dentro de Estados Unidos, Solove (2000, 1127) la ubica dentro del contexto cambiante en el que se encuadra la privacidad en cada momento,

[4] (Westin, 2015).
[5] Gavison (1980) o Iness (1996). Aquí nos ha sido de gran ayuda la magistral obra de Solove y Schwartz (2015, 43-80), en la que sistematizan la ingente aportación doctrinal sobre la privacidad estadounidense.
[6] (Gavison, 1980) (Inness, 1996). Autoras con las que sería oportuno dilucidar si lo privado es sinónimo de lo íntimo o si algo íntimo puede ser independiente de lo privado.

con la importancia de su necesidad normativa para su protección. O la muy interesante aproximación de Anita L. Allen (1999,740) que se muestra inalterable en su defensa de la privacidad como derecho inalienable, del que no se puede disponer. Otros autores (Schwartz, 1999,1658) vinculan directamente su protección al desarrollo de la personalidad y la ven esencial para una sociedad democrática.

En cambio, tenemos a otro grupo de autores más ubicados en la perspectiva de las relaciones sociales, y así citaremos concepciones como la de Simitis (1987, 746) que ve la privacidad como elemento de la estructura social, y la vincula directamente con el buen desarrollo de la democracia. Y apóstoles de la concepción neoliberal de la sociedad también se encuentran en el debate sobre la concepción del término: los más destacados serían Posner (1978, 406 y 421-422) que critica directamente el artículo fundador de Warren y Bradeis, y vincula la privacidad a su valor de mercado para su defensa jurídica, o Cate (2000, 881-882) que enlaza los flujos libres de información a la democratización de oportunidades en Estados Unidos.[7]

De interés nos resulta la aproximación al concepto desde una óptica feminista, y que ha adquirido relevancia en la Doctrina estadounidense. Originalmente en el siglo XIX se dio el particular asunto Rhodes[8], en el que se vinculaba la privacidad o intimidad del hogar por parte del poder judicial americano a la justificación de la violencia dentro de ese hogar, ya que, si bien bajo las leyes del momento no se otorgaba un derecho del marido a reprender o pegar a su mujer, se utilizó por el Tribunal el concepto de privacidad para no castigarlo. Ese precedente judicial hizó que se estigmatizara, desde alguna doctrina, la privacidad en su relación con la igualdad de género. Así Siegel (1996, 2151) lo ve como una primaria coartada para la violencia de género y la preponderancia del hombre sobre la mujer. O la visión de MacKinnon (1989, 191) que vincula el derecho a la privacidad como un derecho del hombre para oprimir a la mujer.

Ahora bien, la perspectiva que compartimos y que conjuga el concepto de privacidad y

[7] Autores que serán muy contestados por otra parte de la Doctrina como Bailey (2004, 26 y 203) que alude a Posner en su teoría sobre los peligros de la "masquerade ball" (globo de mascarada) en el que parecemos instalados con la vigilancia masiva de grandes compañías y gobiernos. O la de Bloustein (1978, 445) que vincula, en sentido contrario a aquellos, privacidad y mejora para la Economía.

[8] State v. Rhodes WL 1278 (N.C. 1868)

su derecho, con el de igualdad entre mujeres y hombres, la encontramos en Anita Allen (1988, 55-56), que se viene a separar de esas visiones, distinguiendo la desigualdad histórica en todos los ámbitos, incluido el doméstico, de la privacidad. Para la autora, la privacidad (como el matrimonio o el amor) no es una amenaza en sí misma para la mujer, más bien al contrario, ya que puede ayudar a esa emancipación (desde la planificación familiar, el aborto, el divorcio…) blandiendo ese derecho a su protección como arma ante la persecución moral; y nos invita a rechazar la utilización del concepto de privacidad como ideología masculina de dominación.

1.2 Los fundamentos de la privacidad en Europa.

A nivel europeo quizá uno de los autores de referencia en la conceptuación de la privacidad y la protección de datos sea Christopher Kuner que junto con Christopher Millard, Dan Jerker B. Svantesson y el estadounidense antes aludido Fred H. Cate, lo categorizan como un concepto "elusivo" (2011, 141-142), centrándose en la tensión entre la concepción de la privacidad como derecho humano o como mercancía personal, la tensión entre su defensa y los intereses gubernamentales, o la tensión entre privacidad y seguridad.

La Declaración Universal de Derechos Humanos de 1948 establece la privacidad en su seno de protección, como nos apuntan los autores (Kuner et al., 2011). También la Convención Internacional de Derechos Civiles y Políticos de 1966, en su artículo 17. En la UE sin lugar a dudas. Si bien en algunos tribunales internacionales de derecho mercantil se tiene en cuenta la segunda visión, más mercantilista.
Como ejemplo de manifestación de libertad del individuo frente a los poderes públicos también se configura ese concepto. Sobre todo en el mundo jurídico y político anglosajón. Y sobre todo en su versión acuciante como protector de la seguridad pública y colectiva (y también individual). De esas tensiones surge ese carácter "elusivo" de la privacidad. Los autores abogan por la aceptación de ese carácter y la tendencia al equilibrio en su configuración, y por el robustecimiento del derecho a la privacidad como especialidad jurídica propia. (Kuner et al., 2011)

En España, Lucas Murillo de la Cueva (1990) o Pérez Luño (1991) han prestado igualmente su atención a la conceptuación de la privacidad y la protección de datos con

maestría. Así Pérez Luño (1991, 304-305) afirma que: "La libertad informática y la autodeterminación informativa son términos más coincidentes aludiendo en ambos casos al nuevo derecho fundamental resultado de la incorporación de la informática a las sociedades contemporáneas…".[9]

Igualmente citaremos la aportación de Rebollo Delgado (2008, 78-80) que nos habla en este ámbito de la "Drittwirkung"[10], idea aceptada en Europa que nos remite a que los derechos fundamentales operan en dos ámbitos: entre el Estado y el ciudadano, pretendiendo el ciudadano la garantía de su ejercicio, y una segunda sobre la posible vulneración por otros ciudadanos, es decir el conflicto de derechos fundamentales entre particulares.[11] Para terminar prestando especial relevancia como antecedente normativo a una norma americana que estudiaremos en este trabajo: la Privacy Act[12] (2008, 87)

Más institucional y positivista se muestra Hustinx (2015, 15-16), que ubica el inicio del derecho a la privacidad en el derecho internacional después de la segunda guerra mundial, en el artículo 12 de la Declaración de los Derechos Humanos, y su protección sustancial con el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH). Destacando la relación conceptual de protección de datos y privacidad en, por un lado, una mayor amplitud, y por otro, una mayor estrechez de contenido. Más amplitud por concernir a otros derechos fundamentales y mayor estrechez porque solo alude a la información personal, quedando sin observar otros aspectos de la vida personal.

[9] Realiza Lucas Murillo de la Cueva (1999, 37) una lúcida ubicación del problema:
"El progreso científico y tecnológico ha traído consigo unas posibilidades antes insospechadas de reunir, almacenar, relacionar y transmitir todo tipo de información (…) la combinación que las técnicas de la información, la automatización y la telemática ofrecen permite obtener, centralizar, utilizar, elaborados del modo que se desee, y conservar por tiempo ilimitado todo tipo de datos de carácter personal. De esta forma resulta que, normalmente, sin que medie advertencia alguna y, en consecuencia, sin que nos percatemos de ello, bien los poderes públicos, bien los sujetos privados, tienen —o pueden tener sin excesivo esfuerzo— conocimiento de amplias parcelas de nuestras vidas y utilizan esa información que de nosotros disponen en su beneficio, pero también de una manera que puede causarnos notorios daños." Combinación que afectará de lleno a la esfera y aspectos de la intimidad, anticipándonos el autor el riesgo de la elaboración de perfiles.

[10] En este sentido véase (De Vega Garcia, 2003) sobre el concepto de "Drittwirkung", y la eficacia frente a particulares de los Derechos Fundamentales.

[11] Y ahí aporta que "…hay derechos fundamentales en que la Drittwirkung es inherente a la propia naturaleza del derecho, a su esencia constitutiva, entre estos se encuentra indiscutiblemente la vida privada…" (2008,80). Contenido de esta idea que nos dice, se desprende del artículo 13 y 17 del CEDH y de la Jurisprudencia.

[12] Nos lo dice así: "En 1974 entrará en vigor en Estados Unidos la "Privacy Act", que será el texto más completo y mejor estructurado jurídicamente hasta esa fecha, y que es el auténtico precursor de las posteriores normas sobre protección de datos de carácter personal en Europa"

Concepción que sirve de puente entre los dos posicionamientos de las orillas del Atlántico sobre privacidad.

1.2.1. La diferenciación netamente europea: La protección de datos

Podremos afirmar que el concepto de protección de datos como elemento desgajado y autónomo del de privacidad es una creación jurídica propia de Europa, vinculada en último término con su precisión como derecho fundamental diferenciado.

Kuner (2009) fija su atención en la distinción netamente europea entre privacidad y protección de datos. Se hace eco además de un cierto clamor internacional para la regulación de las transferencias de datos a nivel global que comenzaría con la Declaración de Montreal en 2005 en la "27th International Conference of Data Protection and Privacy Commissioners".[13]

Esa diferenciación entre el concepto de protección de datos y de privacidad parte para Kuner (2009), de la tradición jurídica alemana, de las leyes de los años 70 (principalmente la Ley de Hesse de 30 de septiembre de 1970, la Ley francesa de 6 de enero de 1978 sobre informática y ficheros y libertades individuales, y la Ley Sueca de Protección de Datos de 11 de mayo de 1973), así como del pronunciamiento judicial del Tribunal Constitucional alemán sobre la Ley del Censo de 1983, que va perfilando el concepto del derecho a la autodeterminación informativa, (que pasamos a referir) tan importante en Europa y de gran influencia en la Directiva de 1995.[14]

Es así, en la sentencia del Tribunal Constitucional alemán sobre la Ley del Censo de 1983 donde se declara como clave de bóveda de la norma constitucional alemana el valor y la dignidad de la persona actuante con libre determinación en una sociedad libre. Ante las nuevas amenazas que presenta la sociedad en aquel momento y que llegan hasta hoy, se da esa significación especial del derecho a la autodeterminación informativa del que va a partir el derecho a la protección de datos. Los datos partirán ahora del reconocimiento del derecho fundamental a esa autodeterminación que surge

[13] En la que se animaba a la Naciones Unidas a la creación de un instrumento legal, general y vinculante al respecto. O en 2009 desde el sector público por un grupo de autoridades públicas (autoridades de protección de datos) en su defensa, presidida por la Agencia Española de Protección de Datos. Basados ambos encuentros en el peligro de la ausencia de estándares internacionales en el tratamiento de datos vinculados al gran intercambio global de los mismos, y la interacción del sector público y privado de manera equiparable en esa "autopista mundial" de datos.

[14] E igualmente recomendable la lectura de Heredero Higueras (1983) sobre la sentencia referida.

directamente de la personalidad, su desarrollo y su dignidad.[15]

Así la sentencia nos lo relata y define con la habitual maestría del Tribunal Constitucional de Karlsrue:

> *"… la autodeterminación individual presupone (…) que a los individuos se les dé libertad para decidir sobre qué actividades emprender y cuáles omitir, incluyendo la posibilidad de comportarse efectivamente de conformidad con esa decisión. Quien no pueda estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información. Quien piense que los comportamientos atípicos pueden en todo momento pueden ser registrados y archivados como información, utilizados o retransmitidos, intentará no llamar la atención incurriendo en ese tipo de comportamientos (…) Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar."*[16]

Como nos dice Kuner (2009, 309) los conceptos de privacidad y protección de datos son gemelos pero no idénticos (serían conceptos mellizos si seguimos el casticismo de la lengua española). Kuner observa como en Europa el concepto de privacidad tiene un elemento "más allá", más amplio que el de protección de datos en la esfera personal,

[15] En el Considerando II de la sentencia sobre la Ley alemana del Censo de 1982 se sustancia esta nueva teoría que abandona la previa del Tribunal de las tres esferas de la personalidad (la esfera privada, la esfera íntima y la esfera individual) como medio de defensa de la Privacidad e Intimidad, y que ya presentaba limitaciones en la nueva era informática.

[16] Sentencia sobre el Censo de Población del Tribunal Constitucional alemán. Sentencia de la Primera Sala, del 15 de diciembre, 1983 (Sentencia BVerfGE 65, 1)

mientras que Estados Unidos ve valores de protección también más amplios en la privacidad, con decisiones jurisprudenciales en clave constitucional. Si bien el concepto de protección de datos es una invención jurídica netamente europea, que ha influido en buena parte del resto del mundo que ha optado por su recepción.[17]

1.2.2 El derecho fundamental a la protección de datos: su contenido

Numerosos autores han investigado la protección de datos como derecho fundamental, atendiendo a factores diversos en su consolidación con tal carácter. Esa labor, unida a los pronunciamientos judiciales, va separando progresivamente la privacidad de la intimidad hasta llegar esta a una determinación de mayor especificidad en el concepto europeo de protección de datos.

Serrano Pérez (2005, 252), en su estudio que apunta el reconocimiento constitucional de la protección de datos en España como pionero, lo circunscribe a un elemento más acotado que la referencia del término privacidad anglosajón.[18] Se perfilan así los elementos del derecho en: el consentimiento, el derecho de información, el derecho de acceso, el derecho de rectificación, el derecho de cancelación y el derecho de oposición.

Piñar Mañas (2009, 89-99) nos expone que: "…Al par de conceptos intimidad-informática, se añade ahora uno más: valor económico de los datos personales en relación con el respeto a los Derechos y en particular al Derecho a la intimidad" y ubica la consideración del derecho como derecho fundamental en el 2000 con la proclamación de la Carta de Derechos Fundamentales de la Unión Europea, que califica de "giro copernicano"[19] en este ámbito. Y apunta la consolidación del concepto de protección de datos frente al original de autodeterminación informativa, que apuntala también el Tribunal Constitucional alemán en su sentencia de 27 de febrero de 2008[20], y que alude

[17] Kuner (2009, 309) se hace eco de las aprobaciones legislativas desde Argentina, Canadá, Hong Kong, Israel y Rusia en esa incorporación del concepto de Protección de Datos.

[18] Nos dice que: "la palabra privacidad resulta de la traducción más fidedigna del término anglosajón "privacy", aunque con su uso en nuestro ordenamiento se hace referencia sólo a las peculiaridades de la informática y los datos, pues el resto de contenidos de la "privacy" encuentran reflejo independiente entre nosotros a través de categorías constitucionales diferenciadas".

[19] Advirtiendo de que "se abre una nueva etapa, en la que nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad".

[20] Sentencia del Tribunal constitucional federal alemán BVerfGE de 27 de febrero de 2008, (1 BvR

a todo tipo de elementos electrónicos e informáticos incluidos en su protección; y de los sistemas tecnológicos como medios para expresar la personalidad y de los peligros que conllevan. Para el autor adquiere igualmente gran importancia el principio de control independiente como elemento definitorio del derecho a la protección de datos.

Igual consideración de ese avance propiciada por la Carta de Derechos Fundamentales de la UE (CDFUE), lo constata Canales Gil (2007, 21) que asevera que "a diferencia de lo señalado en la Resolución 509 de la Asamblea del Consejo de Europa, en la Resolución del Parlamento Europeo de 1979 y en el propio Convenio 108 ya no se relaciona el derecho a la protección de datos de carácter personal ni con la informática ni con el derecho a la intimidad de las personas. Se reconoce, ahora sí, un derecho sustantivo, autónomo, el derecho de toda persona a proteger sus datos de carácter personal de todas las injerencias que se puedan producir…"[21]

1.2.3 La labor jurisprudencial en el proceso de consolidación.

Igualmente la Jurisprudencia del Tribunal de Justicia (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH) se ha revelado imprescindible en el modelado y desarrollo del concepto de protección de datos en Europa.

Algunos autores, así, ponen el foco sobre esa labor jurisprudencial (y también institucional), como es el caso de Arenas Ramiro (2008, 121-122), que nos dice que "el derecho a la protección de datos personales se ha desarrollado en el ordenamiento jurídico comunitario a través de la actividad del TJCE, «vía pretoriana», como todos los demás derechos fundamentales, pero, también, y especialmente, a través de la actividad normativa de las instituciones, que ha desempeñado un papel determinante en el reconocimiento y desarrollo del derecho y en la labor del TJCE."[22]

Fija su atención la autora además en el primer caso relativo a la protección de datos personales resuelto por el TJCE, el conocido caso Stauder[23] (STJCE de 12 de noviembre

---

370/07)

[21] Igual sentido en su atención brinda a la CDFUE Martínez Martínez (2007) y asimismo en clave legislativa Ruiz Miguel (2003, 15)

[22] Arenas Ramiro (2008, 121-122). Al analizar la STJCE de 26 de junio de 1980, caso National Panasonic; y la STPI de 15 de mayo de 1997, caso N. vs. Comisión. Aunque alega la importancia definitiva de la CDFUE para el nuevo status del derecho se centra en la labor del TJCE en el inicio del reconocimiento del derecho a la protección de datos (vida privada, dignidad) como principio general, para pasar después a incorporar la jurisprudencia del TEDH en la materia.

[23] Que si bien se suele estudiar desde la perspectiva y enfoque de la primacía o eficacia directa del ordenamiento comunitario, su origen sustancial está en la protección de datos del señor Stauder que no

de 1969) en el cual el Tribunal se plantea si "la revelación del nombre del beneficiario a los vendedores era compatible con los principios generales del Derecho comunitario". Caso que además abre la veda para la presentación de demandas relacionadas con datos personales[24], que el Tribunal irá resolviendo de forma diferente, si bien sin pronunciarse expresamente sobre su protección, bien por falta de prueba suficiente o bien por cuestiones procesales.

A partir de este caso, ante el TJCE se presentarán demandas que se resolverán de forma diferente. En primer lugar, se plantearon ante el TJCE demandas que el Tribunal sustanció sin pronunciarse sobre la protección de los datos personales, bien por no poder demostrar el daño causado, bien por cuestiones procedimentales. Y otra etapa[25]se abre entre estas primeras sentencias y las inmediatamente anteriores a la aprobación de la Directiva (que veremos en su epígrafe) en las que el Tribunal ya tiene en cuenta el derecho a la protección de datos personales como parte de los principios generales del derecho comunitario, aunque sin referirse a él expresamente, y aplicando el test de proporcionalidad del TEDH para comprobar si ciertas medidas relacionadas con el tratamiento de datos personales estaban o no justificadas.[26]

Por tanto, en consonancia con parte de la historia jurídica y política de la Unión Europea que sabemos va perfilando expansivamente derechos fundamentales a su nivel, parece que los impulsos de construcción del derecho fundamental a la protección de datos parten de un fracaso: en este caso del de la suscripción unánime por los entonces

---

se quería ver vergonzantemente señalado en su recibo de cupo de mantequilla para pobres.

[24] Arenas Ramiro, (2008, 122-123). Nos pone como ejemplos los siguientes: STJCE de 7 de noviembre de 1985, caso Stanley George Adams, relativo a la transferencia o cesión de datos personales y la divulgación de los mismos; o la STJCE de 7 de octubre de 1987, caso Strack, y Conclusiones presentadas al caso por el Abogado General Darmon el 2 de julio de 1987, donde se analizaba el acceso a los datos médicos contenidos en el expediente personal de un funcionario de las Instituciones europeas.

[25] Arenas Ramiro, (2008, 123). Lo ubica en su origen y lo ejemplifica en el caso National Panasonic, de 26 de junio de 1980, en el que se reconoce por primera vez el derecho a la vida privada, y el caso Hoechst, de 21 de noviembre de 1989, en el que se cuestiona que las personas jurídicas puedan ser titulares del derecho a la vida privada.

[26] Arenas Ramiro, (2008, 123) explica este itinerario de construcción del derecho fundamental. Nos dice que "con el fin de lograr una libre circulación de datos personales entre los Estados miembros que no obstaculizara el mercado interior y la aproximación de las regulaciones existentes, se propuso que los Estados miembros de la Comunidad firmaran el Convenio 108 sobre Protección de Datos Personales. Ante el fracaso de esta propuesta, se decidió elaborar la normativa europea necesaria para la aproximación legislativa entre los Estados miembros en materia de protección de datos personales". Se refiere al Convenio núm. 108, hecho en Estrasburgo el 28 de enero de 1981, relativo a la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; y Recomendación 81/679/CEE, de la Comisión, de 29 de julio de 1981, por la que se anima a los Estados miembros de la Unión a firmar el Convenio 108. Convenio que estudiaremos más adelante.

Estados miembros del Protocolo 108, que impulsará así la adopción de la Directiva de 1995.[27]

Igualmente Campuzano Tomé (2000, 55) se fija en la doble vertiente de su contenido. Por un lado, la de la protección de datos como objeto de valor de mercado enfocado al comercio electrónico como principal para el intercambio de bienes y su vinculación con la protección del consumidor; y por otro la vertiente referida a la protección de la persona en su derecho a la vida privada. Apuesta la autora por la prioridad de este segundo prisma en su análisis, siguiendo el planteamiento del presidente del TEDH, el juez Rysdall. Se hace eco además del largo camino hasta la asunción de los derechos fundamentales en el seno de la UE, del que este derecho a la protección de datos es vivo ejemplo. Y menciona por supuesto la labor del TJUE en esa pavimentación jurídica. (Campuzano Tomé, 2000, 73) en referencia a Rysdall, R. (1992).

En resumen, vemos como la construcción del concepto de protección de datos en Europa y su contenido parten en primer lugar de las leyes nacionales de los años 70 sobre la materia, del Convenio 108 del Consejo de Europa, de la Carta de Derechos Fundamentales de la UE y de la perfilación jurisprudencial, prendiendo en el Tribunal Constitucional alemán al que tomará el testigo el Tribunal de Justicia, con la influencia del TEDH. Y ello para culminar normativamente en la Directiva en el año 1995 y hoy en el Reglamento General. De todo ello podríamos deducir que el derecho a la protección de datos tiene un origen e impulso netamente europeo. Suscribimos así de manera recapituladora la justificación última de esta protección con Rebollo Delgado (2008, 101): "Cabe concluir que el fundamento de la protección de datos, independientemente de la denominación por la que optemos (…) protege originariamente la dignidad de la persona humana, y constituye una ámbito de libertad del individuo, y tiene una concreción inexorable en los derechos clásicos de la personalidad como son el honor, la intimidad y la propia imagen".

[27] Así Arenas Ramiro, (2008, 128) coincide con esta idea: "El reconocimiento de un derecho a nivel europeo, como puede ser el derecho a la protección de datos personales, se ve influenciado por las tradiciones constitucionales comunes y por el CEDH (y, más concretamente, por la interpretación que del mismo haga el TEDH). Pero este «intercambio de influencias» no va sólo de abajo hacia arriba, sino que la regulación a nivel europeo ha contribuido muy mucho a configurar el contenido del derecho a la protección de datos personales en cada uno de los Estados miembros."

2. Directrices internacionales sobre privacidad

2.1 Las Directrices de la ONU

La Organización de Naciones Unidas es la institución internacional surgida a raíz de la segunda guerra mundial con la misión general de asegurar la paz y la seguridad en el mundo, y que se viene a formalizar con la firma de su Carta el 26 de junio de 1945 en San Francisco. En su artículo 1.3 además establece como propósito: "realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión..." y en el artículo 55 incluye la promoción de: " a. niveles de vida más elevados, trabajo permanente para todos, y condiciones de progreso y desarrollo económico y social; b. La solución de problemas internacionales de carácter económico, social y sanitario, y de otros problemas conexos; y la cooperación internacional en el orden cultural y educativo; y c. el respeto universal a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión, y la efectividad de tales derechos y libertades."

La protección de la privacidad, así, como componente de los derechos humanos y elemento internacional necesario en el ámbito económico y social, se manifiesta como uno de los factores a los que prestar estrecha atención por las Naciones Unidas.

2.1.1 La Resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990 por el que se aprueban las Directrices para la regulación de los archivos de datos personales informatizados.

Se trata de un documento de orientación para los procedimientos reguladores de estas prácticas, dejando la iniciativa a cada Estado que deberá sujetarse a unos elementales

principios de garantía mínima a la hora de elaborar esta normativa: el principio de legalidad y lealtad, el principio de exactitud, de especificación de la finalidad (pertinencia y adecuación, no utilización posterior salvo con consentimiento y conservación limitada a lo necesario), de acceso, de no discriminación, la posibilidad de excepción (mencionando concretamente la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros...), el principio de seguridad, el de supervisión y sanción y el de flujo internacional de los datos con salvaguardas similares. Ello en un campo de aplicación que se extiende a todos los archivos informatizados públicos y privados, dejando los manuales a opción del Estado (algo que el tiempo informático ha venido a corroborar como un acierto, estando los archivos manuales cada vez más en desuso). La otra cara importante del documento es la previsión para los Estados de una "autoridad legalmente competente para supervisar la observancia de estas directrices", que pone las bases de necesariedad para las autoridades de control (orientación B).

2.1.2 Las Resoluciones de la Asamblea General y del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital[28]

Tras el convulso verano de 2013 en el que Snowden se nos revela ante el mundo como protagonista en lo que a privacidad global se refiere, un numeroso grupo de países dan su patrocinio a la declaración de 2013 sobre el derecho a la privacidad en la era digital, tras observar que el ritmo del desarrollo tecnológico "incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos". La Organización de Naciones Unidas se muestra "profundamente preocupada por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos" esa vigilancia, para afirmar "que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad". Para hacer una exhortación última a los Estados a respetar y proteger el derecho a la privacidad, adoptar medidas contra sus violaciones, revisar sus

[28] Resolución de 20 de noviembre de 2013 de la Asamblea General así como la Resolución de 24 de marzo de 2015 y la Resolución de 22 de marzo de 2017 del Consejo de Derechos Humanos.

procedimientos y prácticas relacionadas y establecer y mantener mecanismos de supervisión nacionales que sean independientes y efectivos.

Dos años después, en 2015 se mantiene viva la llama de la preocupación y la actualidad del debate sobre la privacidad y los riesgos de la misma en el entorno global por parte del Consejo de Derechos Humanos, si bien con algunas nuevas observaciones como las relativas a los metadatos o a la elaboración de perfiles. Se añaden además apuntes importantes al problema y a la preocupación sobre las amenaza en algunos países hacia promotores de los derechos humanos y sobre las injerencias a la privacidad como resultado de las mismas. Todo ello que anticipa el importante elemento sustancial de la Resolución cual es el nombramiento de un Relator Especial sobre el derecho a la privacidad para un período de tres años. Entre su funciones destacamos la de información y seguimiento del problema, detección de obstáculos a la promoción y protección del derecho a la privacidad, difusión, concienciación y denuncia sobre las violaciones que observe en base al artículo 12 de la Declaración Universal de Derechos Humanos y al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y la presentación de un informe anual al Consejo de Derechos Humanos y a la Asamblea General.[29]

En marzo de 2017 el Consejo de Derechos Humanos sigue prestando atención a la privacidad en la era digital, reproduciendo las preocupaciones de su anterior resolución. Menciona la labor del Relator, figura creada en aquella, y añade nuevas preocupaciones tales como la elaboración de perfiles que puedan suponer discriminación, la falta de consentimiento informado y la interferencia de la falta de respeto a la privacidad en otros derechos relacionados. Renueva el interés en las medidas de seguridad técnicas sobre confidencialidad, y considera el entorno de comunicaciones vital para la defensa de los derechos humanos, y exhorta a los Estados para un respeto más pormenorizado, y un esfuerzo de cumplimiento de las recomendaciones establecidas hasta esa fecha (letras a) a k) del punto 5). Se habla ya de mecanismos de supervisión "de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales..."; de un "acceso a un recurso efectivo" (letra d)

[29] Podremos apuntar que esta asunción de conocimiento especial por parte del Consejo de Derechos Humanos disipa aún más las dudas sobre la consideración de la privacidad como derecho fundamental.

y letra e)), de la promoción de la educación a estos efectos, de la abstención "de exigir a las empresas que adopten medidas que interfieran con el derecho a la privacidad de manera arbitraria o ilegal" (letra i).[30]

Novedad importante es que la exhortación del Consejo de Derechos Humanos de Naciones Unidas no se queda en los Estados, sino que se dirige ya directamente también a las empresas para que "asuman su responsabilidad de respetar los derechos humanos de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos", alentándolas a que "busquen soluciones técnicas que aseguren y protejan la confidencialidad de las comunicaciones digitales, que pueden comprender medidas de cifrado y anonimato..." (Puntos 8 y 9).[31]

2.1.3 Primer Informe del Relator Especial[32]

La figura del Relator Especial cobra una importancia destacada y novedosa en el ámbito de las Naciones Unidas, que viene a ser un reflejo de la relevancia que la privacidad va adquiriendo como asunto mundial. Sus informes serán elementos "soft law" de importante calado para tomar el pulso a la consideración sobre la misma.

El informe, sobre la base de trabajo del estudio comparado y del estudio temático, se presenta como el primer trabajo del Relator tras su creación, y se posiciona como una toma de contacto con el problema desde la propia institución. En esa toma de posición alerta sobre la importancia que supone para la privacidad la actuación de las empresas y su manejo de datos (en comparativa con los Estados). Importancia que no va

[30] Con clara evocación que surge del caso del FBI en su presión a Apple, que recordaremos versaba sobre las presiones no justificadas en la Ley por parte de la agencia de investigación estadounidense sobre la famosa compañía para que le suministrara un acceso al teléfono móvil de un supuesto terrorista, abriendo las "puertas de atrás" para acceder a la información en él contenida sin orden judicial ni, evidentemente, consentimiento del titular.

[31] Debemos hacer alusión también a otras resoluciones del Consejo de Derechos Humanos de Naciones Unidas relacionadas de manera íntima con esta protección, como aquellas bajo el título de "Promoción, protección y disfrute de los derechos humanos en Internet", que tienen una perspectiva más amplificada, aún también centrada en la Privacidad, y que se preocupan además por las brechas de seguridad y la violación de los derechos humanos en Internet, en general. Mencionaremos la Resolución de 29 de junio de 2012 y la Resolución de 27 de junio de 2016.

[32] El primer informe del relator especial se presenta en la 31 sesión del Consejo de Derechos Humanos de la ONU de 8 de marzo 2016 (número A/HRC/31/64)

correlacionada con la actuación concernida en su protección por las compañías. Junto a ello, el Relator presta atención a los programas de seguridad y prevención del terrorismo, que a veces en su desarrollo, atentan a la privacidad de la mayoría de la gente que se encuentra en el fuego cruzado de esa lucha de ciberataques y contraespionaje. Además en su estudio ha merecido especial interés el análisis de los datos abiertos y el *Big Data* y su impacto para la privacidad, la genética, los datos biométricos y las bases de datos forenses; así como la incidencia en la dignidad y reputación de la persona que puedan provocar las violaciones de la privacidad.[33]

Empieza el informe dejando claro, que, a pesar de la existencia del concepto de privacidad en todas las sociedades y culturas, no es un concepto universalmente aceptado en su definición de manera homogénea, con una variada legislación y marcos normativos diferentes que lo atestiguan. Junto a esa falta de valor común legal se añade la dificultad para su protección en base a las múltiples circunstancias socioeconómicas y tecnológicas que se dan en los distintos territorios del planeta. Siendo esa necesidad de establecimiento de un mínimo común denominador en la privacidad universal, la prioridad del Relator de la ONU. Utilizando para ello lo que considera una aproximación que considera de tipo universalista: la de ser un derecho necesario para la dignidad y libertad personales. Y apuntamos nosotros, elemento esencial de los derechos fundamentales y humanos.[34]

Otro elemento que destaca el informe es el caso Schrems que califica como "el inicio del fin judicial de la vigilancia masiva". Siguiendo el caso Schrems también destaca como clave la importancia de la defensa de estos derechos ante una institución supranacional.[35]Junto a ello cita el Relator que la mera existencia de medidas de vigilancia secreta es una violación del derecho a la vida privada. Como elemento

[33] De hecho dedica todo el Anexo II (en 13 puntos de desarrollo) del informe a una "mirada en mayor profundidad" sobre los asuntos del "open data" y del Big Data.

[34] En sus observaciones sobre el estado de la privacidad durante los años 2015 y 2016 llega a algunos elementos de interés: la comparativa contrapuesta entre los Países Bajos y Estados Unidos a la hora de abordar la encriptación por parte de las empresas tecnológicas y la necesidad o no de establecer "puertas de atrás" para el acceso por motivos de persecución criminal. Holanda se opone en su legislación a esa entrada trasera mientras que la posición de Estados Unidos es más preocupante para el Relator (mencionando expresamente el pulso del FBI con Apple al respecto).

[35] Sentencia Schrems que analizamos en la parte final de la tesis.

también clave alumbrado por el Tribunal Europeo de Derechos Humanos se cita el caso Roman Zakharov v. Russia de 4 de diciembre de 2015.[36]

Otro elemento "caliente" de la privacidad en estos años recientes se da en el proyecto de ley británica sobre poderes a la investigación, calificando sus medidas de desproporcionadas e intrusivas para la privacidad.[37]

Por último, deja abierta la puerta a lo que denomina los "primeros pasos para la ciberpaz", con la alusión a la voluntad de diálogo sobre la evitación del robo de información por medios cibernéticos entre China Brasil, Rusia, Estados Unidos y Gran Bretaña y otros miembros del G20.

Tras el análisis, el Relator presenta su plan de acción de 10 puntos sobre el derecho a la privacidad y su relación con otros derechos humanos:

– Ahondar en el sentido y significado del derecho a la privacidad.

– Aumentar la concienciación entre la ciudadanía.

– La creación y mantenimiento de un diálogo estructurado y continuo sobre la privacidad entre los actores implicados.

– Una aproximación integral a las garantías legales, procedimentales y operacionales sobre la privacidad.

– Un renovado énfasis en las medidas técnicas de seguridad.

– Un diálogo especialmente centrado en el mundo de la Empresa, que maneja más datos que el sector público.

– La promoción de avances nacionales y regionales en la protección.

– Aprovechar la energía e influencia de la sociedad civil.

– La atención a las realidades actuales: el ciberespacio, la ciberprivacidad, el ciberespionaje, la ciberguerra y la ciberpaz.

[36] Punto 37 del informe. Citándola como medida "test" para seguir un estándar de protección en la legislación contra la vigilancia masiva.
[37] Investigatory Powers Bill sobre la versión última de 1 de marzo de 2016

– Mayor inversión en derecho internacional, que ayude al desarrollo de nuevos instrumentos legales para la privacidad.[38]

El informe termina con las conclusiones sobre la actualidad de la privacidad y su problemática. Se trata de un tema de máxima actualidad política, judicial y de concienciación individual a nivel global, con análisis contradictorios entre las diferentes formas que los distintos gobiernos tienen para conciliarla con las exigencias de la seguridad (haciendo mención a los Tribunales europeos y estadounidenses en su salvaguarda). Adquiere además especial interés la consideración comercial que se está teniendo sobre la privacidad por parte de las empresas, debido a la toma de conciencia en este sentido por los consumidores a nivel mundial.

Se observa además por el Relator la muy importante diferencia entre los Gobiernos de los países en esa concienciación: de una parte, algunos que ponen trabas a la defensa de la privacidad y otros que en cambio promueven su defensa. El informe implica, en general, a casi todos, para la consecución de avances en sus medidas de seguridad y técnicas (como la encriptación) para estos fines. Trata de fomentar el Relator, al fin, una "privacy-friendly agenda" a nivel global como opuesta a una mentalidad de "mando y control" sobre el tema.

2.2 Las Recomendaciones sobre privacidad de la OCDE[39]

La OCDE, dentro de la ola de concienciación jurídica internacional de los años 70 sobre las aplicaciones y desarrollo de la informática, elabora y aprueba en 1980 unas directrices sobre privacidad internacional que tendrán una gran influencia en la aprobación de las normas de protección posteriores por parte de los países (y también con especial incidencia en las comunitarias).

[38] El Anexo III con el título "Further reflections on the notion of privacy" apunta a ese necesario diálogo de entendimiento para no solo definir el concepto, sino su mejor manera de protegerlo, con aportación de todas las partes interesadas e implicadas.

[39] Disponibles en inglés en (Recuperado el 17 de septiembre de 2018):

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1

Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (en adelante directrices de privacidad) pasaron a hacerse efectivas el 23 de septiembre de 1980, siendo útiles y claros principios aplicables a todas las fases del procesamiento de datos y a sus usuarios, tanto a nivel nacional como internacional. Tienen el carácter de directrices armonizadoras con ánimo global. Recordemos que las directrices no tienen naturaleza jurídicamente vinculante[40] pero, como veremos, resultarán de gran influencia inspiradora en las sucesivas normas de protección.

Fue la necesidad de homogeneización jurídica global la que impulsa la elaboración de estas directrices. Los trabajos se comienzan con un Grupo de expertos en 1978 para estudiar esa armonización legal necesaria, que aportarían, además, un memorándum explicativo de las razones y elementos importantes que habían seguido a la hora de elaborar sus recomendaciones y directrices.

El problema principal que se pretendía atajar es la amenaza para la intimidad personal y para los derechos individuales que el nuevo tratamiento de datos venía a suponer. Había además, planteamientos en común en los ordenamientos nacionales sobre los cuáles se podían extraer elementos comunes de armonización jurídica. Y reconocen además que los problemas no podían ser solucionados a escala nacional, precisamente por su propia naturaleza y la de sus flujos, justificando así su actuación como organización internacional de carácter consultivo.

El Grupo de expertos se interesó en particular por algunas cuestiones clave (que recibían atención divergente a escala nacional). Estas abarcaban la de los hechos específicos o delicados (su carácter universal o no), la del tratamiento automático de datos, la cuestión de las personas jurídicas, la de los recursos y sanciones, los mecanismos básicos de implantación, la elección del Derecho aplicable (y reconocimiento de sentencias extranjeras), las excepciones o la cuestión de parcialidad, que venía a reconocer el conflicto inherente entre la protección de datos personales y la libre circulación transfronteriza de esos datos.

[40] Junto a las directrices debemos destacar otros pronunciamientos de la OCDE relacionados, como son la Declaración sobre flujos de datos transfronterizos adoptada por el Consejo de ministros el 11 de abril de 1985, la Recomendación relativa a las directrices de política criptográfica, adoptada el 2 de marzo de 1997, así como la Declaración ministerial sobre la protección de la privacidad de las redes globales de Ottawa de 19 de octubre de 1998. Más adelante se formulará la Recomendación relativa a la cooperación transfronteriza en la aplicación de las legislaciones que protegen la privacidad de 12 de junio de 2007.

Así el Memorándum del Grupo de expertos en su punto 25 deja clara su motivación y recomendación de observancia, que va dirigida a sus países miembros si bien tiene ánimo de inspiración universalista, se hace "*con vistas a:*

a) conseguir la aceptación entre ellos de ciertos criterios mínimos de protección de la intimidad y de las libertades individuales con respecto a los datos personales;

b) reducir al mínimo las diferencias entre sus normas y prácticas nacionales pertinentes;

c) garantizar que en la protección de los datos personales toman en consideración los intereses mutuos y la necesidad de evitar injerencias indebidas en la circulación de datos personales entre ellos, y

d) eliminar, en cuanto sea posible, los motivos que podrían inducirles a restringir la circulación transfronteriza de datos personales por causa de los posibles riesgos asociados a esa circulación."

Indica además el Prólogo de la Declaración de las Directrices la importancia del asunto en relación con los derechos individuales, ya que establece que lo que trata de evitar son "*vulneraciones de derechos humanos fundamentales, tales como el almacenamiento ilícito de datos personales, exactos o inexactos, o el abuso o la revelación no autorizada de los mismos*". Tienen además un objetivo armonizador facilitador de la circulación de la información y que no dificulte las relaciones económicas.[41] Y establecen una definición de datos personales que se convertirán en un clásico legal para las posteriores regulaciones: "toda información correspondiente a una persona identificada o identificable" (Letra b) del punto 1 de la Parte 1).[42]

Tambien podemos destacar que la posibilidad de excepción (incluida aquella por razón de soberanía y seguridad nacionales y al orden público) a los principios de ser lo más limitadas posibles y con publicidad (Puntos 3 y 4 de la Parte 1).

[41] Destacaremos su inspiración directa para la Directiva 46/95/CE.

[42] Las Directrices definen su objetivo también de forma negativa dejando claro que "*no debieran interpretarse en el sentido de que impiden:*
a) la aplicación, a diferentes categorías de datos personales, de distintas medidas de protección según su índole y el contexto en el cual se recojan, almacenen, traten o divulguen;
b) la exclusión, respecto a la aplicación de las Directrices, de datos personales que evidentemente no contienen ningún riesgo para la intimidad ni para las libertades individuales, o
c) la aplicación de las Directrices sólo al tratamiento automático de datos personales."

2.2.1 Los Principios.

Los Principios Básicos de aplicación recogidos en las Directrices son:

- Principio de limitación de la recogida. Con medios lícitos y justos.
- Principio de calidad de los datos. Pertinentes para los efectos para los que se vayan a utilizar.
- Principio de especificación de la finalidad. O de finalidad específica que debe concretarse a más tardar en el momento de la recogida, limitando su posterior utilización a la misma.
- Principio de limitación de uso. Para otros usos no deberían revelarse salvo con el consentimiento del sujeto de los datos, o por imperativo legal.
- Principio de salvaguardas de seguridad. Para evitar los riesgos de pérdida o uso no autorizado de los datos.
- Principio de apertura. Principio que no parece claro si es un prototipo del principio de de transparencia o del de control y registro de las bases de datos que existan.[43]
- Principio de participación individual. Perfilando ya los clásicos derechos ARCO.
- Principio de responsabilidad. Para hacer efectivo su cumplimiento.

Estos principios parecen tener un destinatario nacional, mientras, en cambio, la parte tercera de las directrices se enfoca hacia lo internacional tratando los flujos entre países y circulación transfronteriza. En esta parte de las Directrices se percibe un ánimo de

[43] Si bien parece una mezcla de ambos a juzgar por la interpretación dada en la Resolución sobre apertura de prácticas de datos personales de la 35 conferencia internacional de autoridades de protección de datos mantenida en Varsovia en septiembre de 2013. Disponible en (Recuperado el 17 de septiembre de 2018):
https://icdppc.org/wp-content/uploads/2015/02/Openess-resolution-ES.pdf

mayor liberalidad, enfocado en garantizar la libre circulación y poniendo el acento en la garantía de flujo ininterrumpida y segura, de los datos personales entre los países.

Las Directrices nos muestran así una doble cara del mismo asunto, si bien complementarias: un enfoque más orientado a la protección del derecho en su recomendación a los Estados y países, y un elemento facilitador de la libertad de circulación de datos y su no restricción en su aproximación a los flujos transfronterizos. Estos elementos conectan en cierta manera con su parte quinta cuando se anima la cooperación internacional entre países para darse a conocer la implantación de los principios en sus respectivos territorios, y el aseguramiento de procedimientos para la circulación de datos entre ellos, que sean compatibles con aquellos principios.

En todo caso, la influencia de la OCDE y de sus Directrices de privacidad de 1980 se ha manifestado como un mínimo suelo de protección en forma de recomendación que acabara estableciéndose de forma irradiadora en las posteriores legislaciones en materia de privacidad que se irán aprobando. Llegando a ser de carácter universal las ideas fuerza contenidas en sus Principios. Así, además de la influencia evidente en las legislaciones nacionales de los países miembros de la Organización y de los que formarían parte de su membresía en un futuro, se observa el seguimiento e incorporación de esos principios en la aprobación de normas en países no pertenecientes a la Organización. Y como veremos más adelante su influencia es medular en el Marco de privacidad APEC de la Organización de Cooperación Económica Asia-Pacífico.[44]

[44] Si seguimos el informe Electronic Privacy Information Center (EPIC) and Privacy International (2006) podemos ver la influencia en la aprobación de los instrumentos normativos sobre Privacidad en los diferentes países. Siendo los principios de la OCDE y la legislación de la Unión Europea con la Directiva de 1995 a la cabeza un referente directo e indirecto en ellas. Así podremos citar como ejemplos de países incorporados a la OCDE en fecha posterior, la norma de Corea del Sur de Protección de información personal gestionada por Agencias Públicas de 1994 (Aún cuando Corea del Sur se incorpora en 1996, esa Ley sigue casi todos los principios de las Directrices). Argentina se inspira directamente en su Ley de Protección del 2000 en la Directiva Europea y en las Leyes españolas (siendo como sabemos la Ley Orgánica de 1999 generación de transposición de la Directiva referida).Para una consulta sobre el extensísimo informe de 2006 y su base de datos podremos consultar (recuperado el 17 de septiembre de 2018): http://www.worldlii.org/int/journals/EPICPrivHR/2006/

2.2.2 La actualización de las Directrices. Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales (2013).

La OCDE nos brinda una actualización sobre la base de las Directrices de 1980, a partir de la necesidad de puesta al día manifestada en las reuniones mantenidas en 2008 por los ministros de la OCDE en Seúl[45], sobre el futuro de la Economía de Internet, y en la que la privacidad fue parte protagonista del debate. Así, a través del Grupo de trabajo de la OCDE en la materia[46], se realizan los estudios pertinentes de carácter socio-económico, de eficiencia y de oportunidad, propios del organismo, sobre los nuevos usos, nuevas aplicaciones y avances de las tecnologías de la información y su relación con los riesgos para la privacidad puestos al día. El trabajo resultante, tras las oportunas consultas, son las Directrices de 2013.[47]

En ellas se añaden algunas definitorias de importancia, reconociendo ya la OCDE a las Autoridades de control públicas como elementos de referencia en las políticas de privacidad y su responsabilidad en la aplicación de las respectivas leyes de protección de datos. Igualmente se vienen a incorporar en las definiciones las leyes nacionales protectoras de la privacidad, que ya son una realidad casi general desde las recomendaciones de aprobación general de 1980.

Lo contenido en estas Directrices vienen a complementar los principios de 1980 que se mantienen como pilares en la catedral de la protección de datos global, y así se recogen y reproducen también en estas Directrices. Estos nuevos principios (o desarrollo de principios) añadidos están en consonancia con una de las principales novedades, como veremos, en el Reglamento europeo, de contenido marcadamente influenciado por el principio de responsabilidad proactiva o "accountability", y basado en la interoperabilidad y la atención a los riesgos y brechas de seguridad.

---

[45] Sobre la conferencia: http://www.oecd.org/sti/40839436.pdf

[46] Para más información del WPSPDE (Working Party on Security and Privacy in the Digital Economy) (Recuperado el 17 de septiembre de 2018): http://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm

[47] Para una perspectiva general del marco de Privacidad de la OCDE y de la revisión en particular de sus guías de Privacidad de 2013 (incluido el proceso y su elaboración) consultar "The OECD Privacy Framework" OECD 2013. Disponible en (recuperado el 17 de septiembre de 2018): http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Así, la parte tercera de las Directrices se encargan de desarrollar la implementación de esa responsabilidad por parte de las Autoridades de control, y la parte sexta en ahondar en la cooperación internacional y la interoperabilidad (Punto 15 letras a) b) y c) y Puntos 20 a 23).

2.3. Otras Directrices internacionales: Las Directrices de la APEC.[48]

Presenta interés para el objeto de este trabajo el marco de privacidad, aprobado el 24 de noviembre de 2004 que, siguiendo el modelo y las Directrices de la OCDE, presenta un modelo de principios de privacidad a seguir por los Estados de las economías concernidas.[49]

Los principios que vienen a ser los originales de las Directrices de 2004, y que siguen las Directrices de la OCDE son los siguientes: prevención de daños, notificación y aviso, limitación en la recogida de datos, uso de la información personal para los fines recogidos y de manera compatible con ellos, elección o información a los titulares de los datos de manera comprensible, integridad de la información personal, es decir, completa, exacta y actualizada, medidas de seguridad, acceso y rectificación asi como responsabilidad (proactiva) o principio omnipresente de "accountability".

Siguen el modelo de implementación de las directrices de la OCDE, y animan, (ya que estas tampoco tienen carácter no vinculante), a la elaboración y aprobación de normas en los Estados afectados que incorporen estos principios a sus legislaciones nacionales. Establece además unos mecanismos de cooperación internacional para la puesta en

[48] La APEC es un organismo de cooperación de las economías vinculadas a través del océano Pacífico, creado en 1989. De sus siglas en inglés Asia-Pacific Economic Cooperation, procede el acrónimo que da nombre a este fórum económico multilateral que reúne a 21 países, destacándose como grupo de discusión internacional que cuenta con Estados Unidos, China y Rusia entre sus miembros, algo poco habitual, mención aparte de las Naciones Unidas. Además de los mencionados encontramos en la organización a las economías de Australia, Brunei Darussalam, Canadá, Chile, Hong Kong (China), Indonesia, Japón, Corea del Sur, Malasia, México, Nueva Zelanda, Papúa Nueva Guinea, Perú, Filipinas, Singapur, Taipei Chino, Tailandia y Vietnam. Podemos encontrar más información en la página de la organización (recuperado el 17 de septiembre de 2018):: https://www.apec.org/

[49] La información puesta al día sobre el marco de privacidad la podremos consultar en el siguiente documento APIC Privacy Framework (2015), publicado en agosto de 2017 (recuperado el 17 de septiembre de 2018):: http://publications.apec.org/publication-detail.php?pub_id=1883

práctica de estos principios en los flujos transnacionales de datos. Dentro de esos mecanismos se especifican dos como destacados: el "Cross-border Privacy Enforcement Arrangement" (CPEA) y el denominado "Cross Border Privacy Rules" (CBPR). El primero enfocado a la privacidad en el ámbito del "Law Enforcement" o de autoridad en la persecución de delitos, y el segundo dentro de la esfera general de los intercambios de datos de los consumidores y usuarios propios de las transacciones económicas. Diferenciación que veremos se repite en los diferentes regímenes jurídicos de protección de datos que estudiaremos.

El sistema CBPR es algo novedoso. Adoptado por algunos de los Gobiernos de la APEC en 2011, se basa en cuatro componentes principales de control: los "Accountability Agents", que serían una suerte de autocertificadores responsables de la privacidad en las empresas adheridas al programa; un segundo elemento de control del anterior, encargado de asegurar el correcto cumplimiento de las políticas de privacidad; un tercer elemento de auditoría sobre el funcionamiento anterior, y una cuarta etapa de revisión en la cúspide, que ya vendría a corresponder a las Autoridades de control de cada uno de los países.[50] El Sistema CPEA está más perfilado como un clásico elemento de cooperación, colaboración y compartición de información entre las autoridades de los diferentes países.

Otro esfuerzo cooperativo de las economías de la APEC en el ámbito de la privacidad transfronteriza se produce en un acuerdo del año 2007 denominado "Privacy Pathfinder" cuyo objetivo era desarrollar el marco institucional y de trabajo del sistema CBPR referido. Bajo el impulso del gobierno australiano se planifica los proyectos de puesta en marcha del entorno de privacidad de la APEC.[51][52]

[50] En el sistema de certificación voluntario CBPR solo hay actualmente cuatro países participantes de las economías APEC: Estados Unidos, Japón, Canadá y México. Que dispone de página web propia (recuperado el 17 de septiembre de 2018):: http://www.cbprs.org/

[51] Siendo su principal documento de trabajo el "APEC Data Privacy Pathfinder Projects Implementation Work Plan" resultante del seminario mantenido en bajo el título "First Technical Assistance Seminar on the Implementation of the APEC Data Privacy Pathfinder" (2009).

[52] Debemos mencionar el grupo de trabajo que el Grupo del artículo 29 de la Comisión Europea mantiene con algunos de los países interesados de las economías pertenecientes al APEC. Y ello debido a la influencia que el sistema de flujos transfronterizos en la protección de datos de la Unión, y que veremos más adelante en este trabajo, sirve de modelo para los mecanismos CBPR de la APEC. (Grupo de Trabajo del articulo 29, 2014).

PARTE II. EL DERECHO A LA PRIVACIDAD EN ESTADOS UNIDOS.

INTRODUCCIÓN

El derecho a la privacidad en Estados Unidos no responde a un criterio normativo homogéneo ni sistemático. Existe una diferenciación importante en su protección, dividida en función de la materia o del instrumento legal o jurídico de utilización. Hay versiones de protección basadas en el derecho contractual, de propiedad o de responsabilidad civil, que si bien serán aludidos, no los encontramos merecedores de una mayor atención, al encontrarse alejados de la consideración jurídica de la privacidad como derecho humano digno de una mejor atención normativa.

Podemos observar, eso sí, cierto acomodo constitucional del concepto y contenido del derecho en la Primera Enmienda (salvaguarda a la obligación de revelar la pertenencia a un grupo o asociación), en la Cuarta (garantía frente a registros y pesquisas arbitrarias) y en la Quinta (Derecho a no incriminarse a uno mismo y a la no obligación a suministrar información personal)[53]

Las Leyes y la Jurisprudencia serán los principales focos de estudio, y seguiremos en ellas una atención lo más sistemática posible, agrupando su análisis en función de la materia, tratando de hacer una clasificación lo más cercana posible a la realidad jurídica estadounidense. Así, dividiremos las normas y los pronunciamientos judiciales en tres partes diferenciadas en el derecho a la privacidad americana. Tanto en la primera como en la tercera se plasma la atención a la protección jurídica de la privacidad desde la condición de ciudadano ante los poderes públicos. En la segunda nos encontramos el juego de esa protección desde la prolongación ciudadana ya en forma de consumidor. Así por tanto la estructura de esta parte queda como sigue.

[53] Viniendo también implicadas la Novena y Decimocuarta Enmiendas a la Constitución de EE.UU.

La primera parte se basa en el estudio de los ficheros mantenidos por el Gobierno y las Administraciones Públicas, empezando además por la primigenia Ley de Transparencia americana.

La segunda parte centra su atención en la protección de la privacidad en base a la determinación del papel de consumidor. En este análisis centraremos igualmente la atención, además de en la ley y en las sentencias, en la actuación jurídico-administrativa del principal órgano regulador y supervisor en la materia: la Federal Trade Commission (FTC). Aquí haremos mención especial a la subespecialidad que se encarga de la privacidad financiera, que pudiera entenderse como una continuación sobre la del consumidor, pero que por su propia entidad y sus importantes leyes de plasmación y desarrollo merece un comentario diferenciado.

La tercera parte nos ofrece la perspectiva, en su otro gran ángulo normativo americano junto con el del consumidor, cual es el de la privacidad cuando confluye con asuntos de seguridad y de inteligencia. Tanto ésta como la anterior serán posiblemente las que más determinen el acceso y la protección del ciudadano americano.

Queremos anotar además que se dan paquetes normativos en los cuáles, y desde la heterogeneidad de la privacidad americana, se mezclan los perfiles de ciudadano y consumidor, y ello en los campos de la salud, la educación y el empleo, en sus diferentes aproximaciones normativas. Por razones de sistematización y claridad de este trabajo, los dejamos solo apuntados más adelante en este mismo epígrafe sin entrar en mayor análisis de los mismos.

El artículo de Warren & Brandeis. "The Right to Privacy" o el inicio de la privacidad del Common Law.[54]

Esta fundamental pieza de doctrina jurídica se puede considerar el hito fundacional de la privacidad americana, que no solo tuvo elemental incidencia en la construcción del

[54] Warren &.Brandeis (1890)

derecho a la privacidad en aquel país, sino también una influencia considerable en la elaboración legal y en los pronunciamientos judiciales de otros sistemas de derecho.[55]

El artículo que podríamos calificar de precursor de la privacidad, viene también, como la canalización de un río jurídico, a desembocar diversas aproximaciones americanas previas (antes y después de la independencia del país) sobre la protección de la intimidad familiar y personal. Si bien es a partir de su aparición cuando toma forma el concepto de privacidad con sustantividad propia.[56]

La obra es firmada a dúo por los dos abogados el 15 de diciembre de 1890 en la "Harvard Law Review" bajo el título "The Right to Privacy", como reacción a las publicaciones de determinada prensa que hacía de la intromisión en la vida privada su principal quehacer y negocio.

Los dos juristas se pusieron de acuerdo en que había llegado el momento de construir una determinación general de *Common Law* como fuera el "derecho a ser dejado solo", principalmente por dos razones: las nuevas tecnologías acaecidas (tales como los daguerrotipos y fotografías) que se reflejaban en los periódicos, y el abusivo uso de esas tecnologías por los medios de comunicación.

Y ello sobre todo a partir de 1884, con la invención por la Eastman Kodak Company de la "snap camera" que permitía recoger imágenes en el espacio público por una cámara manejable, barata y de fácil uso y funcionamiento (Lane 2011, 61-62).

Fue principalmente esa nueva invasión tecnológica de la privacidad la que motiva a los autores a elaborar su famoso ensayo, con ánimo de Principio General que se pudiera invocar en un futuro por los ciudadanos. Concretan este derecho a no ser molestado en

[55] Tenemos multitud de artículos de comentario sobre este ensayo jurídico. Nos parece de útil lectura en castellano, y así hemos seguido, el de la profesora de la Universidad de Huelva, Saldaña Díaz (2012).

[56] En las conclusiones del abogado general sr. Niilo Jääskinen presentadas el 25 de junio de 2013 en el Asunto C-131/12 Google Spain, S.L.,Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González, (y que anticiparía fundamentalmente el sentido del derecho al olvido de la sentencia de la Gran Sala de 13 de mayo de 2014), el inicio de su justificación jurídica alude directamente al artículo Warren & Brandeis, expresándolo en el primer punto de su introducción así: "En 1890, en su seminal artículo publicado en la Harvard Law Review, titulado «The Right to Privacy», Samuel D. Warren y Louis D. Brandeis se lamentaban de que «inventos recientes y modelos de negocios», como «las fotografías instantáneas y la prensa, han invadido los sagrados recintos de la vida privada y doméstica». En el mismo artículo se referían «al siguiente paso que es preciso dar para proteger a la persona»". Ello nos puede dar una idea de la importancia del artículo en la génesis de la protección jurídica de la Privacidad.

el de mera libertad individual, y lo desvinculán del respeto a la propiedad individual, ya que lo establecen necesario para la garantía del libre desarrollo de la personalidad.[57]

El artículo nos va ofreciendo la argumentación jurídica necesaria para la conceptuación del nuevo derecho que debe emerger. Esa reacción proporcionada al "cotilleo" de los medios de prensa escritos, se basa en la idea del derecho a que lo dejen a uno tranquilo con principal garante del pleno uso de la libertad individual. Por tanto "the right to be let alone" es lo que se cultiva en este artículo.[58]

Y los autores lo desgranan como derecho también en sus limitaciones (no olvidando que no existen derechos absolutos) en seis grandes puntos configuradores que pasaremos a resumir:

En primer lugar "the right to privacy" no prohibiría las publicaciones de asuntos de interés general; en segundo caso no prohibiría las comunicaciones, aún privadas, bajo determinadas circunstancias amparadas por la Ley (persecución de delitos, actuaciones judiciales etcétera); un tercer elemento implicaría su ámbito escrito (no oral) en caso de que no haya daños; en cuarto lugar el derecho podría venir dominado o excepcionado por el consentimiento del titular de esa privacidad; en quinto término no vendría afectado en su efectividad por su naturaleza falsa o verdadera, y en sexto lugar no vendría siendo necesaria la mala fe para su correcta alegación.

La asimilación del derecho a la privacidad no fue instantáneo, si bien fue calando poco a poco en el derecho norteamericano, con cada vez más alusiones jurisprudenciales (principalmente de tribunales del estado de Nueva York) y sobre todo, a partir de su actualización crítica operada por Prosser (1960), que, si bien enfocaba su protección

[57] Introduciendo una aspiración igualitarista en su concepción, como resalta el artículo de Saldaña Díaz (2012, 212)

[58] *"…and now the right to life has come to mean the right to enjoy life,-the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term " property " has grown to comprise every form of possession- intangible, as well as tangible (….) These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone…"* Forma de construcción jurídica dogmatica de tipo anglosajón que contrasta con el derecho continental de construcción del derecho.

hacia una clasificación basada en el *Tort Law*, establecía eso si un nuevo prisma al derecho que, a partir de ahí, fue asumido naturalmente en algunas sentencias.[59]

La doble dimensión de un mismo derecho

En esta parte americana del trabajo vamos a fijarnos en la doble dimensión del individuo en relación con el panorama jurídico de la protección ofrecida a su derecho a la privacidad y a la protección de sus datos: como ciudadano y como consumidor.

Es evidente que no se podría tratar de una diferenciación jurídica, precisamente porque sus derechos como consumidor parten de sus derechos ciudadanos que le son inherentes como persona. Se trata de una distinción de mera utilidad organizativa y expositiva del trabajo, que se nos ha venido algo revelada, a la luz del estudio de la estructuración y niveles de protección de las principales leyes estadounidenses en la materia.

En efecto, la fuerza configuradora de la actuación de la competente Federal Trade Commission (FTC), así como la importancia de las leyes que regulan la privacidad del consumidor para la vida jurídica diaria de la persona, hacen que la veamos con una perspectiva diferenciada. Añadiéndose además la subespecialidad, de gran relevancia, de la privacidad financiera, que opera en las actuaciones del individuo-consumidor en sus relaciones con las entidades bancarias y de crédito.

Por otro lado, la versión de protección jurídica se nos ofrece también en la perspectiva del ciudadano en sus relaciones con los poderes públicos, administrativos y gubernamentales. En esa parte se nos presentan las grandes limitaciones a su derecho por las razones de seguridad nacional y por motivos de orden público; y que de tanta actualidad se ofrecen en el equilibrio, siempre difícil, entre seguridad y libertad, y ejercicio y protección de derechos. En la protección de la privacidad esa tensión se manifiesta acusadamente.

[59] Katz v.United States sería la de mayor trascendencia en esa línea, y de la que nos ocuparemos más adelante.

Estas dos vertientes las trataremos una en el capítulo segundo, relativa a la protección del consumidor americano, y la otra tanto en el capítulo primero como en el tercero de esta parte del trabajo que se encargan de la privacidad del ciudadano estadounidense en su relación con los poderes públicos.[60]

[60]Por último debemos hacer mención a una serie de normas importantes que se ven mezcladas y salpicadas por ambas percepciones y visiones de protección, y que se adentran en la vertiente del consumo propio de las relaciones de mercado y las connotaciones e incidencias más cercanas a la protección del derecho ciudadano con igual intensidad.
En este sentido, debemos apuntar algunos paquetes normativos que reúnen las dos facetas regulatorias sobre el individuo como ciudadano y consumidor, y de las que haremos solo mera referencia, ya que su estudio y análisis implicaría bucear en elementos de gran dispersión por razón de la materia, y que por orden de sistemática y claridad del trabajo, como hemos apuntado, nos vemos llamados a no abordar. Ellos son:
En primer lugar la privacidad de los registros médicos, que tiene su exponente principal en la "Health Insurance Portability and Accountability Act" de 1996, quizá el intento de mayor sistematización y voluntad homogeneizadora en un mismo asunto legislativo en materia de privacidad en el sistema americano. Contiene en su *Privacy Rule* el ejemplo, en el modelo americano, más cercano a la protección integral de datos acorde con el modelo europeo de protección (Health Insurance Portability and Accountability Act (HIPAA) Pub. L. No. 104–191 (1996). (Contenida en el 45 CFR § § 164.520 - 164.528).
Otras Leyes a señalar que regulan la privacidad en el ámbito sanitario, serían la Sección 543 (codificada en el 42 CFR Part 2 "*Confidentiality of alcohol and drug abuse patient records*") de la "Public Health Service Act" de 1944, que establece de manera específica la privacidad para los casos de información relacionada con el abuso de drogas y situaciones de drogodependencia; así como la "Genetic Information Nondiscrimination Act" de 2008 (Genetic Information Nondiscrimination Act 29 C.F.R. §§1635.1 – 1635.12 (2008)), que prohíbe que los planes de salud individual o de grupo exijan cargas adicionales o sean denegados basándose en información de genética familiar. Además de una variedad de leyes estatales, ya que competencialmente les vienen atribuidas a los Estados materias sensibles que afectan profundamente a la información de salud. Desde licencias para el ejercicio de profesiones médicas hasta planificación e introducción de planes de salud mental estatal, pasando por toda la información que las autoridades gubernamentales estatales y sus administraciones recaban sobre salud.
En segundo término otro elemento de regulación normativa se da en el ámbito educativo. "The Family Educational Rights and Privacy Act of 1974 (FERPA)" (The Family Educational Rights and Privacy Act, compilada en el 20 U.S.C., § 1232g), es una de sus normas destacadas y establece la posibilidad de supervisión y control por los padres sobre los registros y datos personales que las entidades educativas que reciban fondos públicos dispongan de sus hijos.
Por último citaremos la privacidad en el ámbito laboral con la "Employee Poligraph Protecction Act" de 1988 como ley destacada regulando el uso del polígrafo (permitido en EE.UU.) en el ámbito laboral, en defensa de la privacidad de los empleados o trabajadores (Employee Poligraph Protecction Act, 29 20 U.S.C , §§ 2001 – 2009 (1988)).

CAPÍTULO PRIMERO

LOS ARCHIVOS DE LOS PODERES PÚBLICOS (GOVERNMENT RECORDS)

Estados Unidos empezó a recopilar de manera masiva datos para el correcto funcionamiento de la Administración de su estado federal con el siglo XX. Al igual que en Europa, cuando se desarrolla la necesidad de un estado de mayor capacidad interventora y de iniciativa de prestación de servicios públicos, se requiere una mayor y más adecuada identificación y mantenimiento de información sobre sus ciudadanos.

Es, sobre todo a partir de los años 30 del siglo XX, cuando se crea el sistema de Seguridad Social estadounidense, y con la asignación de un número de identificación único (Social Security Number también conocido por sus siglas SNN), el momento en que los ficheros de titularidad pública empiezan a recopilar el gran grueso de la información personal ciudadana.[61]La llegada de la computación con la Segunda Guerra Mundial y su desarrollo en los años 60 va abriendo mucho más el campo de posibilidades de retención y almacenamiento de los datos.[62]

Así, veremos en este bloque de la privacidad estadounidense las principales normas de regulación de los poderes públicos americanos en su uso de los datos individuales de sus ciudadanos, así como el derecho del acceso de estos a los ficheros de su titularidad mantenidos por aquellas Administraciones.

Este reto regulatorio no solo afecta al Gobierno y Administración federal sino también a las Administraciones de los Estados y entidades públicas locales que mantienen ficheros de manera muy habitual, debido a las competencias que tienen atribuidas.

[61] Bosch (2010: 433) que nos ilustra que la Ley de Seguridad Social de 1935, que fue un "empeño personal de Roosevelt para intentar proteger a los ancianos y desempleados y dar seguridad económica al conjunto de la población…"

[62] Miller (1971) El gran escritor ya nos advierte de los "peligros" del desarrollo de la computarización para la privacidad estadounidense.

1. The Freedom of Information Act

Será precisamente otro presidente demócrata, Lyndon B. Johnson, el que firmara la que podría ser la primera Ley de Transparencia escrita y codificada en la Historia, y el debido contrapunto a la recopilación y uso masivo de datos por parte del sector público introducidos con los New Deal's roosevelianos. Se enmarca esta ley en el segundo mayor esfuerzo de protección jurídica pública del bienestar del ciudadano americano tras aquellos, que fue llevado a cabo a través de su *Big (o Great) Society* por este trigésimo séptimo Presidente estadounidense.[63]

La que podríamos traducir como Ley de Libertad de Información se encuentra contenida en el Título 5 del U.S. Code, bajo el epígrafe "§ 552 Public information; agency rules, opinions, orders, records, and proceedings". La FOIA es probablemente la precursora del conjunto normativo que se ha venido a establecer generalmente bajo el concepto de "Open Government".

Fue promulgada en 1966, y se encuentra en vigor desde el 5 de julio de 1967. La Ley no la ubicaríamos tradicional y estrictamente en los apartados de protección del derecho a la privacidad, pero las implicaciones evidentes que ofrece para la misma, y que también actúa, como veremos, como límite en algunos casos de divulgación de la información; nos parecen razones suficientemente adecuadas como para que sirva de entrada o pórtico a este estudio del derecho a la privacidad en EE.UU.[64]

[63] Del propio y famoso discurso en su sede, la Universidad de Michigan tiene publicado un pequeño análisis de Robert M. Warner (1978) disponible en (Recuperado el 5 de septiembre de 2018): http://bentley.umich.edu/exhibits/lbj1964/lbjspeech.pdf

[64] La Ley ha sufrido numerosas reformas y puestas al día. En 1974, su principal reforma salvó incluso el veto del presidente Ford. En 1976, 1986, 1996, 2002 y 2007 también fueron años con enmiendas a la Ley: *The 1974 Amendments to the Freedom of Information Act, The 1976 Government in the Sunshine Act amendments, The 1986 Omnibus Anti-Drug Abuse Act, The Electronic Freedom of Information Act Amendments of 1996, The Intelligence Authorization Act of 2002 y the OPEN Government Act of 2007*.

1.1 Contenido.

La FOIA dispone que cualquier persona tiene el derecho de obtener acceso a los registros y archivos federales, a menos que dichos registros (o partes de ellos) se vean excepcionados de su divulgación pública; bien por una de las 9 exenciones (letra b) en ella contenidas, o por una de las 3 exclusiones para los registros de las fuerzas de seguridad y orden público (letra c) que la Ley nos señala. Conviene advertir que este derecho se presenta en la Ley con fuerza ejecutoria judicial.[65]

La solicitud de acceso que permite la FOIA lo es para cualquier registro que mantengan las entidades u organismos públicos federales, que en la Ley vienen referidas genéricamente como agencias[66]. Previo a la presentación de la solicitud se debe identificar y determinar cuál es la posible entidad responsable de los registros en los que el ciudadano se encuentre interesado. En este sentido desde hace unos años se mantiene un portal de Internet que contiene y ofrece información sobre el tipo de registro del que cada entidad federal es responsable.[67]

Bien es cierto igualmente que la Ley viene a "poner las cosas fáciles" para ese acceso, exigiendo a las entidades o agencias la divulgación automática y permanente de determinadas informaciones en su poder, entre las que se incluyen aquellas que se solicitan con mayor asiduidad. Además, el hecho de crear un contacto "*ad hoc*" a través de línea telefónica y página web es ejemplo de ese empeño.

La información que la Ley obliga a mantener abierta al público a las agencias podríamos decir que es hoy habitual en cualquier Administración de muchos países

[65] Terminología del derecho anglosajón, que viene a traducirse en su exigibilidad ante los tribunales de Justicia.

[66] La Ley las refiere como "*Agencies*", que coincide prácticamente con cualquier entidad pública administrativa o gubernamental que mantenga registros de datos de los ciudadanos.

[67] En la página web que mantiene el Gobierno estadounidense dedicada a esta Ley (una suerte de inicial e iniciático portal de la Transparencia) se llega a calificar a la misma como "una parte vital de la democracia americana". En un país como los Estados Unidos, históricamente receloso con el poder público, el derecho de acceso a la información del Gobierno Federal se ofrece como un bien esencial para el ciudadano libre e informado. Otra cosa será la gran línea de excepción en que determinados asuntos públicos ven cortada su luz y su transparencia por las razones conocidas de protección o secreto, y que también ocupa ya casi un lugar común en la historia estadounidense.(Recuperado el 5 de septiembre de 2018): https://foia.state.gov/

democráticos, si bien en los años 60 suponían un gran avance en la transparencia pública.

La letra a) de la Ley, y que establece el derecho general objeto de ella, señala la información que debe estar por las agencias "actualizada y puesta al día", y que incluye muchos ámbitos de conocimiento y actuación gubernamental y administrativa, que van desde la información general, localización de sedes y contacto, hasta las normativas de interés relacionadas con la entidad; y toda la información pertinente para un adecuado acceso a los registros a modo de resumen. También se establece (punto 2) el derecho a obtener copia de los documentos solicitados, a no ser que estos ya se encuentren publicados, debiéndose facilitar su ubicación. Se pueden establecer tasas de expedición de las mismas (punto 3) atendiendo a las circunstancias.[68]

Como ejemplo jurisprudencial ilustrativo sobre los límites al derecho de información pública en la privacidad de los ciudadanos y en sus datos personales citaremos la sentencia del Tribunal Supremo *United States Department of Justice v. Reporters Committee for Freedom of the Press.* 489 U.S. 749 (1989)[69]

Después de unas interesantes consideraciones sobre la limitación de los derechos, el Tribunal establece la necesidad de equilibrio sobre la revelación de información pública y los datos personales. Primando en este caso la privacidad del asunto y su no revelación por no estar ubicado el supuesto en el propio espíritu de la FOIA.[70]

---

[68] El incumplimiento o mala práctica en la atención a estos derechos o en relación con el cobro de tasas puede dar lugar a responsabilidad civil de la agencia respectiva, siempre claro con el procedimiento contradictorio previo entre el "requester" de la información y la agencia correspondiente. Ya que, si la información recibida o la actuación pública para cumplir con esta obligación legal no es de la conformidad del ciudadano, se le ofrece, a lo largo de la Ley, el derecho de revisión tanto administrativa como la ulterior judicial.

[69] La familia Medico era una familia de amplio historial delictivo relacionada con la delincuencia organizada. El interés que estas historias presentan para la prensa y el público en general es innegable. Así, y en base a la FOIA se solicitaron la revelación de documentos de interés para los medios por parte de esos mismos medios (principalmente por la CBS) sobre las fichas delictivas de los miembros de la familia, que el departamento de Justicia deniega en base a la excepción del punto 7 c) de la Ley, y basándose en la privacidad de esa familia.

[70] Expresándolo así "*Thus, whether disclosure of a private document under Exemption 7(C) is warranted must turn on the nature of the requested document and its relationship to "the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny. (…)*
In other words, although there is undoubtedly some public interest in anyone's criminal history, especially if the history is in some way related to the subject's dealing with a public official or agency, the FOIA's central purpose is to ensure that the Government's activities be opened to the sharp eye of public scrutiny, not that information about private citizens that happens to be in the warehouse of the Government be so disclosed (…) What we have said should make clear that the public interest in the

El engranaje de procedimiento administrativo y obligaciones de las entidades se refleja a partir del punto 4 hasta el final de la letra a). Las agencias deben, así, establecer regulaciones y normativas de acceso a sus registros, que deberán ser publicadas y respetar los términos de la Ley, y deben tener un sistema de registro de las solicitudes de acceso a sus registros así como habilitación de consulta vía telefónica y telemática.

Debemos apuntar que, en todo caso, el respeto a la privacidad es una constante en el procedimiento de consulta pública, estableciéndose la vigilancia sobre la misma en los documentos que se liberan al público. A modo de ejemplo, podremos destacar el "tachado" de cualquier información que afecte a otras personas en esos documentos, cuando se ponen a disposición de los solicitantes.

1.2 Excepciones y exclusiones.

La letra b) de la Ley es la que interpone las excepciones al derecho general establecido en el anterior apartado legal. Se establecen así las nueve categorías de información que son excepciones de la Ley y a la que no se encuentran sujetas. Las describiremos así:

Primera excepción. Aquella información clasificada por razones de interés o seguridad nacional. Esta clasificación se produce por orden ejecutiva, con lo que podemos entender el gran poder gubernamental de excepción que ampara la Ley.

Segunda excepción. Información interna de la Agencia. (Personal y normas de funcionamiento interno)

Tercera excepción. Aquella información protegida por otra ley federal.

Cuarta excepción. Secretos comerciales o prácticas comerciales o financieras protegidas.

---

release of any rap-sheet on Medico that may exist is not the type of interest protected by the FOIA…"

Quinta excepción. Información interna de trabajo de las Agencias (cartas, comunicaciones, etcétera). En caso de procesos judiciales, claro esté que sí que se podrían poner a disposición de los abogados de las partes.

Sexta excepción. Aquella información que pueda afectar a la privacidad de otra persona, como ya hemos apuntado.

Séptima excepción. Razones de orden público, si pudieran producirse perjuicios para terceros, que incluyen también los que se puedan dar en su privacidad. (Letras A a F del punto 7)

Octava excepción. Aquella información de las agencias supervisoras de las entidades financieras.

Novena excepción. Información geológica y geofísica.

Existe, sin embargo, la posibilidad de que las agencias puedan en parte excepcionar estas excepciones, bajo criterio razonado y siempre que no se produzca perjuicio alguno. (Último párrafo de la letra b)

La letra c) nos señala las exclusiones de tipo especial por razones de policía. Las tres vienen referidas a las especiales necesidades de investigación penal y a la necesidad de su no entorpecimiento.

Otro caso de interpretación directa de la FOIA por parte del Tribunal Supremo, y en el contexto de una investigación criminal, está en la sentencia *National Archives and Records Administration v. Favish*. 541 U.S. 157 (2004), remitiéndose además a la sentencia anterior que analizamos anteriormente para establecer diferenciaciones muy pertinentes.

En este caso se atiende a la situación de una investigación oficial sobre el suceso en el que Vincent Foster, antiguo consejero del Presidente Clinton, es encontrado muerto en un parque de las afueras de Washington D.C. por un aparente suicidio.

Un ciudadano interesado en el asunto, el señor Favish, no cree esta interpretación, y solicita conocer los archivos del expediente policial, entre las que se encuentran fotografías del cadáver. El tema plantea si la revelación de esas fotografías pudiera

afectar a la privacidad y constituir una invasión en la misma (de una persona muerta). Argumenta Favish que la familia no tenía ningún interés personal en la privacidad del fallecido. Argumento que pasa a denegar categóricamente el Tribunal, ampliando el derecho a la privacidad personal a la familia, y negando su confinamiento en uno mismo. Y alude en su pronunciamiento incluso en los rituales del duelo, inmemoriales en la humanidad, en Sófocles, e incluso en la Enciclopedia de la Religión, al ser una interpretación novedosa con escasos precedentes judiciales en que soportarse.

Para terminar con el reconocimiento explícito al derecho a la privacidad de la familia del fallecido y su reconocimiento en el espíritu de la FOIA.[71]

El Congreso y sus registros están excluidos de la Ley (letra d) y por último, en la letra e) se establece el "feedback democrático" (cursivas mías), que, iremos viendo, se repite en las leyes de privacidad estadounidenses, y que se da en forma de informes entre las principales instituciones del país. En este caso, entre las agencias y el Fiscal General, y entre éste y el Congreso. Estos informes versarán sobre el número de solicitudes, temáticas afectadas, habitualidad de ellas, media de tiempo de respuesta, etcétera. Los informes son anuales.

1.3 Consideraciones

En consonancia con todo lo anterior podemos pensar que nos encontramos ante una pionera ley de transparencia, pero quizá esté más a medio camino entre ese perfil y la del consagrado derecho de acceso a los registros administrativos, que se establece en otras leyes administrativas generales, y que facilita el conocimiento de la actividad de la Administración Pública y de las actuaciones y planes de los Gobiernos.

[71] Expresándolo de manera indubitada: *"…we hold that FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images (…) Our ruling that the personal privacy protected by Exemption 7(C) extends to family members who object to the disclosure of graphic details surrounding their relative's death does not end the case*"

Podríamos, además, observar algunas especiales consideraciones que se dan en la Ley sobre la privacidad.

En primer lugar, para casos de solicitud de información de registros relacionados con otra persona en general, y como ya hemos visto en las exenciones (Sexta), no se suministran siempre que puedan afectar a la privacidad de aquella.[72]

En segundo lugar, debemos apuntar que las dos principales órdenes ejecutivas de excepción de la FOIA aprobadas por el Gobierno Federal sobre seguridad o interés nacional (Exención primera) son la "*Executive Order 12958 on Classification of National Security Information* (1995)" y la anterior de 1982 "*Executive Order 12356 on National Security Information*." Que nos sirven de ejemplo sobre la referida discrecionalidad presidencial que sobrevuela a la Ley.

Además es necesario observar que la "*Electronic Freedom of Information Amendments Act*" del año 1996 ha sido la principal ley de modificación de la FOIA, si bien sufrió otras pequeñas enmiendas, ya apuntadas, y principalmente en los años 1974 y 1986. Con ellas no se vieron perturbadas las exigencias sobre privacidad originalmente establecidas.

Por último, debemos señalar que el Congreso, además, ofreció todo una guía de recursos explicativos para facilitar la comprensión y ejercicio del derecho de acceso por parte de los ciudadanos a través de una guía ciudadana con indicaciones sobre la FOIA[73]

---

[72] Como paradigma del tachado de privacidad, que también hemos apuntado para las copias (letra a) punto 2 in fine): "*To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction, staff manual, instruction, or copies of records referred to in subparagraph (D).*"
Particularmente, en caso de registros que afecten al propio sujeto, y para el caso de que la persona pida información sobre sí mismo, este deberá acreditar su identidad en la solicitud, que puede presentar forma notarial o declaración responsable firmada.

[73] "*7th Congress, 2d Session. House Report 107-371. A citizen's guide on using the freedom of information act and the privacy act of 1974 to request government records*". En ella se explica la exención sexta por privacidad personal:
"The sixth exemption covers personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. This exemption protects the privacy interests of individuals by allowing an agency to withhold personal data kept in government files. Only individuals have privacy interests. Corporations and other legal persons have no privacy rights under the sixth exemption.
The exemption requires agencies to strike a balance between an individual's privacy interest and the

Como recapitulación general sobre la norma podríamos establecer que, a pesar del derecho recogido en la FOIA sobre acceso y conocimiento de los ficheros públicos, las excepciones en ella son de carácter tan extensivo que vacían de contenido el derecho mismo. Si bien ello favorece establecer una ayuda no buscada de protección sobrevenida de la privacidad que pudiera verse en juego. Efecto irónico y no pretendido que perfilará ya las relaciones futuras propias de posible conflicto entre el derecho a la transparencia exigible de los poderes públicos y el derecho a la protección de datos de las personas afectadas.

public's right to know. However, since only a clearly unwarranted invasion of privacy is a basis for withholding, there is a perceptible tilt in favor of disclosure in the exemption. Nevertheless, the sixth exemption makes it harder to obtain information about another individual without the consent of that individual."

Si bien al tiempo de cerrar este apartado del trabajo, está en trámite parlamentario y recién aprobado su versión por el Senado estadounidense, la "*Cybersecurity Information Sharing Act (CISA*)" que puede dejar bastante "tocada" la efectividad del objetivo de transparencia de la FOIA.

2. La Privacy Act de 1974.

Al igual que la FOIA, esta importante Ley General se enmarca y se codifica dentro del Título 5 del U.S.C., que viene a ocuparse de las agencias federales y de sus previsiones administrativas de actuación, es decir, del funcionamiento de las Administraciones Públicas federales. Luego, podríamos entender a esta Ley, al igual que la anterior, como concebida en aquellas de tipo transversal sobre y para el funcionamiento jurídico administrativo de EE.UU. en sentido amplio.

Podríamos igualmente recordar en este sentido de influencia estadounidense, nuestra redacción constitucional del artículo 18 encargado del derecho a la privacidad e intimidad, que en su punto 4 se enmarca dentro de esta general inquietud "setentera" que anticipa los retos que la informática iba a provocar en la protección de los derechos individuales.[74]

Aquella evolución humana hacía cada vez más sencillo el tratamiento de datos personales de y para una multiplicidad de individuos, así como su computarización.

2.1 Contexto y antecedentes.

La Ley nace, por tanto, debido a las preocupaciones que en los años 70 se dieron en torno al desarrollo de la informática, de incipiente aparición, y el impacto que la misma pudiera tener en los derechos individuales.

En 1973 el *Department of Housing, Education and Welfare (HEW)* elaboró un informe que recogía estas preocupaciones sobre el desarrollo de la informática y sus retos para la privacidad. Así, el informe estableció un código de buenas prácticas en relación con el

[74] Recordémoslo: "4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

tratamiento de la información, y relacionado con los derechos y responsabilidades que esa incipiente masiva transferencia de datos personales vendría a alumbrar.

El "HEW Report" se puede entender como el documento iniciático para la elaboración de esta Ley. El documento cuyo nombre obedece a las siglas de su órgano creador y elaborado por el Departamento referido, llevaba por título "Records, Computers, and the Rights of Citizens". En él se recomendaba la adopción de legislación reguladora al Congreso para adoptar un código de información justa ("Code of Fair Information") cuyos principios son básicamente los de cualquier ley actual de protección de datos en su mantenimiento por el poder público: la no existencia de recopilaciones de archivos de forma secreta, la necesidad de informar a los ciudadanos al respecto y de los derechos que le asisten, de recabar su consentimiento debidamente informado, la capacidad ciudadana de corrección e impugnación de sus archivos concernientes, así como la precisión, justificación y exactitud de los datos.

El informe también refería a recomendaciones concretas de modificación legal o indicaciones sobre otros asuntos relacionados con la privacidad, como por ejemplo sobre el tratamiento del número de seguridad social estadounidense.

La influencia e inspiración del informe en la redacción de la Privacy Act fue, por tanto, de gran calado.[75]

Así, la Ley es firmada primero por el Senado (17 de diciembre) y luego por el Congreso (18 de diciembre), siendo rubricada por el Presidente Ford al inicio del año 1974.

En la propia Ley se estableció una comisión de estudio y seguimiento de la misma, que estaría encargada de hacer una valoración de sus resultados. Así se crea la *Privacy Protection Study Commission* ("PPSC") emanante de las propias previsiones legales, que en 1977 dio a luz el trabajo para el que fue creada. En el informe de título "Personal Privacy in an Information Society", que reconocía el gran paso adelante que supone la

[75] En este enlace del departamento de Justicia estadounidense se puede encontrar una imagen en pdf cercana al original (recuperado el 5 de septiembre de 2018): www.justice.gov/opcl/docs/rec-com-rights.pdf
La ley fue fruto del consenso entre la Cámara de Representantes y el Senado que, en principio, tenían distintas interpretaciones de enfoque. Más que interpretaciones, eran textos legales distintos. La de la Cámara de Representantes, la The House bill, H.R. 16373 y la del Senado, The Senate bill, S. 3418. Si bien la aprobación legal final fue producto de lo que podríamos entender por una comisión mixta (Joint Committee on Government Operations, (1976)).

Ley, se ofrecía además una visión insatisfactoria en relación con los resultados de la misma, sobre todo teniendo en cuenta las expectativas que el Congreso tenía depositadas.[76]

2.2 Contenido.

La Ley viene sustanciada, en el parágrafo 552a, del referido título 5 del U.S.C. con el título "Records maintained on individuals". Por lo tanto, viene referida y actúa sobre los archivos en posesión por parte de las agencias gubernamentales sobre los ciudadanos.

La letra a) ofrece una extensa definitoria jurídica de los términos de la Ley. Desde "individual", que sería todo ciudadano americano o persona con válido permiso de residencia, hasta el término "record" y sus derivados, que se traduciría en todo tipo de archivos o red de archivos mantenida por el poder público. Es importante la distinción que nos presenta del término "matching program" que sería una comparación computadorizada (salvando las de objeto estadístico o exigidas por la Ley), y que vendría a convertirse en uno de los principales focos de regulación.

Otra importante distinción es la establecida entre "*recipient agency*" y "*source agency*" ya sea la entidad pública receptora de archivos o fuente de los mismos.

La letra b) nos ofrece el mandato general de la Ley.[77]En esta letra hay una prohibición genérica de divulgación o publicación de los registros mantenidos por las agencias públicas, si bien establece las condiciones del mismo en caso de poder producirse.

Se puede producir por consentimiento del titular o bien en los casos señalados en este apartado, y que nos llevan a las posibles excepciones, (desarrolladas en los números 1 a

[76] Privacy Protection Study Commission (1977). El informe también realiza críticas a cierta definición (o indefinición) terminológica de la Ley, y sobre todo, a la falta de impacto general que estaba teniendo hasta aquel momento, sin que el público en general (es decir sus destinatarios) se hubiera visto repercutido por ella. Sobre todo en comparación con la relativa popularidad y conocimiento que la "Freedom of Information Act (FOIA)" había ocasionado en la sociedad americana del momento.
Igualmente las grandes trabas en forma de excepción que los asuntos de inteligencia (principalmente provenientes de la CIA) e investigación policial ejercían sobre las previsiones generales de la Ley, también fueron motivo de preocupación en el informe de la Comisión de seguimiento.

[77] Bajo el enunciado "(b) Conditions of Disclosure"

12 de la letra), y que podríamos resumir en dos grandes categorías: bien en lo exigido por las necesidades del funcionamiento regular de las instituciones, o bien para aquellos casos legalmente contemplados y permitidos.

La letra c) con el enunciado"*Accounting of Certain Disclosures*", establece la obligación a las agencias de observar una llevanza adecuada de los archivos en su poder, y la justificación precisa de la puesta a disposición que hagan de los mismos.

La letra (d) "*Access to Records*" es un apartado muy parecido a nuestro articulado administrativo (del artículo 35 de la ya antigua Ley 30/1992) de accesos a los archivos y registros que nos afecten directamente y que mantengan la Administraciones públicas. Así como el derecho a su corrección o rectificación.

La letra (e) "*Agency Requirements*" establece los requisitos que las agencias deben observar para el mantenimiento de los registros de que se traten, fijándose de manera especial en su pertinencia. Artículo que está muy relacionado con lo que se establece en el mismo sentido en Europa y en la Unión Europea para las Administraciones públicas, en las que se identifican los responsables de los ficheros y archivos, y se atiende a su justificación permanente.

Una especial atención merece la importancia que se ofrece en la Ley a la protección dada a la privacidad del número de identificación o de identidad, en la forma estadounidense de número de seguridad social.[78]

Lo que también se traduce en la no necesidad por parte de los ciudadanos de dar su identificación para ejercitar los derechos, beneficios o privilegios que pudieran corresponderles por Ley. Por lo tanto, el número de identificación de la seguridad social solo se podría poner a disposición entre agencias federales, previo consentimiento de su titular, aunque fuera para el ejercicio administrativo propio de esa agencia o entidad gubernamental.

[78] La Sección 7 de la letra e) de la Privacy Act nos dice:" *Each agency that maintains a system of records shall (…) (7)maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity*"

La letra (f) "*Agency Rules*", impone obligaciones genéricas a las agencias para mantener y conservar adecuadamente los registros en su poder, así como para una adecuada relación de los usuarios y con los titulares de los mismos.

De igual manera la letra (g), y continuadora de la anterior, establece también, de manera genérica, las posibles responsabilidades de tipo civil que podrían contemplarse para el caso de incumplimiento por parte de las agencias en sus obligaciones referidas.

Para el caso de la letra (i) se nos presentan ya previsiones de responsabilidad de tipo penal, en caso de conducta delictiva con respecto a estos ficheros y su divulgación por parte de las agencias o de cualesquiera de sus empleados.

La letra j) y la letra k), por su parte, estipulan las excepciones legales. La primera (j) establece las excepciones tasadas en la propia Ley. La letra recoge las excepciones generales a lo establecido para los casos de ficheros mantenidos por la CIA o por las agencias encargadas de la persecución del crimen penal (FBI, etcétera), con lo que ya observamos la gran falla (no en sentido peyorativo) que se vislumbra siempre (también en Europa) a la hora de regular y legislar el derecho a la privacidad individual: la exigencias de la Seguridad. En la segunda (k) se observan excepciones de tipo más particularista en cuanto a los ficheros. Como ejemplos citaremos la motivada por la protección del Presidente (número 3) o aquella necesaria para el acceso o promoción a la función pública federal y sus necesidades previas de comprobación de candidatos (número 6). Si bien todos están relacionados de manera más o menos directa con la seguridad del Estado.

La letra (l) viene referida al mantenimiento de los archivos de tipo histórico o que se pudieran convertir en tales con el paso del tiempo, asignando al cuerpo de archivística de los Estados Unidos la responsabilidad de su custodia y mantenimiento.

La letra (m) se encarga de los adjudicatarios de contratos públicos que deban trabajar y prestar servicios con el tratamiento de los archivos, vinculándolos a la misma capacidad de uso y responsabilidad que los empleados de las agencias públicas.

Las listas de distribución de correos están por lo general prohibidas para las agencias (según la letra n), así como los "*matching programmes*" (letra (o) "*Matching Agreements*") o vinculación computerizada a los que se le prestaba especial atención y consisten en el enlace automatizado de datos, salvo excepción por acuerdo interinstitucional[79]; que deberán especificar condiciones y requisitos similares a las determinadas en las agencias para la divulgación de los ficheros. Estos "*computer matching programmes*" podrían ser definidos como sistemas automáticos de emparejamiento de datos a través de archivos electrónicos, y que permiten buscar e individualizar personas determinadas.[80]

Importante nos parece también la letra (p) ("*Verification and Opportunity to Contest Findings*"), que establece en general la prohibición de que se puedan producir efectos adversos contra la persona titular de los ficheros por los datos en ellos contenidos, y que se produzcan a raíz de ese cruce computarizado de datos que se hubiera realizado como consecuencia de las excepciones amparadas por el artículo anterior (acuerdo interinstitucional) a esa prohibición genérica de los "matching programmes."

En la letra (q) la Ley prevé la responsabilidad de la agencia matriz caso de no poner a disposición los datos a la agencia receptora, si tiene razones para creer que las anteriores determinaciones legales (letras p y o) no están siendo cumplidas.[81]

Las letras (r) y (s) establecen la supervisión política federal de la actuación de las agencias por parte de las Cámara de Representantes y del Senado a través de sus respectivos Comités así como de la obligatoriedad de informe bienal del Presidente a las Cámaras sobre la actuación ejecutiva al respecto.

Por último la letra (u) asevera y ordena a las agencias la integridad de los ficheros con la necesaria constitución de un órgano que vele por los mismos en aquellas, así como de la correcta aplicación de esta Ley en las respectivas Instituciones.

[79] "*except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency*"

[80] En este sentido nos parecen útiles las descripciones contenidas en Clarke (1994)

[81] Exactamente nos dice lo siguiente:" *… if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency*"

La última letra (w) de la Ley establece la capacidad y competencia de supervisión y velar por la observancia de la misma a la "Bureau of Consumer Financial Protection".

2.3 Ejemplos Jurisprudenciales (cases)

Uno de los temas de mayor importancia dentro del campo regulado por la Ley es el de la dinámica del "uso del uso rutinario", por lo que en primer lugar, dentro de esta mención jurisprudencial, veremos el coto que los Tribunales han puesto al mismo.

El caso quizá más importante en la jurisprudencia americana sobre el tema es el de "Britt v. Naval Investigative Service, 886 F.2d 544 (3d Cir. 1989)".

En este caso, "*the Naval Investigative Service (NIS)*" investigó al señor Britt, que era un empleado público del Servicio de Inmigración ("*the Immigration and Naturalization Service (INS)*") y ex miembro de la Reserva de la Marina de la que fue expulsado por un asunto de confiscaciones impropias.

El Servicio Naval (NIS) puso a disposición del empleador del señor Britt, (el INS) sus primeras investigaciones, a lo que el señor Britt contestó con una demanda, ejercitando los derechos conferidos en la "Privacy Act". Las alegaciones del NIS se basaban en la excepción del "uso rutinario" ya que argumentaba ese uso se incluía y estaba amparado por la publicación en el "Federal Register" bajo el epígrafe de "*other investigative units (federal, state or local)*".

El NIS alega su naturaleza de agencia federal reguladora, con una unidad de investigación y que por tanto, se le podía aplicar esa excepción publicada como "uso rutinario".

El Tribunal no estuvo de acuerdo con esta interpretación. No la admite porque no encuentra pruebas de que el NIS estuviera llevando una investigación penal propia, aduciendo que solo ponía a disposición esos datos personales por el mero interés de la otra agencia (INS) en saber que empleaba a un subordinado falto de integridad.[82]

[82] Concluye: *"We conclude therefore that NIS' use of the information compiled as to Britt, which was merely a preliminary investigation with no inculpatory findings, by disclosing it to Britt's civilian employer*

Cree además el Tribunal que se contravenía el espíritu de la Ley[83], y alude a la la laxitud en el contenido del término alegado de uso rutinario.[84]

Otra sentencia importante es la de Pippinger v. Robin 129 F.3d 519 (10th Cir. 1997).

En este caso el empleado público señor Pippinger demanda a su organismo y centro de trabajo, el Internal Revenue Service (IRS), por poner su información personal a disposición del registro ALERTS ("*Automated Labor Employee Relations Tracking System*"), sistema de fichero de los expedientes disciplinarios del sector público estadounidense. En él se reflejaba el procedimiento disciplinario administrativo que Pippinger tuvo que afrontar por mantener una relación con una subordinada. Alega violación de la Privacy Act, debido a que su precedente fue utilizado y salió a la luz en otro procedimiento de la misma naturaleza, transfiriendo esa información al "*Merit Systems Protection Board" ("MSPB"*) y protagonizado por el señor Schuluck. El MSPB era el órgano encargado de decidir la degradación de nivel del señor Schuluck, en un procedimiento por hechos similares a los del señor Pippinger, habiendo sido además Schuluck supervisor de este.

El Tribunal no acepta las pretensiones del señor Pippinger (que dirigía además directamente la demanda contra el Secretario del Tesoro como máximo responsable de su organismo), argumentando el Tribunal que la relación de Pippinger asi como su condena disciplinaria de dos días de suspensión por los hechos, eran perfectamente conocidos por los integrantes de la plantilla, y que la transferencia de su información al MSPB estaba dentro de los objetivos legítimos de los sistemas de gestión del personal y empleado público federal.[85]

(albeit a government agency) was not compatible with the purpose "for which the information was collected"

[83] "*We believe that to hold otherwise would frustrate the congressional purpose behind the Privacy Act. One of the goals of the Act was to prevent the federal government from maintaining in one place so much information about a person that that person could no longer maintain a realistic sense of privacy*"

[84] *"…the breadth of the clause relied on does not provide adequate notice to individuals as to what information concerning them will be released and the purposes of such release*."

[85] Otros "*cases*" importantes en la jurisprudencia de la Privacy Act son:

- Clarkson v. Internal Revenue Service, 678 F.2d 1368 (11th Cir. 1982).
- R.R. v. Department of the Army, 482 F. Supp. 770 (D.D.C. 1980).
- Doe v. Chao, 306 F.3d 170 (4th Cir. 2002), cert.granted, 2003 U.S. LEXIS 5035, (No. 02-1377, 2003 Term) Siendo Doe y Chao el pseudónimo utilizado por un grupo de mineros por un lado y el departamento de Trabajo por otro. Llegando hasta el Tribunal Supremo y relacionado con la puesta a disposición de sus

2.4 Consideraciones.

Como elemento positivo podremos decir que nos encontramos ante una Ley que se presenta como precursora en un camino legislativo de los que se van abriendo con la fuerza de un derecho fundamental sustentador para una nueva garantía de protección ciudadana. En este caso la de la privacidad. Y lo hace estableciendo una referencia específica a la protección de la Primera Enmienda constitucional.

Además, alumbra novedades importantes en la regulación hasta la época, como la restricción a la compartición de datos entre administraciones federales, con la limitación de los "*matching programs*" referidos. O la concreción y duración determinada de los acuerdos ("*agreements*") entre ellas, en lo que pudiera afectar a la privacidad. Y cierra la puerta a convenios generales de cooperación que pudieran ser un "agujero" indeseado en la privacidad de los ciudadanos.

Por lo tanto destacaremos que no se permiten las transferencias automáticas o automatizadas de datos entre agencias federales como elemento de interés. Además, la transferencia tendrá que venir amparada por un convenio o acuerdo por escrito entre las agencias federales sobre el caso concreto, que deberá ser puesto a disposición de sendos comités (del Senado y de la Cámara de Representantes), que actúan como vinculadores democráticos a través de sus respectivos Comités ("*The Committee on Governmental Affairs of the Senate y the Committee on Government Operations of the House*"). Estos acuerdos, igualmente, solo pueden tener una duración máxima de 18 meses, si bien pueden ser objeto de prórroga, caso de no cambiar sustancialmente las condiciones que existían al firmarse.

Ahora bien, también podemos observar algunos puntos oscuros en la norma. El ámbito subjetivo de la Ley viene referido solo a ciudadanos americanos o con permiso legal de residencia. Es importante destacarlo ya que se trata de una ley de privacidad con

---

números de seguridad social (o de identificación personal).

vocación generalista, y condicionante en las relaciones de los ciudadanos con las administraciones públicas federales en EE.UU., y que por tanto abre una distinción importante con las personas en situación irregular (que abundan en aquel país.)

También es limitada en cuanto a las propias administraciones afectadas, ya que solo las agencias federales referidas en la Ley se ven obligadas de manera directa, dejando a un lado a los Estados y Administraciones Locales. Estas administraciones tendrán su propia regulación, otrora lógica en el respeto federal estadounidense.

Algo que veremos habitualmente (una pauta marcada) en este estudio general de la legislación de privacidad estadounidense se puede empezar a comprobar con esta *Privacy Act*, como es lo que podremos venir a asimilar como una horadación progresiva de las reglas generales, con infinidad de excepciones en cada una de las leyes sobre privacidad. Horadación que incluso suele continuar tras las excepciones generales, escarbando en subsiguientes excepcionalidades de esa ya tenue regla general de protección individual; muy débil ya por esas continuas e individualizadas excepciones.[86] Es un proceso habitual que iremos observando y que, aunque comparte rasgos con el caso europeo, no se observa tan acusado en el viejo continente.

Además sobre esta Ley se han cernido críticas importantes desde su aprobación. Una de ellas parte de que previsiones de calado de la misma, previsiones que pudiéramos calificar de control democrático, y que consistían en la necesidad de informe bienal del Presidente de los EE.UU. sobre la vigilancia y supervisión de su aplicación (su seguimiento presidencial), fueron derogadas con la "Federal Reports Elimination and Sunset Act of 1995".

[86] Como ejemplos de algunas excepciones que pudieran romper el principio de protección legal general de privacidad al que aspira la Ley podríamos hablar, siguiendo el centro de investigación y ONG Electronic Privacy Information Center (EPIC), de la demasiado estrecha y acotada definición de archivos que hace la Ley. La web EPIC nos dice: *""records," "systems of records" and "agencies" are narrowly defined, the Act may not cover many types of databases and data-gathering activities*." Criticando también el amplio ventanal de excepción que se abre con los objetivos de ejecución o aplicación legal del término "uso rutinario" que equivaldría a nuestro "habitual ejercicio de sus funciones"; que excepcionan, en esa horadación permanente, el sentido primero de la ley. Lo alude así: *"Also, there are certain exceptions given for "law enforcement purposes." Finally, the "routine use" exception allows government agencies to disclose individually identifiable information simply by stating their plans to disclose that type of information when they create or alter the database*."
Recuperado el 26 de julio de 2018:
https://www.epic.org/privacy/1974act/

Por último, la web EPIC y algunos autores[87] también critican el envejecimiento que ha sufrido la Ley para ejercer esa protección. Eden (2005) se hace eco de las deficiencias de protección de la privacidad que puede presentar la *Privacy Act* ante los sucesivos retos tecnológicos que le suceden (entre ellos la aparición de la tecnología RFID y que da contenido al artículo).

Además, sobre el concepto de "uso rutinario" y su sobreexplotación de excepción, entenderemos otro de los elementos negativos, ya que la Ley lo define como aquel uso para un propósito compatible con aquel para el que fue recabado. El filón de escape, por tanto, es inagotable. Un concepto jurídico indeterminado (el de uso rutinario) que se alega tan asiduamente (con la única principal obligación de ser inscrito en el Registro Federal como tal), que trasciende su esencia, y se convierte en un recurso de excepción permanente para las agencias federales en su sorteo de la privacidad individual estadounidense. Esas listas de inscripción son amplísimas, conteniendo prácticamente todas las posibles excepciones potenciales en forma de usos rutinarios.[88]

Por último y respondiendo a las propias críticas, la Privacy Act ha sufrido un esfuerzo de actualización a través de su última modificación, con la "P*rivacy Act Modernization for the Information Age Act of 2011*", que se impone un objetivo de puesta al día de la misma, iniciándose a través de los empeños del senador por Hawái Daniel Akaka.[89]

La *PAMIA Act* consiguió actualizar la Privacy Act en sus conceptos, clarificando términos y poniéndola en general al día también en sus excepciones. Refuerza además el objetivo de control civil y penal. Si bien los retos sobre el envejecimiento de la Privacy Act, como el de todas las leyes y más acentuadamente el de la leyes de Privacidad, sigue estando presente y activo cada día que pasa.[90]

---

[87] EPIC nos dice: "*While it may have been extremely difficult in 1974 to affect someone's privacy without knowing their name, Social Security number or appearance, the sophistication of today's databases make it much easier to single out an individual from a set of facts, none of which is in itself an "identifying particular.*"". Coincidiendo con Eden (2005) si bien este se centra en el ejemplo de la aparición de la tecnología RFID.

[88] Coincidiendo en esa crítica más doctrina especializada. Citaremos como ejemplo a Gellman (1997).

[89] Justificándolo ante el Senado (S.1732) en la "*expansion of technology and the proliferation of personally identifiable information in the hands of government agencies*".

[90] Otra reforma relevante de la Ley y a la que no hemos aludido expresamente, se produjo en 1988 con la "*Computer Matching and Privacy Protection Act*" que introducía precisamente en la Ley la regulación de esta práctica del "Computer matching", requiriendo para ella la necesidad de acuerdo por escrito.

3. Driver's Privacy Protection Act (1994)

La Ley (DPPA) está establecida dentro del marco de regulación más amplio del Título 18 del U.S.C. (encargado de la tipificaciónn penal) y del Capítulo 123 de ese Título, que lleva por título "*Prohibition on release and use of certain personal information from State motor vehicle record*s", que engloba desde el parágrafo 2721 hasta el 2725. Si bien su concreto contenido coincide con el primer parágrafo (§ 2721) coincidente en su enunciado con la prohibición general del Capítulo "*Prohibition on release and use of certain personal information from State motor vehicle records*". Se encuadra así dentro de las regulaciones que afectan a los archivos y registros gubernamentales y su relación con la privacidad individual.

3.1 Antecedentes de la DPPA

Sería la senadora Barbara Boxer la que tomó el inicial impulso legislativo de la norma. Ejemplo de sus planteamientos motivadores para ejercer su función legisladora, plantea la senadora, en la justificación de la versión del Senado de la Ley, el contenido de unas cartas de acoso que pudieron enviarse a una dirección de remisión por la falta de protección de la que esta información adolecía con anterioridad a la ley. Recibiendo apoyo de otros senadores, entre ellos, el Senador Chuck Robb y el Senador Harkin[91]

En cuanto a la historia del formalismo legislativo debemos señalar que la DPPA se aprueba como una enmienda de la "*Violent Crime Control and Law Enforcement Act of 1994*".[92]

---

[91] Presentada el 26 de octubre de 1993 (103rd Congress, 1993–1994).
La motivación para la creación normativa de la DPPA parte de un supuesto abuso gubernamental en la utilización de la información personal de los conductores y de sus registros de Tráfico. El paradigma iniciático de ello se produce en 1989 con la muerte de la actriz Rebecca Schaeffer, que fue asesinada por un fan perturbado que consiguió su información personal de domicilio de residencia, entre otros datos, a través de un investigador privado, que, a su vez, se nutrió de los registros estatales de conductores.

[92] En la Cámara de Representantes del Congreso como 103 H.R. 3365 y en el Senado de ese Congreso por la senadora Boxer como 103 S. 1589.

En 1999 el Congreso modifica a su vez la Ley añadiendo figuras adicionales de protección a la privacidad en la que se conoció como la "*Shelby amendment*", y que entró en vigor el 1 de junio de 2000. Introduce el consentimiento previo expreso de los conductores para la divulgación de su información personal como regla general para los Estados.

Importante a destacar fue el reto constitucional que superó la Ley tras el pronunciamiento del Tribunal Supremo en el caso "Reno v. Condon, 528 U.S. 141 (2000)", en el que el Estado de Carolina del Sur atacaba la Ley argumentando que contravenía los principios mismos del federalismo. El Supremo no estimó esta visión, argumentando en su sentencia que era un ejercicio propio de la autoridad del Congreso salvaguardar y regular el comercio interestatal bajo la *Commerce Clause.* El Supremo avala por tanto la constitucionalidad de la norma ante la pretensión de Carolina del Sur.[93]

3.2 Contenido.

El parágrafo 2721 de la Ley contiene su principal alcance normativo. La letra a) nos ofrece la prohibición general de divulgación por el poder público (principalmente el estatal) de la información personal de los conductores relacionada con el registro y

[93] Lo expresa de siguiente manera: "*…The United States asserts that the DPPA is a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause, U.S. Const., Art. I, §8, cl. 3.2 The United States bases its Commerce Clause argument on the fact that the personal, identifying information that the DPPA regulates is a "thin[g] in interstate commerce," and that the sale or release of that information in interstate commerce is therefore a proper subject of congressional regulation*
(…) we turn to South Carolina's argument that the DPPA is unconstitutional because it regulates the States exclusively. The essence of South Carolina's argument is that Congress may only regulate the States by means of "generally applicable" laws, or laws that apply to individuals as well as States. But we need not address the question whether general applicability is a constitutional requirement for federal regulation of the States, because the DPPA is generally applicable. The DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information–the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce."
Llamándonos la atención la similitud de la argumentación entre el modelo federal americano en su aplicación y revisión de actos jurídicos y legales, y el del TJUE y los Estados miembros de la UE en relación con la protección del comercio y la libre competencia.
Y debemos añadir el apunte de que la privacidad de los conductores americanos los acompaña allá donde se desplazan, también cuando lo hacen en su coche en los viajes icónicos a través de la mítica carretera interestatal 66.

mantenimiento de los vehículos a motor, y sobre todo de la "highly restricted personal information", que se diferencia de la anterior de tipo general, en un nivel más restrictivo para sus excepciones. La diferenciación entre ambas se relaciona en las definiciones contenidas en el parágrafo 2725, que se asemeja a la distinción habitual entre datos personales y datos personales especialmente sensibles.[94]

Si se ha prestado consentimiento, la Ley lo limita para cada caso y no para una relevancia ilimitada. Al igual que muchas otras leyes de privacidad federal se trata de una ley de mínimos, que puede ser más protectora o garantista por acción legal de los Estados. En este sentido seguimos a Karras (1999, 132-133) que cita algunos Estados como ejemplo de ello (Wyoming o Arkansas entre otros), que aumentan los requisitos para disponer de los datos de los conductores en su poder, y solo los revelan para casos de consentimiento expreso por escrito del titular de los datos, o en base a licencia válida o por razones de ejecución normativa para la necesaria acción pública de que se trate.

Las excepciones, apartado ineludible de la legislación de derechos en general y de la de privacidad estadounidense en particular, se nos despliegan en el aparatado b) que nos reporta los "*Permissible Uses*".

Básicamente las dos (no solo la menos agravada "*personal information*") se excepcionan para los casos de investigaciones en caso robo de vehículos o de delitos relacionados con vehículos y su identificación, dentro de la primacía habitual de seguridad para casos de persecución de delitos[95]

[94] § 2725 en sus puntos 3 y 4:
"(3) "*personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.*
(4) "highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information."

[95] "*Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act*".

Continúa el artículo de manera desglosada la forma en que esa puesta a disposición de información permitida debe realizarse para la "highly restricted personal information" (normas y pasos desde el punto 1 al 14). Se justifica, y podría resumirse, en el normal funcionamiento del negocio de transmisión de coches nuevos y usados de manera amplia, y que incluyen desde la actividad gubernamental de control, hasta el negocio de seguros, pasando por la mera actividad estadística. Observamos aquí una amplitud excepcional que podría socavar ese derecho a la privacidad que se venia titulando, de manera quizá algo engañosa, como altamente restringida en su acceso.[96]

Podremos resumir, por tanto, los usos permitidos de la Ley en los siguientes:

- Los propios de las funciones de la Agencias gubernamentales habilitados por Ley.

- Los necesarios para asegurar la seguridad de los vehículos, o relacionados con el robo de vehículos o con las emisiones de los mismos.

- Los relacionados con las investigaciones del mercado de vehículos o encuestas.

- Los propios y necesarios de la actividad "legítima" del tráfico jurídico de vehículos.

- Los relacionados con los procesos civiles, penales o administrativos.

- Los relacionados con actividades estadísticas o de investigación académica.

- Los amparados por la actividad de seguro o la actividad de investigación privada.

- Los relacionados con las notificaciones de vehículos retenidos o remolcados por la autoridad pública o en las actividades de peaje.

- Los que vengan amparados por previa autorización o consentimiento de uso obtenido por el Estado del titular de los datos. También si existe ese consentimiento al Estado para marketing.

- Para cualquier solicitante que acredite consentimiento escrito del titular de los datos.

- Para cualquier uso legítimo estatal justificado por seguridad pública.

[96] Vistas las excepciones y la permisividad de usos el término "*highly restricted personal information*" parece quedar desnaturalizado.

Además se permite la reventa o nueva puesta a disposición de esos datos por uno de los poseedores autorizados de los mismos, a excepción de los casos establecidos en los números 11 y 12 anteriores sobre la "highly restricted personal information". Requiriéndose una nueva autorización para ese nuevo negocio jurídico, así como para la distribución general por razones de encuestas, marketing o requerimientos. Debiéndose mantener un control y registro temporal de ello de al menos 5 años.[97]

El resto del articulado termina la regulación dentro de un interés menor. El parágrafo 2722 presenta clausulas de mayor salvaguarda para el caso de contrataciones fraudulentas, o falsas representaciones para conseguir acceder a los datos personales al amparo de los usos permitidos por esta Ley. El 2723 con el enunciado "Penalties" establece las sanciones a las infracciones de la Ley, siendo el recurso habitual la multa que está habilitado a imponer el Fiscal General de cada Estado en no más de 5.000 dólares por día de incumplimiento. El 2724, por último, con el título "Civil action" establece la posibilidad de interponer recurso de responsabilidad civil.[98]

[97] En la letra (c) "*Resale or Redisclosure*": *"...Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request. "*

[98] Como jurisprudencia importante sobre esta Ley citaremos: el caso "Margan v. Niles 250 F. Supp. 2d 63 (N.D.N.Y. 2003)" o el caso "Luparello v. The Incorporated Village of Garden City, 290 F. Supp. 2d 341 (E.D.N.Y. 2003)".

CAPÍTULO SEGUNDO

LA PROTECCIÓN DE LA PRIVACIDAD DE LOS CONSUMIDORES EN EE.UU.

1. Introducción.

El ciudadano en las últimas décadas ha devenido, de manera cada vez más inexorable, en consumidor. A través de esa figura, antes en parte y ahora en casi todo, se ha revelado cada vez más en el ejercicio de sus derechos. Ello en EE.UU se observa quizá todavía en una mayor magnitud.

Así, las entidades comerciales de todo tipo han venido mostrando un interés creciente en nuestros hábitos de consumo. Esa información es, hoy por hoy, valiosísima. Y demuestra tener un interés comercial enorme para otros sujetos distintos a su titular. Esa información personal de hábitos de consumo se traduce en innumerables posibilidades para el marketing, las técnicas de venta o cualquier otro medio de aprovechamiento comercial, que ofrece un enorme valor a las empresas en la economía de mercado.

Esos datos personales se graban, se almacenan, y se comercian. Nuestra huella digital vale dinero en el mundo electrónico y en el mundo físico. Desde la publicidad personalizada hasta las características de personalidad y gustos musicales, preferencias literarias o audiovisuales, que pueden utilizarse para prevenir o favorecer en futuros perfiles laborales, nuevas ofertas de cliente o vigilancia policial, nos pueden servir de claros ejemplos. En Estados Unidos al menos es así. En Europa en general y con algunos matices, también.

1.1 Sistema de protección jurídica del consumidor en EE.UU.

En EE.UU. existen multiplicidad de leyes que nos ofrecen regulación sobre privacidad, pero además esta multiplicidad se expande exponencialmente dentro de la protección de

la privacidad de los consumidores. No solo nos encontramos con varias leyes, que estarían a su vez dentro del círculo más amplio de la protección de la privacidad en general, sino, además, con un sistema de jurisprudencia de mayor abundancia e incidencia que en otros campos; con un sistema de acuerdos civiles y jurídico mercantiles de gran importancia regulatoria; y, sobre todo, con una actuación administrativa muy poderosa y de nivel cuasiconstitucional reflejada en las regulaciones y actos de la Federal Trade Comission (FTC), que es el órgano regulador del Comercio (y de buena parte de la Competencia) en EE.UU.

Junto a lo anterior, debemos apuntar que el nivel de garantía para los derechos de privacidad varía en función del régimen sectorial y el contexto regulatorio en que nos encontremos.

Nos parece importante, así, la apreciación que realizan Slove y Schwartz (2015, 759) en la que ponen como ejemplo la consistencia del sistema europeo de protección de datos que salva esta "aproximación sectorial" con una ley "ómnibus" "*that provides a general safety-net in these countries (european) for areas or regulatory issues that a sectoral statute may not adress*". Es decir que provee de una seguridad jurídica que las Leyes sectoriales estadounidenses no alcanzan.

Esa falta de coherencia es, por tanto, un foco de crítica de esa orilla estadounidense y de su propio sistema de protección (en este caso de privacidad del consumidor). Si bien debemos añadir que esa armonización europea que se pone de ejemplo, es mérito de la Unión Europea, como veremos, a través primero de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (y que supuso como sabemos un cimiento sobre el que se construyeron todas las legislaciones de protección de datos nacionales en Europa); y ahora más si cabe con la mejor homogeneización de derechos en su forma de Reglamento europeo de protección de datos (2016/79 del Parlamento y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)).

Otra característica es la posibilidad abundante de uso de la autorregulación. Algo consustancial a la protección de la privacidad del consumidor americano y muy enraizado en el espíritu fundador del país.

Las propias empresas se dotan de verdaderos reglamentos para tratar de proteger los datos de sus clientes, como una forma más de su política de empresa y de atractivo comercial. En la vigilancia de los usos de esas prácticas, la FTC es la que tiene el poder regulatorio posterior más amplio.

Además, y conectado a la idea anterior, ha proliferado todo un negocio de profesionales de la privacidad que provee de certificaciones de garantía a las empresas en estos ámbitos. Son como las agencias de calificación de la deuda o los grupos de acreditación en auditorias de calidad pero en el campo de la privacidad. Incluso algunas empresas han instaurado su propios CPO's (Chief Privacy Officer) encargados de la protección de datos en la compañía. La figura del Reglamento Europeo del Delegado de Protección de Datos parece seguir esta estela.

Por último, debemos presentar asociada la idea jurídica de la *Personally Indentifiable Information (PII)*, concepto principal y sobre el que pilota toda la protección de los datos personales del consumidor americano. Básicamente es aquella información que permita identificar personalmente. Es objeto jurídico de protección de muchas de las leyes de privacidad en EE.UU., principalmente en las que ahora nos ocupan sobre protección del consumidor. Podemos observar que guarda similitud con el carácter de identificable y de identificada de la información de persona física, para que entre en juego la protección de datos europea.

La definición que hemos dado es la "tautológica" (de mayor repetición) que es la contenida en la "*Video Privacy Protection Act (VPPA)*". También se puede conceptuar como lo hace la "*Gramm-Leach-Bliley Act*" (que veremos en la parte de privacidad financiera) como la información no pública; o en una tercera manera al estilo de la COPPA ("Children Online Privacy Protection Act") que es la de los "tipos específicos" que permitan "construir" la identidad de la persona. Además leyes estatales ofrecen su propia visión conceptual.[99]

[99] La "Song- Beverly Credit card Act" californiana de 1971 es muestra de ello. Además esta Ley de California ha originado dos casos interesantes de construcción jurisprudencial sobre el concepto y que

1.2 Tipos de regulación de la privacidad del consumidor estadounidense.

Debemos relatar que hay distintas aproximaciones a la hora de defender la privacidad del consumidor en EE.UU. y se posicionan desde distintos ámbitos del Derecho. Por tanto no ya solo se nos presenta la heterogeneidad y sectorización en la construcción legal de esta defensa, sino que, además, hay distintas posturas de esa defensa desde ámbitos y niveles jurídicos distintos. Podemos resumirlas previamente así:

- La aproximación civil y mercantil, que se compone por una atención jurídica a la protección de la privacidad desde posiciones propias del derecho de la persona y de la propiedad, con tres ramas principales: la *Tort Law*, o la construcción del sistema de protección de la privacidad por la vía de la responsabilidad civil (en un traducción literal sería el derecho de agravios), y se trata de una primigenia manera de defensa de los datos personales en EE.UU. La *Contract Law* o defensa de la privacidad por acuerdos mercantiles o civiles, que es la vía puramente contractual entre particulares. Para alguna doctrina también la privacidad se puede afrontar desde el derecho de propiedad (*Property Law*). Como si aquella fuera un derecho de disposición y la persona pudiera enajenarla o desprenderse de ella por dinero.[100]

---

han influido más allá de los límites del Estado: Florez v. Linens'N things Inc. 108 Cal. App.4th 447,450 (2003) que prohíbe recoger de los usuarios de tarjetas de crédito su PII en las transacciones y que se cita y sirve de precedente en el caso Pineda v. Williams-Sonoma Stores 246 P.3d 162 (Cal. 2011). Otros de los casos a citar en la construcción del PII es el de Apple v. Krescent 292 P. 3d 883 (Cal.2013) basado en esa Ley estatal y también sobre la información personal contenida en las transacciones de tarjeta de crédito.

[100] Desde la óptica europea consideramos el derecho a la protección de los datos personales como parte de los derechos personalísimos y contemplamos esta aproximación como una curiosidad propia de EE.UU. más que como un sistema de protección de derechos válido.

Hay, sin embargo, corrientes doctrinales en EE.UU que abogan por una menor regulación de los poderes públicos, y una mayor autorregulación personal de la privacidad aduciendo que, así, este derecho se adaptaría mejor a la realidad. Cate (2001) o Goldman (2002) son ejemplos de estas teorías puramente mercantilistas que tienen su encaje en EE.UU pero todavía resultan algo chocantes en Europa.

Otros comentaristas legales abogan por una posición intermedia que mezcle la regulación pública al uso, con la autorregulación. (Hirsch, 2006)

Otros se preguntan directamente si realmente sigue existiendo la privacidad. Si ya no es demasiado tarde. Y si lo que debemos conocer es más bien quien nos vigila aludiendo a la Transparencia. (Brin, 1998).

- La aproximación jurídico-administrativa y legal, que establece el derecho positivo sustantivo de protección válida para la privacidad del consumidor en EE.UU., aproximación que seguiremos y estudiaremos más adelante.

En un primer nivel se encontrarían las regulaciones legales que se distinguen en función de la competencia del órgano político jurídico actuante (principalmente planos federal o estatal) (*Federal Statutory regulation* y *State Statutory Regulation*). Dentro de ellas, (si bien casi únicamente en su ámbito federal), las estudiaremos en función de las distintas materias de consumo que vienen a regular, que de manera sintética hemos establecido en: la privacidad del consumidor en el ámbito del entretenimiento, en el ámbito de consumo de internet y en el de marketing. Mención especial y en último término recabaremos de la privacidad financiera que la estudiaremos como una subespecialidad con entidad propia dentro de la privacidad del consumidor estadounidense.

En otro nivel se encontraría el desarrollo institucional e institucionalizado de la protección de la privacidad del consumidor a través de la *Federal Trade Commission* (en adelante FTC) que se manifiesta como el órgano superregulador y de vigilancia en el desarrollo normativo y protección del derecho a la privacidad del consumidor estadounidense. Las Regulaciones de la FTC, que siguen el mandato de la sección 5 de la *FTC Act* (contenida en el parágrafo 45 del 15 del U.S.C.), suponen un verdadero corpus de derecho de desarrollo normativo que contiene buena parte de las obligaciones que en materia de privacidad de consumo las empresas de Estados Unidos deben observar y acatar.

En esta aproximación legal y reglamentaria, que dicho sea, es la de mayor abrazo jurídico y consistencia general en la protección de la privacidad estadounidense, es en la que centraremos nuestra mayor atención.

2. La aproximación civil y mercantil

2.1 *Tort Law*: el intento de defensa de la privacidad del consumidor por la vía del ilícito civil.

Con raíces en el *Common Law* y sobre la base de la doctrina ya estudiada de "Warren & Brandeis"[101], piedra angular y fundacional de la privacidad en EE.UU, se plantea esta vía de aproximación de manera original, para afrontar posibles responsabilidades por la información vertida en los medios de comunicación, y cercana a lo que conocemos como la protección del derecho al honor y a la propia imagen. Es evidente que esta aproximación, para la efectiva y general defensa de la privacidad del consumidor en el día a día, se ha visto superada. Si bien como precedente en su defensa de la privacidad, y como recurso al que acudir para algunos casos flagrantes, presenta un interés digno de reflejar.

Algunos autores ven esta forma de manifestación del derecho, ya no solo alejada del propósito de defensa de la privacidad, sino contraria a la misma, aduciendo mayores posibles inconvenientes con la revelación de información, que ventajas para su adecuada defensa. (Volokh, 2014)

El inicio de la sustanciación de este tipo de protección de la privacidad en Estados Unidos lo encontramos en el mencionado trabajo doctrinal de Prosser, "Privacy" (1960) y al que ya aludimos en la primera parte del trabajo. En su artículo, Prosser definía los cuatro posibles agravios civiles que se podían dar en la perturbación de la privacidad:

1. El de intrusión en los asuntos privados del demandante.

2. El de revelación pública de hechos privados y embarazosos sobre el demandante.

3. El de la publicidad que ponga al demandante en una imagen pública falsa o errónea.

[101] Warren & Brandeis (1890)

4. El de apropiación del nombre o imagen del demandante, para provecho del demandado.

En cuanto a construcción jurisprudencial, quizá uno de los pronunciamientos judiciales más importantes sobre *Tort Law* y privacidad se nos presenta en "Dwyer v. American Express Co. 652 N.E.2d 1351 (1995)". En este caso, un grupo de usuarios de esta conocida forma de pago con tarjeta, se queja del uso que la empresa hace de sus datos, y que revelan hábitos de compra. Se consideran víctimas de una invasión de su privacidad y de fraude contra el consumidor. El fiscal general de Nueva York mandó nota de prensa (mayo de 1992) informando del acuerdo al que los demandantes habían llegado con la empresa. Posteriormente los periódicos se hacen eco de la noticia. El jugo informativo era atrayente, ya que los artículos de prensa informaban de la clasificación que hacía American Express de sus clientes en seis categorías en función de su capacidad de gasto, y que podían conceptuarse incluso como del tipo "Rodeo Drive Chic".

En definitiva, como nos dice el Tribunal, los demandantes consideraban violado su derecho a la privacidad.

El Tribunal es didáctico al respecto, estableciendo las causas por las que la *Tort Law* podría operar en defensa de la privacidad: invasión de la misma, apropiación de nombre o identidad, revelación de hechos privados y publicidad falsa sobre una persona (calumnias).[102] Los demandantes alegaban el primer supuesto ("*Intrusion upon Seclusion*"), si bien se desestima por el Tribunal en su pretensión, ya que el uso de la tarjeta es voluntario, y refleja información de manera automática para los demandados (American Express), si bien estos no cometen una intrusión no autorizada.[103]

[102] *"There are four branches of the privacy invasion tort identified by the Restatement (Second) of Torts. These are: (1) an unreasonable intrusion upon the seclusion of another; (2) an appropriation of another's name or likeness; (3) a public disclosure of private facts; and (4) publicity which reasonably places another in a false light before the public"*

[103] *"…Plaintiffs' allegations fail to satisfy the first element, an unauthorized intrusion or prying into the plaintiffs' seclusion. The alleged wrongful actions involve the defendants' practice of renting lists that they have compiled from information contained in their own records. By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation…"*

El Tribunal cita un caso que sí considera más cercano al que le ocupa, en un magnífico alarde propio de *Common Law*, con el asunto "*Shibley v. Time*", en el que también se observaba una posible apropiación indebida del nombre de suscriptores para crear listas y elementos distintos a los autorizados en su recabación.[104] Para acreditar que, al igual que en aquel, no se observan los requisitos de antijuridicidad que venían alegando los demandantes.[105]

Por tanto, con este caso tenemos un claro ejemplo de las limitaciones que el "Tort Law" puede ofrecer en la defensa de la privacidad, que no podría alegarse cuando se cedan voluntariamente los datos.[106]

Si bien hay otros casos en los que sí que ha habido un reconocimiento por los Tribunales del daño económico, como en el famoso caso Fraley v. Facebook[107] en el que se utiliza a un consumidor en la publicidad de la red social con la aplicación "*Sponsored Stories*", argumentándose no ya un daño mental o moral por parte de los demandantes, sino un daño económico por utilización de imagen sin compensación por parte de Facebook.[108]

Se manifiesta así de nuevo la excesiva determinación de la voluntariedad o no en la cesión y suministro de datos como elemento esencial para que juegue o no la protección de la privacidad desde esta perspectiva del *Tort Law*.

---

[104] *"…However, we find that this case more closely resembles the sale of magazine subscription lists, which was at issue in Shibley v. Time, Inc. (1975), 45 Ohio App.2d 69, 341 N.E.2d 337. In Shibley, the plaintiffs claimed that the defendant's practice of selling and renting magazine subscription lists without the subscribers' prior consent "constitut[ed] an invasion of privacy because it amount[ed] to a sale of individual `personality profiles,' which subjects the subscribers to solicitations from direct mail advertisers...."*

[105] *"…we again follow the reasoning in Shibley and find that plaintiffs have not stated a claim for tortious appropriation because they have failed to allege the first element. Undeniably, each cardholder's name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess…"*

[106] En parecido sentido denegatorio en el ámbito *Tort Law* para la efectiva protección de la privacidad podemos citar el caso *Remsburg v. Docusearch INC. United States 090 DNH 2002 (District Court, D. New Hampshire.Civil No. 00-211-B)*

[107] *Fraley v. Facebook (830 F. Supp. 2nd 785 (N.D. Cal. 2011)*

[108] La Corte californiana da la razón a los demandantes por esa violación para uso comercial y Facebook accedió a un acuerdo para poner fin al procedimiento, que incluía, además de una serie de rectificaciones en su actuación de privacidad, un pago de 20 millones de dólares a repartir entre los afectados.

Siguiendo esa linea de crítica general con esta aproximación de protección y en este sentido, lo que parece evidente es que nuestros patrones de consumo son una marca permanente sobre nuestra identidad, que son aprovechados día a día por las empresas. Hasta el punto que pueden llegarse a construir verdaderos perfiles psicológicos, ideológicos, o de comportamiento que están fuera de nuestro control de privacidad.[109] Autores como Kang (1998) opinan que esa vigilancia inhibe nuestra libertad individual de elección.[110]

Esta visión del problema está en que esta forma de vigilancia acorta la libertad individual. Para Slove (2006) la diferencia con el gran hermano orwelliano se prevé en una partida distinta. En una supuesta libertad de actuación virtual que hace que esos datos lleguen a ser recogidos de manera voluntaria y cedidos así. Diferenciándose de la mucho más evidente orquestación orwellinana totalitaria. Por lo tanto aquí el mundo orwelliano difiere, no en los medios, sino en los fines de la actual vigilancia, al menos en la llevada a cabo por el Mercado.[111]

Resulta asimismo muy interesante la posición de Schwartz (1999) sobre la información que se ofrece no solo sobre lo que se compra sino en el consumo de las ideas.[112]

Sobre estos parámetros resulta muy difícil una protección efectiva de la privacidad sobre la base de un mero "face to face" con empresas multinacionales que disponen de manera rápida e incontrolada de nuestros datos (aún prestados voluntariamente). Sería un escenario de protección propio de multitud de David(es) aislados contra Goliats perfectamente armados y preparados.

[109] Karas (2002) alerta sobre la facilidad para identificar nuestra ideología.
[110] Recordándonos el Gran hermano de Orwell, que puede llevarnos a la autocensura.
[111] Solove (2006, 36) El argumentario del proceso de Kafka resulta más apropiado para el autor para la problemática y dimensión del dossier digital. El problema se planteaba en quien le acusaba a Joseph K. y en cual era la autoridad que estaba detrás de aquella acusación.
[112] Schwartz (1999, 700) Concretamente nos asegura su inconveniente democrático: "…*This state of affairs is bad for the health of a deliberative democracy. It cloaks in dark uncertainty the transmutation of Internet activity into personal data that will follow one into other areas and discourage civic participation. This situation also has a negative impact on individual self-determination; it makes it difficult to engage in the necessary thinking out loud and deliberation with others upon which choice-making depends. In place of the existing privacy horror show, we need multidimensional rules that set out fair information practices for personal data in cyberspace*…"

2.2 *Contract Law* o el respeto a lo pactado en materia de privacidad.

Esta aproximación nos presenta la protección de la privacidad como un elemento de cumplimiento contractual (*pacta sunt servanda*) que se puede manifestar, o bien a través de una catálogo de políticas de privacidad que nos concede la empresa y que nosotros aceptamos, o bien con contratos con cláusulas que fijen y establezcan los impedimentos a las revelaciones o las protecciones de privacidad a seguir.

Las políticas de privacidad que vienen ya dadas por las grandes empresas nos parecen un elemento de hegemonía empresarial en su relación contractual con el consumidor fuera de toda duda. Además, estas políticas suelen venir acompañadas de esa previsión *opt-out* trasladando al consumidor la carga de ir estableciendo los momentos en que su privacidad se encuentre protegida (optar por que no sea revelada), lo que en muchas ocasiones las pueden hacer inútiles para su supuesto objetivo de efectiva protección. El modelo *opt-in* parece más adecuado a este propósito, presentando en principio la posibilidad de excepción en que sean reveladas, y requiriendo para ello consentimiento.

En este sentido citaremos a Sovern (1999) que nos dice básicamente que los consumidores no pueden proteger de manera efectiva su información personal a través de estas políticas.[113] Otros autores como Staten & Cate (2003), nos ofrecen también estudios sobre el impacto positivo de las políticas *opt-in*.

Algunos otros comentaristas (Solove & Hartzog, 2014, 595) se plantean la idoneidad de esta figura contractual de protección de la privacidad. Además de informarnos de su escaso recorrido jurídico, ya que tomar la normativa de privacidad como contractual se plantea de manera muy reciente (a partir de 2001 es cuando aparece el primer pronunciamiento judicial sobre el tema.) Así, se preguntan si son contratos las políticas de privacidad. Y se remontan para su contestación al primer pronunciamiento judicial al

[113] Sovern (1999, 1079 y 1129*):"…consumers cannot protect their personal information when they are unaware of how it is being used by others". Si bien nos asegura que un modelo "opt-in" puede ser preferible: "…an opt-in system is preferable, chiefly because it eliminates the incentive firms have to engage in strategic behavior and thus inflate consumer transaction costs*."

respecto, que establecía que "el acuerdo de uso es un documento legal", y que venía a establecer la relación entre el usuario y la empresa en el asunto del caso Ebay. Mediante el acuerdo se ponían de relieve y se determinaban "los servicios, el precio, la política de privacidad y la relación entre el comprador y el vendedor…"[114]

Igualmente,y por último, podemos fijar nuestra atención en esta irrelevancia sobrevenida, y gradualmente creciente (o a *sensu contrario* de influencia decreciente) de la *Contract Law* en la protección de la privacidad siguiendo a los propios Solove y Hartzog (2014), que así la establecen expresamente como tal. Aquel derecho que pareciera fuera a jugar un papel importante, ha jugado al final "solo un papel marginalmente significante"[115]

Comprobamos así la posible irrelevancia que se nos revela con esta opción para una efectiva protección de los datos personales de los consumidores y su aseveración por la mayor parte de la Doctrina.

Otro elemento de consideración que consolida esta línea de crítica lo encontramos en la Jurisprudencia, en el asunto "*In Re Northwest Airlines corp. privacy litigation (No. 1618. 337 F.Supp.2d 1360 (2004)")*, en el que el Tribunal avala la teoría de los demandados de que las políticas de privacidad en forma de "*general statements*" no tienen fuerza contractual, y que la clausula de privacidad no era un contrato en sí mismo.

[114] Asunto Raley v. Michael, 56 Va. Cir. 87, 88 (2001) Si bien los autores establecen otro pronunciamiento judicial como el primero que afronta las políticas de privacidad bajo el prisma de la teoría del "Contract Law" como es en el caso Crowley v. CyberSource Corp 166 F. Supp. 2d 1263, 1267–68 (N.D. Cal. 2001)

[115] Solove & Hartzog (2014, 596-597) "…Today, contract law—formal contract and promissory estoppel—plays hardly any role in the protection of information privacy, at least visà- vis websites with privacy policies. Contract law litigation theories have barely been attempted, as the number of cases involving these theories has been exceedingly low over the past fifteen to twenty years after the rise of privacy policies."

"*…Thus, contract law, which initially seemed to be the most appropriate tool to redress privacy policy violations, has played only a marginally significant role in these disputes. Instead, such violations have predominantly been redressed through the public enforcement of the FTC.*"

2.3 *Property Law*. La privacidad como mercancía personal.

Tal y como hemos adelantado, dejaremos citada algunas posiciones doctrinales que defienden la privacidad (y su posible protección) dentro de los bienes susceptibles de comercio. Principalmente son algunos autores estadounidenses, como Murphy (1996) que propugna la información personal como una propiedad más, con la pretendida facultad de disposición sobre la misma, o Lessig (1999) que la asimila directamente a la propiedad. Y otros como Kang, (1998) que ofrece una interpretación y visión de la privacidad como mezcla entre derecho de propiedad y derecho contractual, pudiendo el consumidor recibir ofertas para vender la parte de información personal que decida y que las empresas consideren de mayor valor para sus fines.

Son otros muchos autores los que no solo no abogan, sino que critican duramente esta aproximación mercantilista y economicista al derecho de privacidad. Entre ellos podremos destacar la posición de Byford (1998) que nos dice que la privacidad como elemento de comercio solo le da valor desde la perspectiva del que quiera pujar por ella o comprarla. O la posición de Pamela Samuelson (2000) y lo inadecuado, desde su punto de vista, de la protección de la privacidad a través de los derechos de propiedad.

Y se hace eco de la historia y el derecho europeo para defender su postura (que compartimos totalmente incidiendo desde la perspectiva de la defensa de los derechos humanos) (Samuelson, 2000, 1143-1144):

> *"…From a civil liberties perspective, propertizing personal information as a way of achieving information privacy goals may seem an anathema. Not only might it be viewed as an unnecessary and possibly dangerous way to achieve information privacy goals, it might be considered morally obnoxious. If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.*
>
> *Europeans have more of a civil libertarian perspective on personal data protection in part because of certain historical experiences they have had. One factor that enabled the Nazis to efficiently round up, transport, and seize*

assets of Jews (and others they viewed as "undesirables") was the extensive repositories of personal data available not only from public sector but also from private sector sources. Europeans may realize more than most Americans the abusive potential for reuses of personal data that may initially have provided to a particular entity for a specific, limited purpose. If more Americans had an appreciation of the negative consequences that might arise from commercial distributions of their personal data, they might perceive personal data protection differently."

Solove (2001) lo critica desde la perspectiva de la visión de mercado sobre los derechos de privacidad y su incapacidad para darle un valor real. Algo así como una puesta al día de la famosa y sabia aseveración de Quevedo de que solo un necio confunde el valor con el precio. Incidiendo además en la falta de equidad entre los actores (empresas - consumidores) [116]

Solución de conjugación de tipo ideal la propugna Schwartz (2004) con su modelo de datos personales que se puedan hacer propiedad en un entorno de respeto y protección de la privacidad individual. Una especie de limitación del derecho individual parcial con intervención de las instituciones, también en su supervisión. Con la aproximación de su concepto de "inalienabilidad híbrida", que consistiría en la posibilidad de restricción de esa transferibilidad de uso. El usuario podría transferir en una primera instancia sus datos, pero con la posibilidad de cortar o bloquear esa autorización en un futuro y para otro tipo de entidades no vinculadas en esa primera relación de autorización, y que requerirían ya nuevas autorizaciones *opt-in*.[117]

[116] Solove (2001, 1392-1393) Es interesante el tenor literal de sus palabras cuando afirma: *"…These solutions cannot work effectively in a situation where the power relationship and information distribution between individuals and public and private bureaucracies is so greatly unbalanced. In other words, the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that a regime of default rules alone (consisting of property rights in information and contractual defaults) will not enable fair and equitable market transactions in personal information."*

[117] Schwartz (2004, 2094) *"…This Article calls this model "hybrid inalienability" because it allows individuals to share, as well as to place limitations on, the future use of their personal information. The proposed hybrid inalienability follows personal information through downstream transfers and limits the negative effects that result from "one-shot" permission to all personal data trade…"*

3. La previsión legal y reglamentaria.

Comenzaremos este apartado de la protección de la privacidad del consumidor estadounidense por el estudio de la sección 5 de la FTC Act y el análisis de las reglamentaciones surgidas de la FTC. Precisamente por conjugar la aplicación y mandato legal de esa "Fair Trade Comission Act" con su importantísimo desarrollo reglamentario y de órdenes ejecutivas, así como con el estudio de los asuntos de mayor interés en los que la FTC ha actuado en su función reguladora, y que han podido influir en la creación de derecho y comportamiento jurídico posterior de las empresas estadounidenses.

Después haremos un análisis del resto de leyes, principalmente federales, que afectan y tienen algo que decir sobre la privacidad del consumidor en EE.UU. y que, junto a lo anterior, configurarán el principal de esta parte del estudio. Esas leyes, como hemos apuntado, las hemos agrupado en función de su temática en los siguientes apartados:

- Regulación legal de la privacidad en el consumo de entretenimiento (*The Cable Communications Policy Act* de 1984 y *The Video Privacy Protection Act* de 1998)

- Leyes en el del uso y consumo de Internet (*The Computer Fraud and Abuse Act* de 1984 y *The Children's Online Privacy Protection Act* de 1998)

- Regulaciones legales en la privacidad en el Marketing (*Telephone Consumer Protection Act* de 1991; *Telemarketing and Consumer Fraud Abuse Prevention Act* de 1994 y *The CAN-SPAM Act* de 2003)

En último lugar, y destacando su importante especialidad dentro de la privacidad en el consumo de la sociedad estadounidense, veremos la privacidad financiera (*Financial Privacy)* que se manifiesta de mucha relevancia en la protección del consumidor en sus relaciones con los bancos y otras entidades financieras. Aquí veremos de manera destacada la *Fair Credit Reporting Act* de 1970, *The Right to Financial Privacy Act* de 1978, *The Identity Theft Assumption and Deterrence Act* de 1998 así como *la Financial Modernization Act (Gramm-Leach-Bliley Act)* de 1999.

3.1. La *FTC Act* y su importante desarrollo reglamentario. Las actuaciones de la FTC.

Debemos partir, como premisa aclaratoria, de que la *Federal Trade Commission* (en adelante FTC) es el órgano encargado de velar por la protección de la competencia en el comercio estadounidense y que, estando su principal bien jurídico a proteger en la competencia de los mercados, actúa mediatamente en la protección de la privacidad del consumidor; precisamente por ser el cumplimiento de esas obligaciones de respeto de privacidad dadas una de las más importantes consideraciones para que una empresa no se encuentre en posición ventajosa en ese mercado frente a otras que sí las cumplen. Y ello en virtud del mandato legal de la sección 5 de la ley federal que regula su funcionamiento.

La FTC como institución fue, así, creada bajo el impulso planificador y de ánimo regulatorio que la crisis de 1929 hizo germinar en el Gobierno de Franklin Delano Roosevelt. Sería la precursora en EE.UU. de la defensa de la competencia y del control del comercio, y garante de su defensa. Órgano institucional omnipotente en las relaciones comerciales que, desde entonces, se viene encargando de la crucial tarea de evitar los monopolios, y de velar por los derechos e intereses de los consumidores y usuarios. Una especie de reunión de la comisaría europea de competencia y de agencia de protección de consumidores, que, por si fuera poco, ocupa un lugar prevalente en la protección de los datos personales de los ciudadanos en sus comportamientos como usuarios de consumo.[118]

[118] Su símbolo en forma de estatua en la puerta de su sede en Washington es el de un hombre fuerte controlando un caballo que representaría el Comercio. Una metáfora muy directa del ánimo de los tiempos de su fundación, que refleja el espíritu intervencionista y regulador de la economía, y que marcaría el periodo económico desde entonces hasta 1973. Hoy parece que el toro bravo y desbocado que domina la portada de la Bolsa de Wall Street es el símbolo más vinculado a nuestros tiempos, sobre todo hasta 2008.
La composición de la FTC se establece en el título 15 U.S.C. § 41 bajo el título "*Federal Trade Commission established; membership; vacancies; seal*".
Es un órgano de supervisión y control y cuya formación responde a criterios político-democráticos, más que estrictamente técnicos. Hay 5 comisionados nombrados por el Presidente de EE.UU. con el visto bueno del Senado. No más de tres serán miembros del mismo partido y por periodos máximos de 7 años. El Presidente de EE.UU. elegirá quien de los miembros presidirá el órgano, siendo el cargo incompatible con cualquier otra actividad y quedando reservada al Presidente de los EE.UU. la remoción

3.1.1 Estudio de la sección 5 de la *FTC Act.* Ámbito y contenido.

La *Federal Trade Comission Act*, codificada en el título 15 del U.S.C. (Parágrafos 41 a 55) se aplica a la regulación del comercio y la realización de negocios en EE.UU. siendo éste el objeto de su actuación.

La Ley (*FTC Act*) no es propiamente una Ley de protección de la privacidad ni regula categorías determinadas de datos personales (relacionados con la actividad comercial), si bien protege de conductas o prácticas fraudulentas, que pueden afectar a los consumidores. También de aquellas prácticas que, con la utilización o mal uso de los datos personales extraídos de esa actividad comercial puedan afectar a la misma.

En su autoridad, la FTC sanciona, y en general, revisa el comportamiento de las empresas que no observan la protección de datos de los consumidores, que hayan modificado su política de protección de la privacidad sin una adecuada publicidad, o que no hayan cumplimentado la obligación de comunicación de esa política de privacidad. Pero ello no como agencia de protección de datos, sino como órgano regulador del comercio en EE.UU. Nos encontramos, así, ante una protección de "aproximación indirecta" pero que resulta de suma importancia para la protección de la privacidad del consumidor americano, como veremos.

La sección 5 de la Ley es precisamente la que se utiliza para gravar y sancionar a las empresas que no han cumplido con su propia política o principios de privacidad. Esta determinación no está específicamente contenida en la norma, ya que esta sección 5 es de tipo amplio y va dirigida a la sanción de conductas monopolísticas. Es la propia interpretación del órgano FTC de la norma la que incluye como conducta contraria a la competencia el uso y diseminación de la información personal y datos de los usuarios, contraviniendo las propias políticas de privacidad de la empresa. Será a partir de 1998 y con el asunto *Geocities*[119], el primer momento en el que actúa la FTC sobre la

de sus miembros por ineficiencia, negligencia o infracción en el cargo, teniendo su sede en Washington D.C. y siendo su jurisdicción federal.

[119] United States of America Federal Trade Commission in the matter of Geocities, a corporation. File no. 9823015.

privacidad en Internet, donde se asimila como competitivamente engañosa ("*deceptive*") la recopilación de información personal sin consentimiento ni información.

No obliga, por tanto, a que las empresas mantengan una determinada política de privacidad, (algo que dista mucho de la regulación "erga omnes" europea), pero sí a que se cumpla la que la propia compañía se haya impuesto. En una determinación reglamentaria del clásico principio "pact sut servanda" de manera general.

También seria penalizable un cambio retroactivo de la propia privacidad de la empresa sin la consiguiente comunicación de *opt out* a sus usuarios que puedan verse afectados. Se trata de asegurar la falta de engaño a los consumidores. También en lo que a privacidad se refiere.

La FTC en su actuación amparada en la sección 5, establece asimismo algunos consejos de regulación de buenas prácticas a las empresas en su elaboración de sus políticas de privacidad, principalmente encaminados a que se implemente el consentimiento expreso de los usuarios por parte de las empresas en esas políticas.

Hace también especial hincapié en sus sugerencias a las empresas para el consentimiento expreso en los siguientes temas:

- Datos financieros.

- Datos que afecten a menores.

- Información y datos de salud.

- Información y datos sobre localización geográfica precisa.

- Números de seguridad social.

La Ley marca los objetivos de actuación de la FTC, dirigiéndola de manera principal a prevenir prácticas ilegales que afecten a la competencia en personas, corporaciones, empresas (personas jurídicas en sentido amplio), dejando a un lado a las que operen en el sector bancario y financiero, que tendrá su regulación diferenciada en cuanto a competencia y también en lo que a privacidad se refiere (como veremos más adelante en la subespecialidad de la *Financial Privacy*).[120]

[120] Las excepciones afectan concretamente a las establecidas en el Título 12 del U.S. Code, que viene

En el parágrafo 44 se definen ya los conceptos y definiciones para el adecuado seguimiento de la Ley.[121]

Ahora bien, quizá el artículo más importante y de principal efecto regulatorio de la *FTC Act*, en el sentido que nos interesa, se encuentra en el parágrafo 45 de la sección 5 bajo el enunciado de "*Unfair methods of competition unlawful; prevention by Commission*".

En este epígrafe se sustancian las conductas monopolísticas o anticompetitivas, empoderando a la FTC para su vigilancia y control, con excepción de los negocios financieros y bancarios que se regulan en la normativa de privacidad financiera que también será objeto de nuestra atención.

Es por tanto este, el artículo en el que se fundamenta la actuación de la FTC en defensa del derecho a la protección de datos de los consumidores. Constituye la protección de la privacidad en el ámbito del consumo y a través de la FTC, como apuntábamos, una consecuencia más o menos directa de la protección del derecho de competencia en Estados Unidos, ya que se conceptualiza una quiebra en la privacidad del consumidor como una posible brecha ventajosa para determinadas empresas.

El primer punto de este parágrafo 45 (letra a) dota de jurisdicción y de ámbito sustantivo a la FTC para declarar la ilegalidad y prohibir los actos contrarios a la Competencia.

La definición por excelencia de esta norma que sirve para la principal función de la FTC es la "Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign tradees" y que se materializa en la de atajar todos aquellos métodos que ya son declarados ilegales por esta Ley.[122]

---

referido a entidades bancarias y de ahorro "*Banks and savings*". Encargándose la sección 1813 básicamente de la definición de bancos y entidades de ahorro que incluye a todo tipo de estas entidades, incluidas también las estatales, de depósito y de crédito. La sección 1766 se encarga de establecer los poderes de administración y regulación de "The Board" Según la sección previa 1752 se refiere a la entidad de supervisión bancaria

[121] 15 U.S.C. § 44 "*Definitions*". Se tratan las definiciones de Comercio, Corporación o de "Antitrust Acts". Si bien todos son de relevancia, aquí destacaríamos una de interés como es la definitoria de las agencias y autoridades extranjeras (entres ellas las de protección de datos europeas por ejemplo)

[122] *Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful*.

Dentro de esos métodos "injustos o engañosos" se ubica, según la FTC, la falta o dejación de protección de la privacidad de los usuarios, sobre todo tal y como debería haberse cumplido por las empresas.[123]

Como ilustración del grado de importancia que la FTC tiene en la defensa de la privacidad estadounidense podremos hablar de que algunos autores (Solove & Hartzog, 2014) la califican de primera autoridad para su protección en Estados Unidos, y además nos aclaran su actuación para mejor acercamiento al concepto y objeto de la Ley en su función protectora de la privacidad.

En cuanto a las relaciones comerciales extranjeras, (de especial importancia en la globalización y sobre todo desde un país exportador y con las empresas que EE.UU. alberga), diremos que esta Sección con sus definiciones, no es de aplicación al caso de "*unfair competition*" en comercio con "naciones extranjeras" (las autoridades cuya definición hemos referido anteriormente) a menos que (número 3 de la letra a) haya un efecto directo, sustancial y razonablemente predecible sobre el comercio estadounidense de esos métodos de competencia comercial.

Es decir, podríamos resumir lo estipulado en que esa actividad comercial afecte a la economía estadounidense con un efecto directo. En esos casos la Ley sí deja abierta la puerta a esa eventual intervención de la FTC también con autoridades extranjeras[124] si el comercio estadounidense se viera sustancialmente afectado.Ya que sí que podría aplicarse la Ley para el caso de daños al negocio de exportación estadounidense de manera directa. Es decir, el de que esa falta o no de observancia a la privacidad pudiera afectar de manera dañosa a la exportación de EE.UU. provocaría la entrada de la FTC como conocedora del asunto.[125]

[123] Recordamos que es a partir del año 1998 cuando la FTC empieza a involucrarse en este sentido regulador de la privacidad con el caso *Geocities*.
La letra a) que conforma la primera parte del precepto establece la fuerza configuradora de su actuación y contenido. No aplicándose en principio al comercio extranjero, a menos que como establece en su punto 4 tengan un efecto directo y sustancial en el comercio interior y exterior estadounidense, caso en el que la FTC entraría igualmente a ejercer su labor de supervisión.

[124] En este caso habrá además que estar muy atento a lo que estipule el próximo acuerdo transatlántico de comercio (TTIP) caso de aprobarse.

[125] Es de señalar que el punto 3 se refiere al comercio con naciones extrajeras, es decir con entidades estatales no estadounidenses. Entendemos que el término debería entenderse en sentido amplio, como el comercio que se pudiera suscitar entre EE.UU. y toda forma de Estado extranjero, como podrían ser en el caso español Comunidades Autónomas o Entidades Locales.

Además es importante señalar que la participación de la FTC lo será en función de con quien se realicen los negocios de exportación estadounidenses. En el caso de que simplemente se trate de "*foreign commerce*" sigue interviniendo la FTC.[126]

Se procede aquí, por tanto, a la distinción entre el negocio internacional público o privado. Y aún si se tratara de negocios con otras "naciones" o entidades estatales, sí que entraría a actuar legitimada la FTC para caso de negocios dañosos para la exportación de EE.UU.

Esto, en un entorno de comercio mundializado, es una distinción muy importante, ya que el negocio internacional es mayoritariamente privado, o en este caso también público estadounidense-privado resto del mundo. Esto copa, como podemos imaginar, prácticamente la distinción a aquella parte en favor de la actuación de la FTC.

Si bien esa arrogancia de competencia del asunto de la FTC puede conllevar también su actuación reparadora hacia "victimas extranjeras" de esas conductas.[127]

Esa restitución en sus derechos a extranjeros significaría también que en caso de que hayan sido víctimas, en esa exportación, de conductas contrarias a la privacidad que lleven a situaciones anticompetitivas y dañosas, particulares y empresas extranjeras (incluidas claro está las europeas) podrían convocar la actuación de la FTC.

3.1.2 Procedimiento de aplicación de la Sección 5.

La segunda parte del precepto se encarga de regular ese procedimiento de declaración de ilegalidad de esas conductas injustas o engañosas; dentro de las que están incluidas las procedentes por infracción o inobservancia de la privacidad de los consumidores.[128]

En el procedimiento se tienen que establecer y demostrar una serie de elementos:

[126] Siguiendo la definitoria establecida en el punto (4) (A) del precepto.
[127] *"(B) All remedies available to the Commission with respect to unfair and deceptive acts or practices shall be available for acts and practices described in this paragraph, including restitution to domestic or foreign victims*."
[128] Se regula a en la letra (b) y siguientes del parágrafo 45 de la Sección 5 de la Ley

- La premisa de un comportamiento engañoso (“unfair or deceptive”) para la competencia, entre los que se incluyen las inobservancias a la privacidad.

- La apreciación por parte de la FTC del interés público para atajar esa situación.

- La iniciación del procedimiento por parte de la FTC implica el envío de la reclamación con los correspondientes cargos y con una fijación de audiencia (día y lugar), que deberá ubicarse en el plazo de 30 días desde la fecha de la reclamación, con el correspondiente derecho de la persona natural o jurídica a ser oído, y negar los términos de la reclamación. De la audiencia debe establecerse testimonio escrito.

- La FTC puede continuar el procedimiento haciendo ya un informe de requerimiento para que la persona cese o desista de su actuación, teniendo la posibilidad la FTC de modificar este informe durante el tiempo previsto para su apelación.

- Tras el transcurso del plazo de apelación o revisión de la reclamación, la FTC puede seguir haciendo modificaciones al informe, o informes complementarios sobre el caso si las circunstancias han cambiado. Ello siempre que la persona natural o jurídica afectada por el procedimiento en 60 días haya obtenido una revisión del caso en la corte de apelación correspondiente, y en el caso de un mandato que haya tenido que ser revisado por la propia FTC.

El tercer punto se encarga ya de la posibilidad y derecho de revisión del procedimiento, así como el proceso a seguir en el mismo. Y se establece la exclusividad de la revisión en la Corte de Apelaciones.

Se establece esa posible entrada en escena de la Corte de Apelaciones en el procedimiento de revisión. Un tribunal de naturaleza judicial y de gran peso político pero de decisión jurídica intermedia. La Corte de Apelaciones tiene la facultad de cambiar, anular, dejar sin efecto, o dar por válida la actuación de la FTC. El pronunciamiento de la Corte suele ser definitivo con la única excepción de la posibilidad de revisión para el caso previsto en la sección 1258 del título 28 del U.S.C., que establece una suerte de certificación de la decisión por el Tribunal Supremo de Estados Unidos.

Se observa la finalización del procedimiento indicando que el mandato o la orden de cesar y desistir de la FTC pone fin al procedimiento, o bien terminado el plazo de

apelación sin su ejercicio por el afectado. Es decir, por transcurso del plazo de revisión; o bien con el archivo de las actuaciones por la FTC, la Corte de Apelación correspondiente o por el Tribunal Supremo, a menos que tuvieran pronunciamientos pendientes.

Seguidamente se asevera la competencia del Tribunal Supremo para dejar sin efecto o modificar un mandato de la FTC, haciéndose eficaz en el plazo de 30 días. Mismo plazo que se establece para que sea firme la decisión de la Corte de Apelaciones correspondiente, que igualmente tiene la facultad de modificar o dejar sin efecto la decisión de la FTC.

Además, se regulan las sanciones por violación de la orden o mandato de la FTC, una vez firme. La multa por cada infracción no será superior a 10.000 dólares, si bien podrán ser acumuladas y demandadas en un proceso civil por el Fiscal General de EE.UU. En caso de reiteración o no atención al mandato de manera reiterada, cada día subsiguiente en que esa actitud persista, puede ser considerado una violación en sí misma y separada. Regulándose asimismo el proceso de acción civil para la reclamación de estas infracciones y sus multas.

Será la FTC la que tenga la iniciativa para pedir esa reposición procedente de un mandato u orden "final" no atendida o violada.

Es, en esta competencia, la jurisdicción de la FTC exclusiva, y su mandato (que se sustancia en forma de "order") de cesación de la actividad antimonopolística o contraria a las buenas prácticas comerciales (también en la quiebra de la privacidad de los consumidores), sería el acto administrativo final y último en este sentido. Con la posibilidad ulterior, según los casos, de revisión jurisdiccional ante el Tribunal Supremo.

Por último, debemos resaltar la capacidad que otorga la Ley a la FTC para obtener medidas cautelares, y su monopolio de puesta en práctica de lo contenido en la Ley, que no está abierta en su legitimación de actuación a particulares.[129]

Es, por tanto, básicamente esta *Section 5,* dentro del paquete anticompetitivo o de competencia desleal junto a la defensa de los consumidores, la que se utiliza por la FTC

[129] Bajo el epígrafe 53. "False advertisements; injunctions and restraining orders"

para poner bajo su paraguas a la privacidad en el comercio, velando por su respeto y luchando contra sus violaciones.

Debemos apuntar, además, que de lo contenido en la Sección 5, la FTC es también el órgano responsable de ejecución para lo contenido en la Ley *Gramm-Leach Bliley Act* (GLBA) y en la *Children´s Online Protection Act* (COPPA) en lo que a estas conductas vienen referidas. Si bien ambas leyes serán objeto de atención más adelante.

3.1.3 Consideraciones sobre la sección 5 de la FTC Act

Podemos observar aquí una regulación más permisiva, en la línea de una mentalidad jurídica muy liberal (en acepción europea) y no regulatoria o no intervencionista; aplicando a las empresas una amplia liberalidad de acción, así como una llamada extensiva y legal a su responsabilidad corporativa. En un tema (el de la protección de datos) en que, además de tratarse regulatoriamente de manera indirecta, como hemos apuntado, se aprecia un tratamiento jurídico apartado del acostumbrado en Europa, donde este derecho (aún manifestándose en actividades de consumo o en cualesquiera otras de la vida), se concibe de manera más integral y como un derecho adherido a la persona.

Esa liberalidad y esa sugerencia legal, (si bien parece que seguida por muchas empresas en sus buenas prácticas), que forman los principios de la *FTC Act* en materia de privacidad, sustrae a esta Ley de la compulsión directa que todo derecho fundamental tutelado requeriría en Europa a la hora de ser tratado y respetado por una norma legal.

3.1.4 Desarrollo reglamentario e institucional en aplicación de la sección 5 de la FTC Act. Las Recomendaciones de la FTC.

El importante desarrollo institucional y reglamentario de la FTC para la defensa de la privacidad se puede percibir, por un lado, en la importancia que sus *orders* han supuesto, y que se reflejan en los asuntos FTC (recopilaremos más adelante los de más

calado), y por otro lado en sus recomendaciones y propuestas de actuación, que sirven de guía para esa defensa de la privacidad a empresas y corporaciones.[130]

Estas últimas son guías, recomendaciones y sugerencias de actuación[131] que la FTC presenta y mantiene actualizadas para las empresas en materia de privacidad. Es una brújula que la FTC aporta y publica para dar un conocimiento de lo que se espera en la actuación de privacidad por parte de las empresas.

Conocido el carácter y poder regulatorio de la FTC, nos parece muy interesante apuntar cuáles son sus indicaciones y orientaciones sobre privacidad, ya que van a mediatizar el comercio y la actividad jurídica en EE.UU. en este sentido. Es por ello que consideramos el estudio de estos documentos de recomendación esenciales para conocer la deriva de la protección de la privacidad en EE.UU. por parte de su elemento institucional más activo. Nos haremos eco del mismo en diferentes partes de este bloque, también en la parte dedicada a la privacidad financiera.[132]

El resultado de este informe (FTC, 2012) se da tras un proceso participativo en el cual, tras ser sometido a proceso de información y participación públicas, los *commenters*, es decir, compañías, empresas, organismos, asociaciones y personas naturales, interesados todos, presentan sus ideas y aportaciones. Es así como se ha ido conformando el propio informe final con asunción de respuestas expresas y consideraciones finales por parte de la FTC.

El informe final de recomendaciones y buenas prácticas para la privacidad (FTC, 2012) que la FTC publica, se basa en una serie de principios de actuación para las empresas y público en general y que pudiéramos ver resumidos en los siguientes[133]:

[130] La página web de la FTC mantiene actualizada información en relación con su actividad en la defensa de la Privacidad. En ella podemos encontrar resúmenes y explicaciones de las principales resoluciones y sus casos para la defensa de la misma. Nos ha resultado muy útil esa información para conocer la casuística y la importancia de la actividad administrativa de la FTC en su vigilancia de la privacidad. Recuperada el 27 de Julio de 2018: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

[131] Las podríamos asimilar en cuanto a su naturaleza jurídica a Recomendaciones europeas en su fuerza jurídica, y dirigidas al sector privado. O a Libros Blancos de actuación.

[132] Hemos estudiado el informe final y consultado su borrador previo: (FTC, 2012) y (FTC, 2010).

[133] "FTC Report Executive Summary" (pag. i)

-“Privacy by Design”: construir la privacidad en cada escalón o etapa del desarrollo del producto. Es decir, una privacidad omnipresente.

-“Simplified Choice for Businesses and Consumers”: dar la capacidad a los consumidores de tomar decisiones sobre sus datos, incluido el *Do Not Track mechanism* o posibilidad de no almacenamiento, además de reducir las cargas y trabas sobre esta capacidad de opción.

-“Greater Transparency”: que el almacenamiento y uso de esa información personal sea más transparente.

Debemos observar, además, que este informe no solo funciona como guía de buenas prácticas para el mundo empresaria,l sino que ofrece, en sus líneas generales, la opinión consultiva que la FTC presenta al Congreso de EE.UU. para que adopte su legislación con ese marco de privacidad de referencia.[134]

Sigue, por tanto, los principios antes apuntados, dentro de las propuestas legislativas a adoptar el documento de propuesta marco, que se muestra preciso y concreto, y principalmente con la iniciativa *Do Not Track*[135], que se perfila en el mismo como una de las más adecuadas.

Es el mecanismo que permite a los consumidores controlar la recopilación y uso de sus datos *online*. Este principio de actuación también ha ido calando, por actuación de la FTC, en los principales buscadores de Internet, que tendrán en sus sucesivas nuevas actualizaciones la posibilidad de que no se monitoricen por las webs esa actividad de búsqueda (entre ellas Mozilla, Apple o Microsoft), dando información cuando se “clickea” sobre las posibles opciones al respecto.

Este mecanismo, ubicado dentro del principio antes referenciado del “Privacy by design” en el informe, debe ser de implementación universal. En segundo término, el mecanismo de elección ha de ser fácil de encontrar, entender y usar. En tercer lugar las

[134] Tal como se informa en su página 3, el departamento de comercio presenta un “white paper” sobre privacidad de los consumidores, animando al Congreso a aprobar una legislación o “Bill of Rights” sobre privacidad siguiendo las recomendaciones basada en los principios de buenas prácticas de la FTC. Ello nos pone en conciencia de la importancia de este órgano y sus consideraciones también en el ámbito consultivo.

[135] “Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011).”

opciones deben ser persistentes (ejemplo de las cookies, con una vez que digas que no debería bastar). Y en cuarto punto el sistema debe ser integral, efectivo y eficaz y quinto no debe ser simplemente un sistema que impida recibir publicidad sino un sistema *opt-out* en toda regla (FTC, 2012, 53).

También ha habido avances en la industria de la publicidad por Internet en este campo, donde las principales compañías y asociaciones de las mismas parecen haber adoptado una intención de puesta en práctica. Entre ellas el propio *World Wide Web Consortium*, que acuerda la creación de un grupo de trabajo para crear el standard universal *Do not track* (FTC, 2012, 4).

Además de esta iniciativa específica (*Do Not Track*), encontramos en el informe ejemplos de otras de tipo más transversal para mejorar la legislación concerniente a la privacidad en EE.UU. Sobre todo teniendo en cuenta el carácter internacional o global de este asunto.[136]

Ello adquiere fuerza y se dota de mayor sentido junto al estudio de algunos de los casos y asuntos más relevantes donde la FTC ha ejercido su autoridad en materia de protección de la privacidad de los usuarios. Recordando la idea de la fuerza efectiva que esta construcción del derecho a la privacidad tiene en la perspectiva estadounidense.

Intercalaremos los asuntos con las recomendaciones marco para ilustrar mejor el trabajo sobre la defensa de la privacidad de la FTC.

3.1.5 Asuntos de la FTC. Principales ejemplos de su actuación y de la aplicación de sus recomendaciones.

Las principales manifestaciones de la FTC, ya sea en forma de órdenes ejecutivas o ya sea en forma de acuerdos con empresas para cumplir esas órdenes, son relativamente recientes. Esta actividad se produce de manera sustancial a partir del siglo XXI.

[136] FTC (2012,5) sobre consideraciones del Congreso en Leyes generales de privacidad que mejoren la transparencia. En este sentido la tramitación parlamentaria de "*Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Congress (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Congress (2011).*"

En 2009 se llegó a un acuerdo en el cual la compañía CVS Caremark aceptaba su responsabilidad en la falta de sensibilidad necesaria en el tratamiento de datos médicos de sus usuarios.[137]

El caso está originado por el abandono de informes con todo tipo de información médica y personal especialmente delicada, en contenedores de fácil acceso público. La reclamación a la FTC se basaba en la sencilla premisa de falta de "razonables y apropiados procedimientos para manejar y gestionar la información personal de sus clientes y empleados". Además se incluía una reclamación de publicidad engañosa sobre la privacidad[138]

La actuación coincide y se anticipa a las principales preocupaciones extraídas del proceso de información pública del informe de la FTC (2012, 7-14) analizado y que fueron: la atención a los daños a la privacidad, el ánimo de un mayor esfuerzo de autorregulación a las empresas y el problema de la interoperabilidad global de cuya importancia la posición gubernamental y administrativa parece tomar conciencia.[139]

El resultado contenido en la orden o mandato de la FTC por violación de las dos Leyes (la FTC Act y la HIPAA en la que es también organismo responsable) en el caso Caremark, fue el de la restauración de la privacidad por parte de la empresa, con la implementación de un adecuado sistema informático al efecto. Además del sometimiento de la empresa a una auditoría independiente bianual durante los siguientes 20 años. En cuanto a la información de la salud además de la multa a la que nos hemos referido la empresa afrontaría un programa de formación específica sobre tratamiento de

[137] Asunto Caremark con número de expediente FTC 072 3119.
CVS Caremark es la cadena de farmacias más importante de EE.UU. y el caso afectó a diez millones de personas. Además el asunto está relacionado, si bien en causas diferentes, con una violación por parte de la empresa de la "Health Insurance Portability and Accountability Act (HIPAA)" (que referiremos más adelante) por la que además tuvo que pagar una multa de 2,25 millones de dólares.

[138] "*CVS/pharmacy wants you to know that nothing is more central to our operations than maintaining the privacy of your health information*." Reclamos publicitarios como el citado hicieron que la FTC actuara en varias de sus vertientes de trabajo de las que giran alrededor de la Privacidad.

[139] (FTC, 2012, 9) Haciéndose eco del resumen de prioridades en el documento de la Casa Blanca que cita (White House, 2012). La declaración de la Casa Blanca es realmente interesante ya que aboga por todo un "Bill of Rights" de Privacidad que sería conveniente aprobar y así lo expresa mostrando su disposición de propuesta legislativa al Congreso en ese sentido.

datos sensibles a nivel general de la compañía, junto con una evaluación del mismo durante tres años por expertos independientes.[140]

Otras veces la actuación de la FTC no es tanto coactiva o sancionadora como de vigilancia y advertencia. En 2010 establece la "*P2P alert*", en la que enviaba cartas de advertencia a casi 100 empresas que venían utilizando la tecnología "*peer to peer (P2P)*" para compartir documentos y que podría suponer un riesgo para la privacidad.

En el mismo año de 2012 se resolvió una reclamación de la FTC contra "Wyndham Hotels" que afectaba a la quiebra de seguridad en las tarjetas de crédito de cientos de miles de personas.[141]

En 2013 podemos fijarnos en un caso con implicaciones médicas delicadas en cuanto al tratamiento de datos. La empresa "CBR Systems", la principal empresa en gestión de donaciones de sangre y tejidos en EE.UU. (negocio privado legal allí), fue señalada por la FTC por mantener una inadecuada protección de los datos de 300.000 de sus usuarios entre los que se encontraban datos sensibles relativos a la salud.[142]

El resultado de la aceptación de estos cargos fue similar a los observados anteriormente: compromiso de establecimiento de un mejor sistema de seguridad y auditoría del mismo por 20 años.

En estas dos actuaciones sustanciadas en los asuntos Wyndham y CBR Systems observamos la coherencia con el objetivo del marco de actuación de privacidad que propone la FTC en su informe, y que estaría dirigido a todas las entidades comerciales que manejen datos que razonablemente puedan vincular o identificar a un individuo.

[140] Este tipo de resultados legales de protección son los habituales en las intervenciones de la FTC. Una suerte de "soft law", que, en general, podríamos resumir en conseguir el reconocimiento de la infracción por la empresa, una asimilación de actuaciones reparatorias, y un compromiso de actuación acorde con la Privacidad para el futuro.

[141] Asunto Wyndham Hotels FTC número 1023142. Esta era la amable publicidad de la compañía "*We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Program* …" Los fallos de seguridad hicieron que una gran cantidad de clientes fueran objeto de un uso fraudulento de su información personal a través de un acceso no autorizado.

[142] Asunto CBR Systems (y American Apparel) número 1423036.

Por lo tanto, diremos que este marco solo afecta y está enfocado a aquellas empresas (o personas jurídicas) que, por su funcionamiento o tamaño, pudieran ocasionar un riesgo potencial para la privacidad de las personas, o en los casos de una información sensible.

La FTC (2012, 15-16) hace la distinción de información que estaría dentro del enfoque del marco y de las que no, con lo que observamos dejación (quizá lógica) para empresas que conserven o almacenen información limitada y no sensible, y que no se comparta con terceros.

La FTC, además, con este marco niega la creación de duplicidades con otros ámbitos de protección de la privacidad, que era otra de las preocupaciones manifestadas en el periodo de información pública. El marco también se aplica a los datos *offline*. Algo que clarifica la FTC. Además, el marco debe aplicarse cuando el tratamiento de datos esté específicamente vinculado a una persona.

Resumiendo, el objetivo del marco de actuación son las entidades comerciales que almacenen o usen datos personales que puedan identificar a un consumidor, ordenador o artilugio electrónico, a menos de que se traten de datos de menos de 5.000 consumidores al año y que no se compartan con terceros.

Ya en 2014 la compañía textil "American Apparel" acepta con la FTC los cargos que consistían en la falsa información de que la compañía venia adherida y obedecía a lo estipulado en el marco del acuerdo de Puerto Seguro entre la UE/ Suiza y EE.UU.

No significa que la compañía violara este Convenio sino que violó la Sección 5 de la FTC Act, al anunciar esa adhesión que implicaría un grado de privacidad mayor propuesto por ese marco internacional cuando realmente no estaba suscrita al mismo. Es decir, publicitaba una apariencia de seguridad de privacidad falsa utilizando un convenio internacional para ello.

Si entramos ya en el estudio de los asuntos acaecidos con las grandes empresas tecnológicas, se abre en 2010 expediente a Twitter[143], que acepta la reclamación de la

[143] Asunto con Twitter FTC No. 0923093. Estamos hablando de un caso en que Twitter entre enero y mayo de 2009 pudo perder el control de sí misma (de la red) en dos ocasiones, en las cuales los" hackers" pudieron enviar tweets a los más de 150.000 seguidores del entonces candidato Obama ofreciendo la posibilidad de ganar 500 dólares en gasolina.

FTC por no proteger adecuadamente la información de sus usuarios y poner en riesgo su privacidad, siendo el primer caso de la FTC contra una red social. La reclamación perfila a Twitter como una red vulnerable a "hackers" ya que se demuestra la obtención por estos de información personal y privada ("tweets" que se predeterminan como no públicos) de los usuarios. Entre ellos se podían encontrar la de los perfiles del candidato a Presidente de los EE.UU. Barack Obama, o el de la cadena de información *Fox News*. Todo ello a pesar de los anuncios de protección de privacidad que la red aseguraba y publicitaba.

Otro caso llamativo en 2010 fue el de la estafa de *LifeLock Inc*,[144] empresa que prometía absoluta protección al robo de información electrónica a cambio de un precio. La FTC entendía que la protección realmente suministrada era inferior a la prometida, llegando a un acuerdo en el que la empresa llegó a pagar 11 millones de dólares, devolviéndose por parte de la FTC a los 957.958 afectados 10,87 dólares a cada uno.

Ya en 2011 Google fue objeto de la atención de la FTC, que declaraba que su nueva red social *Google Buzz*[145] no ofrecía las garantías de privacidad para sus usuarios, contraviniendo la propia política de privacidad de la compañía. La reclamación contempla, al igual que algunas de las ya reseñadas, que Google estableciera un programa de privacidad para los próximos 20 años, auditable de manera independiente. Es de reseñar que, en este caso, además, se propugnaba la quiebra de la privacidad contenida en el acuerdo de Puerto Seguro (Safe Harbour) suscritos entre EE.UU. y la U.E.[146]

A finales de 2011 otra de las grandes tecnológicas, Facebook, accede al acuerdo y acepta la violación de la privacidad en sus prácticas. La aceptación de acuerdo parece tónica general de las compañías en las reclamaciones de la FTC, quizá conscientes de que una obstinación en el proceso, podría acarrearles atender a mayores

---

El acuerdo al que se sometió Twitter implica la implementación de un programa de seguridad bajo asesoramiento de auditor independiente durante 10 años.

[144] Asunto LifeLock Inc número 072 3069

[145] Asunto Google Buzz número 1023136

[146] Acuerdo de Puerto Seguro aprobado por Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

compensaciones económicas, y aceptando así, de manera general, cierto escape permanente de privacidad en las prácticas comerciales en los EEUU.[147]

El asunto *Facebook* es básicamente similar a los vistos: promesas de privacidad que no se cumplen. Sobre todo a partir del cambio unilateral de su política de privacidad operado en diciembre de 2009. No cumplían ni con que las distintas y miles de aplicaciones vinculadas respetaran la privacidad de los usuarios, ni con el respeto al "friends only check" de las informaciones de los usuarios, ni en las verificaciones de seguridad de las aplicaciones, ni en la distribución de información de los usuarios para publicidad. Tampoco en el borrado de videos, fotos, y demás información una vez que el usuario las había eliminado, o se daba de baja de su cuenta, ni tampoco los términos del acuerdo de Puerto Seguro de EE.UU. con la Unión Europea.

A partir de este acuerdo Facebook se obliga a que los usuarios aprueben cualquier cambio en la política de su privacidad y compartición de datos, implicando también lo que afecte a los ya borrados, y la evaluación de su política de privacidad por experto auditor independiente durante 20 años.

En la misma línea de hechos, y en el mismo año 2012 y con resultados similares *MySpace* se vio compelida por la FTC por las mismas razones de privacidad.[148]

La mayor multa impuesta por la FTC por motivos de inobservancia de la privacidad la ha afrontado *Google*[149] en el año 2012: 22,5 millones de dólares, multa relacionada con la utilización de *cookies* por parte de la compañía, en el buscador *Safari* de *Apple*. La información que *Google* obtenía a través de estos mecanismos de colección los enviaba a su empresa *Doubleclick* que vende publicidad personalizada en la web, en función de esos datos.[150]

Vemos así que la vigilancia ha de ser constante, en una labor permanente, porque aún con acuerdos y resoluciones de la FTC previos, muchas de la grandes tecnológicas siguen haciendo un uso indiscriminado y fraudulento de los datos de los usuarios.

[147] Asunto Facebook número 0923184
[148] Asunto MySpace número 1023058
[149] Asunto Google Inc. número 1210120
[150] Esta acción de la FTC además consideraba roto el acuerdo previo con Google de 2011 en el que nos hemos fijado con anterioridad, (Google Buzz)

Prueba de ello y, en otro orden de actuaciones que podríamos denominar de advertencia, la FTC en el año 2014 envía notificaciones a las empresas *Facebook* y *Whatsapp* (a raíz de su adquisición) sobre sus obligaciones y compromisos de privacidad, que avisan del mantenimiento de la vigilancia sobre ellas y recuerda la necesidad de mantenimiento de unas claras políticas de privacidad, en su compromiso y en su vigencia.[151]

Además estos dos asuntos (*Google* y *Facebook*) son puestos como ejemplo en el Informe de la FTC para ilustrar la idea del *Privacy by Design*, que se propone como una de las "líneas maestras" (cursivas mías) de sus recomendaciones: el de que las empresas deben mantener unos procedimientos integrales en la gestión de los datos personales.

Este principio rector de actuación del *Privacy by Design*[152] será el de privacidad en todos los niveles de la empresa. Se trata del concepto de privacidad multinivel. La base del principio es que las compañías deben promover la privacidad a lo largo y ancho de la empresa y en cada etapa de su proceso de producción o de elaboración del producto o de la prestación del servicio.[153]Anima la FTC a una visión amplia y duradera para apoyar este principio regulatorio, sobre todo a la luz de la globalización, con los principios de privacidad y su respeto impregnados en la atención y compromiso de los empleados sobre esta tema. Resumidos en los ejemplos de seguridad en los datos, limitaciones en su recogida y almacenamiento y la exactitud de los mismos.

La FTC (2012, 23), a respuesta de algunos "*commenters*" en el proceso de información pública del informe marco de actuación, arguye además que los principios de privacidad de la OCDE de 1980 ya están incorporados en este marco. Y considera también que el marco tiene aspectos cercanos al "*Right to be forgotten*" (del "derecho a ser olvidado") que también fue comentado en el proceso de información pública y que surgen del mismo.

El documento aporta, como soporte a esta recomendación y a las consideraciones del *Privacy by design*, el caso de estudio de la privacidad en la rápida extensión del

[151] La carta asevera: "*We want to make clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to consumers. Further, if the acquisition is completed and WhatsApp fails to honor these promises, both companies could be in violation of Section 5 of the Federal Trade Commission (FTC) Act and, potentially, the FTC's order against Facebook*,".

[152] Principio acuñado por Ann Cavoukian en 1995 (Comisionada de protección de Datos de Ontario) y principal madre teórica del concepto.

[153] FTC (2012, 22): "*The Commission is encouraged to see broad support for this concept, particularly in light of the increasingly global nature of data transfers*."

mercado y uso de móviles inteligentes. Y los retos a las prácticas de privacidad que para el consumidor conllevan estos aparatos "inteligentes" y sus características. Sobre todo en lo que a geolocalización se refiere.[154]

Por último, hablaremos del asunto mantenido con la empresa *Snapchat*[155], que ofrecía una aplicación para móviles de tratamiento de fotografías recibiéndose mensajes con videos y fotos conocidos como "*snaps*" anunciando la inmediatez como característica de los mismos. Según su publicidad, un Snap desaparecía tras un contador de tiempo a elección de los usuarios (habitualmente 10 segundos). Si bien esto no resultaba cierto y las fotos y videos podían ser recopilados con una aplicación externa y recoger todos esos datos de manera permanente. La "*agreement containing consent order*" que es el nombre que reciben las resoluciones de la FTC cuando hay acuerdo (la grandísima mayoría de los casos), va en la línea de los anteriores: formación obligada en privacidad, asunción de minimización de posibles riesgos futuros (con introducción de programas o aplicaciones al efecto), y por supuesto la reposición de la práctica a criterios de privacidad.

Estos asuntos de la FTC con las grandes tecnológicas se pueden enlazar con otro de los principios rectores de su informe marco de actuación: el de "*Simplified Consumer Choice*". El Principio es sencillo: las empresas deben facilitar la elección en materia de privacidad al cliente, siendo esencial el entendimiento de los consumidores de las posibilidades de privacidad que las compañías ofrecen así como la transparencia de las mismas FTC (2012, 38-42).

Este principio se desarrolla y matiza en las siguientes ideas:

Para las Prácticas que no requieren elección:

1- El concepto "elección" es innecesario en el caso de prácticas comúnmente aceptadas, creyendo la FTC que los beneficios de "elección" al consumidor en estos casos son reducidos.

2- Los datos recopilados por contacto directo con el usuario ("*First party Marketing*") en general no requiere de la necesariedad del principio de elección si bien hay que estar

[154] FTC (2012, 33): "*The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection…*"
[155] Asunto Snapchat número 1323078

atentos a casos en los que pudiera haber amenazas a la Privacidad, como puede ser la posible extensión de esa información a terceros (como otras páginas webs en el caso de comercio electrónico) debiéndose habilitar el principio de elección.[156]

Y la FTC (2012, 42) está de acuerdo con que esa consideración de "*First Party marketing*" dependa no tanto del canal por el que se establezca el contacto, que puede ser múltiple, sino de que sea por la misma empresa ese contacto directo. Por tanto, por ejemplo, la gran cadena de supermercados "*Wal- Mart*" podría recoger esos datos vía telefónica o telemática de manera directa, pero siempre que fuera "*Wal-Mart*", para poder dejar de ofrecer el principio de "elección".[157]

Otro punto de esta segunda propuesta de excepción ("*First party marketing*") nos dice que, en general, las empresas deben dar a los consumidores la posibilidad de elección antes de recopilar datos especialmente sensibles. Sigue aquí la FTC por tanto su posición de flexibilidad razonable con las empresas en una línea de corte liberal aunque garantista.[158]

Conclusión por tanto de estas prácticas es que las empresas no necesitan proporcionar esa posibilidad de elección en todo momento, estando salvadas en las relaciones normales de transacción de la compañía con el cliente o para casos específicamente autorizados por la Ley.

Para los casos en que se requiera elección:

1- Las empresas deberán proporcionarla en adecuados tiempo y forma. Elección que debe ofrecerse en el tiempo y contexto en el que se toma la decisión por el consumidor.

[156] Además las empresas relacionadas ("affiliates") son consideradas terceros por la FTC, a menos que esa relación de subordinación empresarial sea clara para los consumidores.

[157] Podemos decir que la FTC opina que las empresas deben implementar las prácticas que mejoren la transparencia de ese afianzamiento y revalorización en el tratamiento de los datos referidos en este punto 2 (posibilidad de elección, posibilidad de manejo de datos de terceros etcétera) FTC (2012, 44). Aquí la FTC parece dar más peso a razonamientos comerciales que al reforzamiento de la privacidad, llegando en sus consideraciones quizá a unas determinaciones ideales en el mundo de relación empresa-consumidor, para el caso de que sus consideraciones de este marco sean seguidas, algo en lo que el tráfico jurídico habitual nos invita a ser escépticos.

[158] FTC (2012, 47-48) utilizando el ejemplo de Amazon o Netflix de manera ilustrativa: "*…For example, the Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases. Thus, if Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice...*"

(FTC, 2012, 48,51), con la conseguiente preocupación por la FTC sobre un "lo tomas o lo dejas" en situaciones donde el consumidor tiene pocas alternativas.

Aquí vemos como la FTC hace de la concurrencia adecuada de la competencia el factor decisivo para adoptar o no la consideración positiva o negativa de la medida en que se ha dado la posibilidad en un correcto contexto de tiempo y forma, adquiriendo la protección de privacidad, el manto previo de la protección del consumidor y de la leal competencia. Al criticar el "o lo tomas o lo dejas" del momento electivo sobre privacidad, sobre todo cuando hay poca competencia (como es el ejemplo en el que nos ilustra del acceso a banda ancha de Internet), esa posibilidad de opción se puede volver coactiva, pudiendo estresar al consumidor que puede acabar por desdeñar su derecho. Y ello a favor de la compañía que ejerce una posición de dominio tanto desde el punto de vista del acuerdo con el consumidor como a título competitivo (FTC, 2012, 52).

2- Además las empresas deben proporcionar el *Do Not Track Mechanism* (o principio de no dejar rastro) para permitir a los consumidores el control sobre sus datos e informaciones en sus consultas o "navegaciones" por Internet. Y que será una de las principales propuestas de elaboración legislativa.[159]

3- Prácticas que requieren consentimiento expreso. Las empresas deben obtener consentimiento expreso de sus clientes en cualquier cambio retroactivo de sus modelos o políticas de privacidad así como en la obtención de datos sensibles. Apoyándose en su argumentación en los asuntos y acuerdos con Google y Facebook. En cuanto al consentimiento expreso para datos sensibles se hace hincapié sobre todo en la posibilidad de rectificación o borrado. Es decir, en un consentimiento permanente y activo.[160]

Por tanto, este principio de actuación de prácticas que requieren elección puede ser condensado en la importancia que tiene para la FTC de que sea ofrecido en tiempo y forma. El consentimiento expreso del consumidor, además, viene considerándose

[159] Continua el informe con las preocupaciones manifestadas sobre grandes compañías, quizá demasiado grandes para su efectivo control, principalmente en los casos de proveedoras de los servicios de acceso a Internet o grandes tecnológicas que puedan hace acopio masivo de datos FTC (2012, 55).
Los proveedores de Internet IPS (*Internet Provider Services*) y compañías de buscadores o empresas de redes sociales pueden ser "demasiado grandes y vertiginosas" para la protección efectiva de la privacidad. La FTC tiene el ojo puesto en ello. Lo asume como un reto de nuestro tiempo.
[160] FTC (2012, 58-60) y los Asuntos Google y Facebook.

también relevante para la FTC en los cambios que la empresa unilateralmente proponga así como en datos sensibles.

En un tono más amplio el *Simplified Consumer Choice* junto con el *Privacy by Design*, al lado del de *Transparency*, forman los principios rectores del marco de actuación que establece la FTC en su Informe, tal y como hemos observado. El principio de "*Transparency*" se nos presenta en el informe con mayor vinculación a la "*Financial Privacy*", y es por ello que comentaremos en aquel apartado del trabajo algunas de esas recomendaciones de transparencia referidas que ofrece el Informe.

3.1.6 Consideraciones sobre la FTC y la protección de la privacidad del consumidor

Estas consideraciones van a orbitar sobre la fuerza de la FTC en la construcción del derecho de privacidad estadounidense en cuanto a parte del derecho de los consumidores, y explicamos así el por qué de un estudio de un documento FTC sobre recomendaciones como el que acabamos de analizar.

En primer lugar debemos apostar, junto con los profesores Solove & Hartzog (2014) por el carácter de "cuasi Common Law" que supone la actuación de la FTC, y en segundo lugar resaltar las implicaciones internacionales que lleva su trabajo en EE.UU.

Nuestra especial atención a la labor ejecutiva y de creación jurídica de la FTC la creemos justificada por encontrarnos ante el principal organismo gubernamental o jurídico-administrativo de protección de la privacidad, no solo a nivel nacional estadounidense, sino a nivel global. Si observamos, y tal y como hemos analizado, las regulaciones a las que se ven sometidas por la FTC las grandes tecnológicas con sede legal en EE.UU, pero con influencia y acción sobre las personas en todo el mundo, podremos comprender el porqué una determinación de esta Comisión puede ser más fuerte en la práctica que cualquier Ley; o como un precedente de su actuación u orientación de sanción, puede suponer un "aleteo de mariposa" en las políticas de privacidad de compañías como *Google* o *Facebook* a lo largo del planeta.

En este sentido vemos cómo, además, la FTC tiene una omnipresencia administrativa en la defensa de los datos personales del consumidor, ya como entidad propiamente reguladora del consumo, ya también como encomendada en la ejecución de la defensa de la privacidad de los menores de 13 años por la "COPPA" o de parte de la privacidad financiera que estudiaremos más adelante.

Para apoyar y fundamentar esta tesis acerca de la importancia reguladora de la FTC y de la repercusión jurídica de sus actuaciones, nos valdremos del análisis de dos de los mayores conocedores del campo de la privacidad en Estados Unidos. Solove & Hartzog (2014) presentan esa idea en un novedoso artículo que configura a la FTC como una auténtica productora de *Common Law* en lo que a privacidad se refiere en Estados Unidos. El ánimo del artículo en su enfoque y relevancia parece querer revalidar con el originario de Warren y Brandeis, si bien con un recorrido e influencia mucho más modesta, sobre todo, teniendo en cuenta que buena parte del derecho americano a la privacidad tiene su primera fuente original en ese artículo.

Los autores configuran la doctrina de la FTC y sus pronunciamientos como un auténtico *Common Law*, comprensivo y capaz en sí mismo, en materia de privacidad en EE.UU., apartándose un poco de la opinión generalizada de falta de sistematización en esta materia en América.

Entendemos que este cuerpo de decisiones administrativas que son tomadas por la FTC, y especialmente amparadas por la Ley (y en ello nos recuerda en particular a nuestra Agencia Española de Protección de Datos), se podría asimilar por su importancia en un vertebración legal (quizá parcial) de la privacidad en EE.UU.; pero parece también claro que no hay ni un propósito expreso del legislador en ello, ni un objeto jurídico general y concretado en que la FTC se establezca como garante único y común en materia de protección de datos. Porque, de aceptar ello y de ser así, se reduciría la sustancia del derecho de la privacidad, y se trasladaría su concepción de derecho fundamental hacia la percepción de un bien jurídico más estrictamente mercantil (desde el prisma europeo). Más un asunto de consumo que de protección de derechos humanos.

Lo que sí parece cierto es que, a nivel práctico, ninguna autoridad ha hecho más por la protección de los datos personales en Estados Unidos que la FTC y ello, al fin y al cabo,

es una referencia a tener muy en cuenta, con independencia de la mejor aproximación conceptual que podamos entender y que echamos firmemente de menos en el artículo.[161]

Creemos consistente esta posición que configura a la FTC como piedra angular de la privacidad estadounidense por un lado por su propia evolución, en un proceso en el que se ha labrado su abarcadora presencia en la protección de la privacidad con una omnipresencia regulatoria (sobrevenida según Solove & Hartzog (2014, 588)). Lo que parece evidente es que la jurisdicción de la FTC se ha agrandado de manera paulatina hasta llegar a ser considerada esa gran protectora de los datos personales de los consumidores en Estados Unidos.[162] Por otro lado, por su función reguladora producto de esa experiencia y evolución jurídica, siendo una característica de la importancia de la FTC como protectora de la privacidad su carácter de producto histórico en la aplicación del derecho de protección de la privacidad y de los fracasos de otras aproximaciones a ese objetivo. La FTC también es producto por tanto, en esta función omnipresente de las carencias devenidas de las otras aproximaciones que hemos analizado en la defensa de los datos del consumidor (como puede ser la política de agravios de tipo civil, *Tort Law*), que a la hora de regular las quiebras de privacidad no parecían ser lo suficientemente consistentes para afrontar el problema.[163]

---

[161] Solove & Hartzog (2014, 586) hacen un recorrido sobre las visiones de la privacidad en su protección hasta ir llegando a la conclusión de la construcción de un auténtico sistema de *Common Law* por parte de la acción sostenida por la FTC y de la creciente atribución público-regulatoria de la misma. Parece entonces que el propio instrumento FTC supera y trasciende a su finalidad.
Hemos de decir que otros muchos autores, y de los que se hace eco el documento están en contra de esta teoría y son muy críticos, no solo con la tarea homogeneizadora de la FTC y su perfil de actividad en forma de *Common Law*, sino también con su concreta actividad de correcta protección del derecho a la privacidad.

[162] Solove & Hartzog (2014, 588-589) nos ilustran, en contraste con lo que puede haber sido una menor atención académica de la merecida, si lo ponemos en consonancia con la importancia de su actividad. La razón de esa poca influencia universitaria de la FTC está en su atípica actividad de resolución de conflictos que no generan jurisprudencia (cases) sino acuerdos (*settlements, agreements*), y parece que hace de esta materia FTC un menor objeto de estudio. Y ello a pesar de la denominación de *Common Law* que le otorgan los articulistas.

[163] Se pasa también por una primera tendencia a la autorregulación. Todo ello no fue de utilidad para la gran defensa del consumidor ante la gran empresa, tal y como apuntan Solove & Hartzog, (2014, 591-592, 598). Es, a partir de 1995 cuando la FTC empieza su labor en la protección de la privacidad de manera decidida y protagonista. Ya se ha optado por tanto por un sistema regulatorio de intervención y no por la mera autorregulación. Y ello, a través de la fuerza legal de la sección 5 de la FTC Act y que analizamos anteriormente.
Además su actividad se ha visto acrecentada con el paso del tiempo. De las 9 quejas (asuntos) atendidas en el año 2002 hasta las 24 del 2012, se observa su proyección jurídica exponencial. Desde 1997 en total se ha pronunciado sobre unos 197 casos en materia de privacidad. Contando con una División (subestructura administrativa) ("Division of Privacy and Identity Protection DPIP") formada por 46 miembros cuyo número de personal contrasta con el magno cometido que tiene encomendado en

Junto a lo expuesto la evolución se ha manifestado en la característica también del fomento de la autorregulación por parte de la FTC (Solove & Hartzog, 604). No puede calificarse sino de paradójico que un órgano regulatorio y de intervención como la FTC haya consolidado su carácter prevalente en la protección de la Privacidad americana, fomentando el uso de la autorregulación en las empresas. Luego, lo que podría ser una actitud utilitarista de las empresas ha ido encumbrando a la FTC como autoridad reguladora observada como tal por las mismas. Un posible ejemplo de lo mejor de la loable consecución de cooperación (interesada) de la sociedad civil con la entidad supervisora, que encarna los más ideales principios de ese espíritu fundacional estadounidense.

Por tanto sí podríamos considerar, con algunas reservas a la FTC y su labor jurídica como un *Common Law* de la privacidad estadounidense, sobre todo atendiendo a sus acuerdos; verdadero cuerpo en que pudiera manifestar ese *Common Law*. Solove & Hartzog (2014, 606-614) defienden esa posición sin menos dudas, considerándolo una fuerza jurídica de facto con fuerza fáctica equiparable al *Common Law*, defendiendo su argumentación en la gran cantidad de estos acuerdos y la fuerza ejecutiva y de autoridad percibida para las empresas, que los mismos han ido provocando en los últimos 20 años. Hasta establecerse como incontestada autoridad en la materia a los ojos de corporaciones y consumidores ciudadanos. Y en las que casi todas han terminado en su última palabra en forma de orden de acuerdo (y no en la de la revisión de los tribunales).[164] Y ello a pesar de producir un derecho propiamente consensuado (Solove & Hartzog, 2014, 624-628).[165]

---

comparación con otras divisiones de la Comisión. Recordemos que se encarga de la aplicación de varias leyes en materia de privacidad, que se le han ido asignando en su ejecución gradualmente a lo largo del tiempo, así como del acuerdo de Puerto Seguro (y ahora con el Escudo de Privacidad) con la UE (que se propulsó debido a las reticencias europeas sobre la protección de privacidad estadounidense). Con lo que podríamos afirmar que la fuerza de negociación y preocupación de la Unión Europea sobre la protección de datos a nivel internacional y en sus relaciones comerciales con EE.UU. en particular, también fomentaron (como expone el documento) la consolidación de la FTC como Agencia de la privacidad americana "de facto" Solove & Hartzog (2014, 600)

[164] Los autores incluso configuran los acuerdos FTC en función de una serie de aspectos sustantivos comunes con el *Common Law* en cuanto a forma y requisitos de procedimiento que también se alegan como elementos de configuración típico del mismo. Así clasifican los acuerdos en:
Primero: la prohibición de las actividades injustas o arbitrarias; Segundo: el establecimiento de multas pecuniarias; Tercero: la notificación y reparación al consumidor; Cuarto: la eliminación de los datos o la renuencia a utilizarlos;Quinto: el cambio en las políticas de privacidad; Sexto: El establecimiento de

Visto todo lo argumentado, entendemos que quizá sería bueno ir llamando legislativamente a las cosas por su nombre y dar un efecto de autoridad agravado a la FTC con pronunciamientos vinculantes, ya que de hecho es el papel que parece estar desempeñando. Quizá fuera necesaria una actualización del mandato legal de la FTC para adaptarlo a su verdadero cometido actual. La posición no dista de ser polémica en el sentido habitual de los parámetros positivistas del Derecho, pero es claro que pone el foco en una realidad, con independencia de la actitud más o menos formalista que queramos tomar al afrontarla.

Entendemos que no debemos desdeñar esa posición y percepción sobre la FTC como elemento y motor homogeneizador de la regulación de la privacidad estadounidense y también, en lo que ello supone de acercamiento al régimen europeo de protección integral de la misma. Y que, además, llama a superar aproximaciones americanas de protección que han venido resultando ineficientes para una verdadera defensa de la protección de datos en aquel territorio. Posición, sobre todo, que puede acercar más a disipar la niebla que impide contemplar el derecho fundamental que contiene esencialmente la privacidad.

---

programas de protección adecuados para ello; Séptimo: Asesoramiento por profesionales (auditorías etcétera); Octavo: mantenimiento adecuado de Ficheros y la exactitud de los mismos; Noveno Notificación de los cambios materiales que afecten a estos últimos.

[165] Apelando incluso al precedente administrativo (en formas de órdenes de validación de acuerdos por la FTC) en estos casos como elementos de mayor autoridad jurídica al que viniera siendo considerado comúnmente. Dándoles fuerza de facto similar y no menor a las de la jurisprudencia ("case law"). Debiendo ser estudiadas en el mismo sentido. Ello nos pudiera resultar chocante al establecer la costumbre administrativa (precedente) dentro de las características de las fuentes del derecho (propiamente civiles) y alejadas de la configuración kelseniana clásica de las mismas en el derecho público.

Llegando además a seguir configurando a los pronunciamientos y consideraciones y recomendaciones de la FTC como un auténtico *Soft Law* que se tiene muy en consideración en la actuación jurídica de las empresas (quizá esta aseveración nos resulte menos novedosa y esté más cercana al habitual proceder jurídico acostumbrado) recordando un poco al derecho europeo no obligatorio.

Los autores incluso llegan a hablar abiertamente también de la "Juriprudencia de la FTC", fijándose en su estudio de los pronunciamientos de la FTC que son divididos en tres grandes áreas: la del fraude o engaño sobre privacidad; la de la injusticia o arbitrariedad y la de la aplicación de la ley y del acuerdo de Puerto Seguro con la U.E. Fijando además sus elementos clave de configuración en la definición de "*Deception*" (práctica engañosa) y en el de "*Unfairness*" (tomando como referencia la sección 5 de la FTC Act, anteriormente estudiada. Solove & Hartzog (2014, 634-643)

3.2. Leyes federales sobre privacidad del consumidor

Una vez analizada la importante labor reguladora de la FTC (junto con la Sección 5 de la *FTC Act*), y realizadas las consideraciones sobre su importante presencia en la protección de la privacidad del consumidor, pasaremos a hacer un análisis normativo de los diferentes instrumentos legales de protección de esa privacidad en materia de consumo en Estados Unidos.

3.2.1 Regulación legal de la privacidad en el consumo de entretenimiento

Dentro de este apartado vamos a fijar nuestra atención en dos tipos legales: La *Cable Communications Policy Act* de 1984 que regula las amenazas a la privacidad surgidas del negocio de la televisión por cable, y la *Video Privacy Protection Act* de 1988 que lo hace en el ámbito del suministro del alquiler de videos y de sus posteriores formatos.

3.2.1.1 The Cable Communications Policy Act (1984)

Movida al ritmo de los tiempos, como la gran mayoría de las legislaciones, esta Ley[166] es reflejo del auge en los años 80 de la televisión por cable, panacea de último consumo que nos hace recordar al personaje Homer Simpson, besando la conexión de su televisor como vínculo irrenunciable de su felicidad. Ante ese furor, esta parcelación propia de la regulación americana sobre privacidad tenía que aparecer en forma de *Act* sobre los derechos a la misma en sus afortunados usuarios. Hagamos el preceptivo análisis de la misma.

[166] Contenida en el Título 47 del U.S. Code bajo el epígrafe 551 bajo el enunciado "Protection of subscriber privacy".

La letra a) empieza con la habitual definitoria que establece el objeto y sujeto que se regula con esta Ley, estableciendo la necesidad de informar y advertir al usuario o consumidor de este servicio al respecto de su privacidad, y en el momento del acuerdo o contrato de prestación del servicio, siempre con el concepto PII ("*personally identifiable information*") como elemento de protección, y que tratamos en análisis anteriores.

Definiciones más pormenorizadas en relación con el "mundo del cable" se ofrecen en los primeros apartados de la Ley[167], ya que todo se enmarca codificado en el Título 47 del U.S.C. encargado de las Telecomunicaciones, al cual se remite complementariamente la Ley.[168]

La letra (b) con el título "*Collection of personally identifiable information using cable system*", establece la regla general de prohibición que se impone al suministrador del servicio por cable de recolección y almacenamiento de datos sin consentimiento previo de su titular. Y permite pudiera utilizarla solo por razones profesionales de prestación del servicio que presta.

La letra (c) ("Disclosure of personally identifiable information"), siguiendo la línea general del derecho a la privacidad en EE.UU, establece la prohibición de divulgación de la información relativa a los datos de los usuarios del servicio. También el precepto sigue la regla general americana de establecer y clasificar las excepciones a esa prohibición:

- Cuando sea necesario para la prestación del servicio (legítimas actividades propias del negocio que se presta).

- Por decisión judicial que se encuentre justificada en una necesidad de acción gubernamental.

- Cuando se permita la posibilidad de poner a disposición solo nombre y dirección de los usuarios a otros proveedores de cable por las razones tasadas.[169]

- Para Agencia Gubernamental autorizada por Ley.[170]

[167] U.S.C. § 522 "Definitions"

[168] Esta Ley que estamos estudiando se encuentra codificada en el Chapter 5. Subchapter V-A .Part IV del US Code, siendo el primer precepto de esta parte llamada "Miscellaneous Provisions". Lo que nos da una idea del grado de esparcimiento y del diseminado contenido de la privacidad (como de otros grandes temas jurídicos) en la legislación norteamericana, y aún dentro del esfuerzo codificador.

[169] Letra C del punto 2 de esta letra c) de la Ley

La letra (d) con el enunciado “Subscriber access to information”, establece el ya habitual derecho de acceso a los titulares. Y la letra e) el también ya clásico de destrucción de la información que ya no sea necesaria para la prestación del servicio.

También se nos establece la responsabilidad de tipo civil que conlleva la violación de lo establecido así como sus categorizaciones y graduaciones (letra f). Y contempla la típica excepción de seguridad para poder perseguir actividades criminales con previa autorización judicial (letra h).

No debemos confundir este clásico establecimiento legal bajo mandato judicial, con las excepciones de la *U.S. Patriot Act*, que jalonan parte de las Leyes de privacidad estadounidenses, y que son una excepción legal en sí misma; no surgidas de una decisión judicial en el curso de investigaciones criminales supervisadas por un juez (aunque también tengan su origen en la protección de la seguridad).

3.2.1.2 Video Privacy Protection Act (1988)

El inicio de la ley obedece a una construcción jurisprudencial, podríamos decir. Fue aprobada como reacción a lo ocurrido con el nominado a Juez del Tribunal Supremo Mr. Robert Bork, y la aparición en el periódico de información personal suya relativa a sus hábitos en alquileres de videos. Es por ello que a esta Ley también se la conoce como la “Ley Bork”. Es una Ley que está dentro de la esfera de la protección de la privacidad del consumidor y más concretamente de aquella en sus patrones de entretenimiento.[171]

[170] Letra D) del mismo punto y letra anterior. Siendo el tipo de exigencia “mainstream” que la U.S. Patriot Act, como veremos, ha ido estableciendo en muchas de la Leyes de privacidad de los Estados Unidos.

[171] Los archivos personales del historial de alquiler de videos del Juez Bork fueron puestos a la luz por el periódico local “*The Washington City Paper*”, con el objeto de avergonzar a Bork por sus hábitos de entretenimiento. El resultado fue la propuesta legislativa que el Senador Leahy llevó al Congreso.
Con la siguiente principal preocupación que requería legislación: "*an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers....*" (S. Rep. No. 100-599, 100th Cong., 2d Sess. At 6 (1988)).

La Ley ha tenido más utilidad de lo que en principio pudiéramos suponer, ya que ha extendido su protección a subsiguientes formas más modernas de grabación, como apuntábamos, y a los nuevos soportes que fueron apareciendo, como son los DVD y los videojuegos, en su alquiler, si bien no ha habido interpretación judicial confirmatoria en este sentido.

La Ley se encuentra contenida en el título 18 U.S. Code § 2710, bajo el enunciado "*Wrongful disclosure of video tape rental or sale records*".

En cuanto a su contenido la norma empieza (letra a)) con las habituales descripciones definitorias de las leyes de privacidad estadounidense. Como consumidor se presenta el cliente de bienes y servicios de video club o de alquiler de videos. Por "*video tape service provider*" la persona suministradora del servicio de alquiler de video.

La letra b) es la de mayor contenido normativo de la Ley, ya que establece la prohibición de revelar o publicar información que permita identificar a la persona sobre sus alquileres de videos, con la posibilidad de que el consumidor ejercite el derecho de que se retire esa información. Pudiendo el "*video tape service provider*" (en adelante VTSP) dar solo esa información al propio titular, a cualquier persona con el consentimiento escrito del titular, y a una agencia gubernamental en sus tareas válidas de ejecución legal. Se puede suministrar, asimismo, a cualquier persona solo la información del nombre y la dirección, siempre que se permita al titular prohibirlo, y no se identifique el objeto de alquiler. Sería algo así como una lista de clientes o usuarios sin mayor información sobre el alquiler concreto.

Por último se permite el suministro de información a cualquier persona en el curso habitual de los negocios del suministrador (VTSP) o a requerimiento judicial, también previa notificación al usuario y con el derecho de este a ser oído al respecto.

La Ley nos presenta la posibilidad de ejercitar acciones civiles por parte de los agraviados y perjudicados por la inobservancia de lo publicado en esta norma. También prevé la no utilización como prueba de lo que, según esta ley, se encuentre ilegalmente recabado. Se requiere la destrucción de aquello. Y por último, ofrece su carácter no prevalente ante leyes estatales de mayor protección.

Aquí nos encontramos con el concepto jurídico de la "preemption", o de prevalencia jurídica de la Ley Federal o de las estatales en lo que la superen en su mayor garantía y

protección, es un concepto que se repite en muchas de las leyes que tratan la privacidad en EE.UU. Está relacionada con el concepto de armonización a nivel federal en leyes de mínimos de protección.

En este caso la "*Video Privacy Protection Act*" es una de esas leyes de mínimos que se puede ver superada por las prescripciones estatales más garantistas.[172]

Por tanto y ayudándonos en la capacidad de síntesis que ofrece la página de referencia EPIC,[173] podemos resumir la Ley en lo siguiente:

- Una prohibición general de la revelación de información personal sobre alquileres de entretenimiento sin consentimiento concreto y por escrito del consumidor.

- Las revelaciones a la policía solo con autorización judicial.

- Las revelaciones de las "preferencias de género" estarían permitidas para marketing si bien con la opción "opt-out" al consumidor en todo caso.

- Posibilidad de acciones civiles de reparación.

- La obligación del "video club" de destruir los ficheros con esa información personal de alquiler en un año de plazo tras la marcha del consumidor.

- El carácter no preferente de esta Ley federal, siendo ley de mínimos que puede ser superada por leyes estatales de mayor protección.

[172] En este sentido debemos citar algunos ejemplos estatales que aumentan en su protección. Si bien han sido muchos los Estados trascendentes en su legislación, merecen especial mención por su relevante protección las siguientes:
- El contenido en el "*Connecticut General Statute". Section 53-450 – "Confidentiality of videotape rental information. Cause of action. Penalty*".
- El establecido en la parte 27 del Código de Maryland. Parágrafo 583.
- Lo dispuesto en la *Michigan Law*. Parágrafo 445 punto 1712.
En las dos primeras normas la información de alquiler de videos se considera confidencial y no puede ser objeto de venta. En la norma de Michigan (Ley General) vas más allá, protegiendo además el alquiler o préstamo de los libros.

[173] (EPIC, 2015) Recuperada el 28 de julio de 2018:
https://www.epic.org/privacy/vppa/

Como ejemplo jurisprudencial sobre la protección de la privacidad en el ámbito de esta Ley podremos señalar la sentencia *Dirkes v. Borough of Runnemede*.[174]

Dirkes es un empleado público que, en el ámbito de unas pesquisas internas, es investigado, haciéndose valer el investigador de una lista sobre sus alquileres de video sin autorización judicial ni en amparo de ejecución de Ley. Dirkes demanda por ello en base a esta Ley. El Tribunal admitió de manera amplia, que Dirkes pudiera obtener reparación civil no solo del proveedor (videoclub) sino también del Ayuntamiento para el que trabajaba. Habiéndose esgrimido este precedente judicial como argumento jurídico para una interpretación extensiva de los sujetos de la ley.

Otro ejemplo que nos ofrece un pronunciamiento en sentido diferente sería el caso Daniel v. Cantell.[175]

Daniel demanda no solo a los empleados y propietarios de las empresa en la que alquiló esos videos, sino además a los policías y funcionarios de la investigación criminal, basándose precisamente en la sentencia anterior ("Dirkes v. Borough of Runnemede") para implicar a los agentes de la autoridad. En este caso el Tribunal desestima la pretensión, siendo el criterio distinto al de la sentencia anterior. Estableciendo que el objetivo de la Ley y del Congreso era prevenir la revelación de información personal, pero no la prevención automática de toda revelación justificada por otras causas (como era el caso de investigación criminal).

La Ley, que se nos puede antojar hoy algo obsoleta debido a la caída del negocio de alquiler de videos en su concepción clásica, debemos circunstanciarla en la época de su aparición, en la que debemos recordar, era algo de lo más habitual en aquel momento (que llamaremos era pre Internet), esta actividad. Tan común en lo que a entretenimiento doméstico se refería. Y que además permitiría crearse un perfil (erróneo o adecuado) de la personalidad y elementos personales del cliente y del consumidor de entonces.[176]

[174] Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996)

[175] Daniel v. Cantell. 375 F.3d 377 (6th Cir. 2004)
Aquí el demandante es un condenado por el delito de "*sexual molestation*", que es un tipo de abuso sexual a menores. Dentro de sus actos penales se incluían enseñar videos pornográficos a menores. Dentro de la investigación, los policías obtuvieron la información de esos videos.

[176] Tengo edad para recordar las miradas cómicas que mis amigos adolescentes y yo nos intercambiábamos cuando observábamos entrar a alguna persona mayor (o no tanto a mis ojos de hoy)

Además debemos comentar que la Ley, como veremos, está actualizada, a los diferentes formatos que se han ido apareciendo desde su promulgación (DVD, Blue ray's, etcétera) y que además fue objeto de actualización, a partir de la aparición de las redes sociales y de la inclusión de videos en ellas.

En este sentido, es importante la enmienda o modificación a la Ley, ya apuntada, que se produce en 2011 por pura presión lobista de grandes empresas del "entertainment" estadounidense, entre ellas, y sobre todo, por la gran empresa Netflix, hasta el punto de que se le conozca como la enmienda Netflix. Se introduce, a través del congresista Robert Goodlate en su propuesta *H.R. 2471* para permitir o abrir más la posibilidad de puesta a disposición de la información.

Se trata de un adelgazamiento o relajación del consentimiento, ya que anteriormente el dictado de la ley era de mayor estrictez. No permitiendo esa divulgación a cualquier persona con un único consentimiento que ya sirve para todos en adelante, sin necesidad de volverse a autorizar. Ello, tuvo su principal motivación en la relación de *Netflix* con *Facebook* y la puesta a disposición de sucesivos videos que los consumidores hubieran visto. Se da así la posibilidad de automaticidad a esa puesta a disposición con un primer consentimiento únicamente.[177]

Hay, por tanto, una traslación sobre el control, manejo y disposición de la información de los clientes, que va desde el usuario a la empresa, con posibilidad de beneficio para esta última, sobre todo a raíz de la aparición de Facebook. Es por eso que cualquier "like" en videos que le gustan a otras personas, podamos verlos nosotros sin mayor necesidad de consentimiento (pudiéndonos hacer un juicio de erróneo a adecuado, pero al fin no autorizado, de su persona a través de los videos que ve).[178]

---

en aquella ciudad (y sociedad) de provincias en la sección X del videoclub, anticipándonos al juicio hoy extendido por Internet sobre los gustos de cine ajenos y la calificación de las personas por estos hábitos.

[177] Especialmente interesante resulta el artículo de Macgeveran (2013), donde se advierte de la posible desvirtuación de la protección de la privacidad sobre esta falta de autorizaciones ulteriores de uso.

[178] Hemos de advertir que Facebook, así como otras compañías, siempre venden este tipo de puesta a disposición, como una buena labor al consumidor, Un perfil para que podamos sentirnos publicitados de manera personal y diferenciada, pero realmente, el interés está en el gran negocio de metadatos para *tirar la caña en un posible mejor caladero de información* (cursivas mías). La guía de buenas prácticas de Facebook y su marketing nos dicen:

"[*Facebook Ads and Sponsored Stories] offer the benefits of earned at the scale and predictability of paid. That's because they are shown with stories about friends who have already engaged with your business on Facebook. This is the new word of mouth and it's twice as effective at driving awareness. (…) On Facebook, people discover your brand through trusted referrals from their friends. Then drive*

Por tanto, parece que esa asociación automática a través de videos, no hace más que beneficiar al consumidor, según estas "proactivas" palabras de Facebook. Lo que es cierto es que, con esta enmienda legal, el comportamiento y perfil de los usuarios traducido a través de sus videos, puede ser explotado económicamente con un mero primer consentimiento.

Al final lo que observamos es una visión reduccionista, resumida en que lo que resulte de interés para el capitalismo (en este caso para las grandes tecnológicas), es bueno para el interés general, para la sociedad y para todo el mundo (antiguamente el dicho lo encarnaba la General Motors). Pero a quien realmente está beneficiando esa masiva utilización de nuestros datos es a unas cuantas personas determinadas, propietarias de esas grandes empresas.[179]

La Ley ha sido objeto de algunas críticas que nos parecen relevantes tales como la que alude a su enfoque cerrado, estrecho, muy centrado desde su inicio en el formato video, quizá condicionada por su origen del caso Bork. (Solove &Schwartz. 2015, 880)

Por nuestra parte entendemos excesiva la fuerza configuradora de los Lobbies, y de Netflix en particular, que ha condicionado en buena medida la ejecución de la Ley y ha comprometido en cierto sentido la eficacia de su objetivo.

Igualmente criticable es que la Ley se configura en su protección en el mero derecho privado de acción en defensa de la privacidad, pero no prevé ninguna autoridad ejecutiva de aplicación, apoyo o refuerzo (como es la FTC en otras muchas normas de atención a la privacidad del consumidor).

---

preference by interacting with and rewarding your fans (…)
Facebook turns purchasing into a social decision by enabling people to show what they like and have purchased, both online and in the physical world (…) This combination of word of mouth and your ability to deepen engagement with your customers at the point of purchase (either on your website or in store) is incredibly powerful at driving traffic and sales."

[179](Galbraith, 1963) Precisamente algo muy bien resumido y ya advertido por el gran economista con las siguientes palabras "*The modern conservative is engaged in one of man's oldest exercises in moral philosophy; that is, the search for a superior moral justification for selfishness" advertido al Congreso estadounidense (y principal legislador en este tema), en su discurso "Wealth and Poverty*".

Debemos, en contraste, poner también el foco en la general consideración positiva que, para el avance de la privacidad en el terreno audiovisual, supuso la Ley. Como mejor ejemplo de ello citaremos una de sus aplicaciones prácticas sustanciadas judicialmente en el caso *Camfield v. City of Oklahoma*, también conocido como el caso del "tambor de Hojalata".[180]

3.2.2 Regulación legal de la privacidad en el uso y consumo de Internet.

Nos encontramos en este apartado con dos leyes vinculadas al consumo en Internet. Cronológicamente la primera sería la *Computer Fraud and Abuse Act* de 1984 encaminada a la sanción civil y penal en el acceso no autorizado a ordenadores protegidos, y la otra la muy importante *Children's Online Privacy Protection Act* de 1998 (COPPA), que se ocupa de la privacidad de los menores de 13 años en su acceso a Internet.

3.2.2.1 The Computer Fraud and Abuse Act de 1984 (CFAA)

Contenida en el Título 18 del U.S.C., epígrafe 1030, bajo el título "Fraud and related activity in connection with computers", podríamos definirla como una aseveración que conjuga sanciones de tipo penal y civil para los casos de fraude o engaño a través de la informática, principalmente en el acceso no autorizado a ordenadores protegidos.

[180] *Camfield v. City of Oklahoma City, 248 F.3d 1214 (10th Cir. 2001) (the "Tin Drum case").*
En este asunto un ciudadano de Oklahoma presenta una queja en 1997 al considerar que la película alemana y ganadora del óscar a mejor película extranjera "El tambor de Hojalata", contiene pornografía infantil y que atenta contra la leyes del Estado de Oklahoma. La policía presenta la queja al juez competente, que tras un visionado informal de la película, considera que puede haber elementos ilegales de pornografía infantil en ella. La policía, entonces, requisa todas las copias en tiendas y sitios de alquiler de video de aquel barrio, y obtiene, sin una orden, el listado de las personas que en aquel momento tenían alquilada esa película. Entre ellas, se encontraba Mr. Camfield, un empleado de la ACLU, la asociación estadounidense más importante en defensa de las libertades civiles individuales. Camfield presenta una demanda por la violación de sus derechos amparados en la "*Video Privacy Protection Act*", consiguiendo una indemnización del City Council de 2.500 dólares y una pequeña victoria para las libertades civiles para las que trabajaba a diario.

La Ley se nos presenta en sus objetivos algo duplicada con respecto a las demás leyes de protección de la privacidad, ya que intenta abarcar espacios generales de protección a través del resarcimiento civil y el tipo penal, en áreas ya legisladas en el mismo sentido por las leyes sectoriales concretas en su sección de protección de la privacidad. Además, numerosas leyes estatales reproducen idéntica protección en igual sentido (principalmente en aquellas leyes que regulan la privacidad en el ámbito de la seguridad nacional y que estudiaremos más adelante).

La Ley ha sido modificada en los años 1989, 1994,1996 y claro está en 2001 y 2002 por la *U.S. Patriot Act* y en 2008 por la *Identity Theft Enforcement and Restitution Act*.

Debemos considerarla una ley algo obsoleta en el sentido de primera aproximación a la persecución criminal de "hackers" y elementos domésticos que, a través de sus ordenadores, pudieran entrar en la informática gubernamental y comprometer así la seguridad nacional.[181]

El objetivo de la Ley viene aplicado a todas las "*protected computers*", que se identifican en un sentido amplio. No pasa como en otras Leyes que especifican para qué se utiliza el ordenador, o su tamaño. Aquí la Ley protege además a los ordenadores personales, pero establece una útil distinción terminológica muy referenciada en la codificación legal de la privacidad.[182]

Esta Ley establece tipos penales sobre su objeto. Contrasta con otras leyes anteriormente vistas donde el reproche no era de tipo penal sino ubicado en la infracción administrativa.[183]

---

[181] Recordándonos a la película coetánea "Juegos de Guerra" ("War games") de 1983 y que parece alertar a los legisladores sobre estos peligros en pleno pequeño calentamiento de la guerra fría, a través de los peligros en ciernes de la informática, protagonizada en un informático adolescente.

[182] La Ley nos presenta la distinción terminológica que será usada como referencia en otras Leyes que se remiten habitualmente a esta distinción conceptual. Tales como el término "computer" o el de "protected computer" (letra e en sus números 1 y 2)

[183] La CFAA crea siete tipos penales contenidos en su letra a):

El primero se refiere a la entrada en ordenadores del Gobierno, que afecten a la defensa nacional, relaciones exteriores, etcétera (digamos que de altísima seguridad); el segundo tipo es el que se refiere propiamente a la protección al acceso a cualquier "protected computer", así como a las de establecimientos financieros o agencias del Gobierno; el tercero viene refiriéndose ya a la entrada en acceso restringido a esos departamentos gubernamentales de los Estados Unidos. El resto de tipos van añadiendo la específica y gradual voluntad de defraudar, traficar o extorsionar con la información obtenida con esos accesos.

Todas estas ofensas criminales se ven graduadas en un amplio abanico sancionador que va desde el establecimiento de multas, hasta penas de prisión de 20 años (que se van escalando de 5 en 5 años

La Ley ha sido alegada en numerosas ocasiones, entre ellas en la del mediático caso de acceso no autorizado (y revelación posterior) de la sargento Chelsea Manning (*United States v. Manning*, 2010).

Pero quizá los dos casos jurisprudenciales más reseñables en caso de conflicto entre particulares sea el de *Creative Computing v. Getloaded.com LLC* en 2004, y en caso de disputa con los Estados Unidos el de *Unites States v. Drew* del año 2009.

En el primero[184] compañías transportistas tratan de evitar lo que se conoce como "*Dead heading*" que es básicamente volver a hacer el viaje de vuelta sin carga. Es decir, que tratan la evitación de este hecho por razones de eficiencia.

La empresa Creative Computing desarrolló una web (truckstop.com), que casaba las cargas con los camiones, de gran facilidad de uso y permitía a los camioneros conocer donde podrían realizar una "carga de vuelta".

La empresa Getloaded decide competir en ese mercado pero de una manera deshonesta.[185] En su defensa Getloaded arguye que el suelo mínimo de perjuicio que establece la "Computer Fraud and Abuse Act" es de 5.000 dólares para cada acceso no autorizado, y que no había pruebas para que se hubiera alcanzado ese valor de daño en cada uno de los accesos no autorizados. Alegando distintas versiones de la Ley al tiempo de los hechos.[186]

El Tribunal establece una decisión certera aduciendo que no es necesario enredarse en las versiones aplicables de la Ley. El suelo de los 5.000 dólares de daño se aplica al conjunto del daño o pérdida dentro de un periodo de un año, con independencia de las veces que se hubieran producido los accesos no autorizados.

---

desde el año de encarcelamiento). Además se establece la responsabilidad de tipo civil por los daños y perjuicios que se pudieran causar (letras c) y g)).

[184] Creative Computing v. Getloaded.com LLC 386 F.3d (9th Cir. 2004).

[185] Pensando que las compañías transportistas pudieran usar de manera probable el mismo "log in" y nombres de usuario y contraseñas en las dos empresas, tanto el Presidente como el Vicepresidente de la compañía Getloaded usaron esos datos de suscriptores de su compañía para entrar en la competencia, y así, ver y conseguir la información de Creative Computing, como si fueran esos clientes que compartían. Además los empleados de Getloaded "hackearon" el código de Creative Computing para operar en su cuenta.

[186] Según nos analiza la sentencia: "The old version of the statute defined "damage" as "any impairment to the integrity or availability of data, a program, a system, or information" that caused the loss of at least $5,000.It had no separate definition of "loss." The new version defines "damage" the same way, but adds a definition of loss."

El Tribunal echa por tierra la posición de Getloaded sobre la singularidad de los accesos e iterpreta con impecable lógica jurídica la voluntad legislativa racional del Congreso.[187]

En el segundo caso[188], el Tribunal Central de California fue el encargado de ilustrarnos en una pieza de justicia penal, que se puede considerar además, un hito en la interpretación jurídica sobre privacidad en EE.UU.

En ella el Tribunal dilucida si la violación de unos términos de uso de una página de Internet (en este caso *MySpace*) puede o no ser constitutivo de delito según la CFAA.[189] El jurado acaba determinando que se trataba de un acto de menor gravedad que el propio de mayor tipificación de violación de la CFAA.[190]

Pero en lo que a derecho a la privacidad se refiere, resultan más interesantes las consideraciones del Tribunal respecto al incumplimiento de las normas de uso de las páginas web y sus posibles implicaciones penales.

Tras analizar los propios términos de uso de *MySpace* y jurisprudencia previa (principalmente sobre la doctrina de nulidad o anulabilidad por vaguedad de los términos de las leyes penales), llega a la conclusión de que estos tipos de infracciones (los quebrantamientos de las condiciones de uso de las páginas web) no pueden llegar a blandirse como elementos susceptibles de persecución penal. Y tampoco como del tipo de acceso no autorizado o exceso de acceso no autorizado de la CFAA.[191]

---

[187] Pone además el ejemplo ilustrativo de posibles miles de cuentas "hackeadas" y con un valor de daño de solo 4.999 dólares (o millones de 4,99) para evadir la aplicación de la Ley. Se observa así de nuevo la lógica de la condena a la actuación "desleal" en esa gestión de datos:
"…The statute does not say that"impairment" has to result from a single intrusion, or has to be a single corrupted byte. A court construing a statute attributes a rational purpose to Congress. Getloaded's construction would attribute obvious futility to Congress rather than rationality, because a hacker could evade the statute by setting up thousands of $4,999 (or millions of $4.99) intrusions..."

[188] Unites States v. Drew 259 F.R.D. 449 (C.D. Cal. 2009).

[189] Concretamente en su estipulado contenido en el 18 USC parágrafo 1030 (a) y (c), que prohíbe, como hemos visto, el acceso a todo ordenador personal sin autorización o excediendo de la misma.
Los hechos probados presentan al señor Drew de Missouri, que intencionadamente crea una cuenta de MySpace simulando ser un chico ficticio para, a través de ella, infligir un daño emocional a Megan (siglas M.T.M.), compañera de clase de su hija. El ficticio "Josh Evans" se presenta con una fotografía, siendo además imagen perteneciente a un muchacho distinto sin su consentimiento ni conocimiento. Tras entablar "amistad" con "Megan" por la red social y tras un tiempo de contacto, el perfil ficticio le comunica que ya no le gusta y que el mundo sería mejor sin ella. La chica de 13 años poco después aquel mismo día se suicida.

[190] El de más gravedad contenido en el 18 USC parágrafo 1030 (a) (2) (C) y 1030 (c) (2) (B) (ii)). Estando el de menor gravedad establecido en el 18 USC 1030 (c) (2) (A).

[191] Niega el Tribunal así la posible y apabullante ejecución legal de convertir a multitud de usuarios inocentes de Internet en criminales menores, en los múltiples casos de infracción de esas condiciones.

3.2.2.2 Children's Online Privacy Protection Act (1998) (COPPA)

Contenida en el título 15 del U.S.C., en su capítulo 91, bajo el enunciado “Children’s Online Privacy Protection”,[192] la norma es la principal herramienta jurídica de protección de la privacidad de los menores de 13 años en EE.UU. en su navegación por Internet. Entró en vigor en abril del 2000 y podemos calificarla como de las leyes especialmente garantistas dentro del paquete normativo de la privacidad americana. Tiene asimismo a la FTC como principal supervisora de su ejecución.

Las principales motivaciones para la aprobación de esta Ley surgieron a raíz de la preocupación que suscitaban páginas web y sitios online especialmente dirigidos a niños, y que pudieran recopilar y hacer uso de su información personal sin mediación y permiso de los padres.[193]

En marzo de 1998 la FTC presenta un informe al Congreso de EE.UU alertando de la falta de regulación en la materia, y en julio del mismo año los senadores Richard Bryan y John McCain introducen la propuesta 105 S. 2326, titulada "The Children's Online Privacy Protection Act of 1998." El Presidente Clinton la firma el 12 de octubre de 1998, y entra en vigor en fecha 21 de abril de 2000.

El parágrafo 6501 empieza el dictado de la misma y nos establece los elementos definitorios de regulación de la Ley, empezando por el concepto de niño a sus efectos, en aquellas personas por debajo de los 13 años. Y por padre en el sentido amplio de la persona que ejerza la guarda legal.

Es conveniente que nos detengamos en algunas definiciones del precepto, como la que define qué se entiende por Información Personal, que incluye los principales elementos

---

[192] 15 U.S.C. parágrafos 6501-6506.

[193] A partir de los años 90 más de 10 millones de niños americanos irán accediendo a Internet. Chats, páginas para ellos, donde requerían su inscripción, páginas de discusión sobre asuntos de su interés, todo ello es información que se recopilaba, se utilizaba y se vendía. Un reportaje de la CNN de diciembre de 1995 vino a poner el foco de estos peligros, y puso en guardia a la opinión pública. Cuando un reportero de la CBS pudo comprar el listado de nombres de unos cuantos niños usando el nombre de un conocido asesino, las alarmas se dispararon.

de información básica de la persona. Nombre, apellidos, dirección, número de teléfono y sobre todo e importante, su identificación telemática: correo electrónico y la que recaben las páginas web que visiten. O la del consentimiento paterno verificable, que se define no ya en la autorización en sí misma, sino en todo esfuerzo razonable en recabarla, matiz de gran importancia. Así como la de sitio web o servicio online dirigido a niños.[194]

Continúa la Ley con la consideración de prácticas engañosas o ilegales a sus efectos. [195] En general, nos dice su letra a), es ilegal para un operador de Internet o de página web o servicio "on line" de aquellos considerados como dirigidos a niños, el recopilar información personal de los mismos de manera que se violen las prescripciones de la letra b) de este precepto; si bien con especialidad en el tratamiento, como veremos, para los requerimientos de los padres sobre esa información.

La importante letra b) en su punto 1 ya contiene la regulación del derecho propiamente dicho, ordenando a la FTC, (que es también para el contenido de esta ley, la autoridad competente), las reglamentaciones oportunas en cuanto a requerimientos a los operadores que manejen esa información personal del niño. Para que así comuniquen y detallen el contenido de esa recopilación de datos, y el uso de esa información, así como que obtengan consentimiento verificable de los padres para ello. Igualmente establece la necesidad que esas reglamentaciones ordenen a los operadores la obligación de responder a requerimientos de los padres, un adecuado suministro, y la descripción de los tipos de datos específicos del niño que se hayan recabado, junto a las posibles opciones dadas a los niños para rechazar esa recopilación, así como método razonable para hacer llegar esa información a los padres.

También se mandata que esas reglamentaciones de la FTC articulen la prohibición de aquellas conductas y actividades que hagan a los niños suministrar más información de a necesaria para el objeto de su recopilación, y que requieran a los operadores adecuados procedimientos de protección de la confidencialidad, integridad y seguridad de esa información.

---

[194] Contenidos en su números 8, 9 y 10 ("(8) Personal information"(9) Verifiable parental consent"(10) Website or online service directed to children")

[195] § 6502"*Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet*"

Sigue en su punto 2 la letra b) determinando que las reglamentaciones de la FTC deben establecer que el consentimiento paterno verificable no es necesario en determinados supuestos.[196]

Al final del precepto se establece que ninguna ley estatal de tipo comercial podrá contravenir lo dispuesto en estos apartados, dando así una preeminencia indubitada a la federal COPPA.[197]

Además la Ley garantiza sus exigencias en cuanto a las reglamentaciones FTC en su fuerza vinculante, siempre que se sigan los principios de actuación de autorregulación marcados por las industrias del marketing o por la industria "online".[198]Estos principios de autorregulación deben haber sido aprobados por la FTC. Debemos apuntar que esos principios deben ser "sustancialmente similares" a las prescripciones de la COPPA, y no una regulación libertaria empresarial. Esa determinación de similitud corresponderá ser avalada y vigilada por la FTC.

Debemos recordar aquí el Informe marco de actuación de la FTC antes referenciado en su regulación del principio rector de Transparencia para sus actuaciones reglamentarias, y que establecía también su atención en el acceso a los datos de adolescentes (Access to Teen Data); y que fue otro de los temas recurrentes en el proceso de información pública de aquel documento, con gran preocupación sobre el acceso a datos de estos jóvenes especialmente vulnerables.[199]

---

[196] Que serán en casos de información de contactos "on line" aislados que partan del niño sin mayor progresión o para respuestas relacionadas con este tipo de contacto. O la que se obtenga precisamente para dar a los padres información sobre la actividad de sus hijos online, sin que se mantenga ni almacene de manera recuperable. O bien la que se mantenga para proteger la seguridad del niño y la que sea necesaria para proteger la seguridad del sitio web.

[197] *"(d) Inconsistent State law*

No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section."

[198] § 6503 Manifestado en su letra (a) "Guidelines"

[199] La FTC (2012, 70-71), por lo general, alienta la posibilidad en el informe de que se ponga sobre la mesa la posibilidad del "eraser button", es decir, la posibilidad de un botón de borrado que elimine el contenido de lo que se publica online y que sería especialmente recomendable para adolescentes que no se vienen preocupando de sus acciones y publicaciones "online", y de las comparticiones de sus datos y archivos "a largo plazo". Siempre con la particular precaución que la garantía de la Primera Enmienda de la Constitución de EE.UU. (Libertad de Expresión) debe conllevar en estos casos:

"*The Commission generally supports exploration of the idea of an "eraser button," through which people can delete content that they post online …"*

El siguiente precepto (§ 6504 *Actions by States*) nos establece el cometido de los Estados, según la COPPA. La Ley hace partícipe y protagonista a los Estados, a través de sus fiscales generales, para blandir las regulaciones FTC ante supuestas violaciones de las mismas en el territorio de su jurisdicción, y en forma de acción civil. De la que, según su punto 2, deberá dar debida notificación por escrito a la FTC, como es jurídicamente lógico, en una acción de estas características.

Todo ello podrá dar lugar a la intervención de la correspondiente autoridad regulatoria estatal en el asunto, estando legitimada como parte (letra b), a nos ser que la FTC estuviera ya investigando un asunto sobre los mismos sujetos[200], en cuyo caso los Estados y sus autoridades deberán esperar a su sustanciación para poder actuar (letra d).

El desarrollo de la Ley en las regulaciones de la FTC se encuentran contenidas en el Título 16 del código reglamentario americano, (capítulo 1, subcapítulo C, Part 312 "*Children's Online Privacy Protection Rule*"), según la última versión que la FTC ha establecido de sus propias regulaciones tras las modificaciones efectuadas por ella en enero de 2013 y que entraron en vigor en julio de ese mismo año.

Dentro de estas reglamentaciones de ejecución y que contienen elementos jurídicos de importancia, debemos destacar el definitorio clarificador de "*personal information*" como de tipo amplio, incluyendo voz, imagen, audio, geolocalización, nombre de usuario o de una calle cercana, etcétera.

Por citar alguna de las quejas importantes suscitadas al amparo de la Ley y resuelta en el ámbito competencial de la FTC, podemos mencionar el asunto *United States v. Path Inc. 2012 WL 7006381 (N.D. Cal.2012)* donde se establece sanción a la empresa (que gestiona una "app" del tipo "Todo sobre mi", y que atraía a un gran número de niños menores de 13 años) que no cumplía con las estipulaciones de la COPPA.

[200] Es precisamente el siguiente parágrafo 6505 el que establece a la FTC como la autoridad de esta ejecución legal con respeto a las posibles excepciones de autoridades específicas por razón de la materia (principalmente bancarias y de seguros) si el objeto legal jugara en ese sentido.

Por último, y para que sirva de apreciación crítica sobre la Ley, podemos relatar que según las conclusiones del informe de evaluación y seguimiento de la misma que realizó la FTC (2007, 28), se llega a un análisis satisfactorio en la implementación y cumplimiento de sus objetivos, y anima a mantener el trabajo y el nivel de protección adquirido. Es decir, concluye la aprobación de la intervención legal y la línea mantenida y a seguir.

En contraste, debemos apuntar algunas críticas a la Ley por parte de algunos sectores que han señalado que las medidas de regulación de la FTC para comprobar la edad de los niños y su veracidad, así como las autorizaciones paternas (envíos de faxes o documentos firmados, llamadas a números de teléfono gratuitos, o firmas digitales a través de correo electrónico, información adicional de tarjeta de crédito, etcétera) son gravosos y poco ágiles, y que además pueden perturbar la privacidad de los adultos implicados. Recordemos que son medidas de implementación para las empresas (algunas como Amazon han optado por no vender productos a niños para no tener que cumplir con las directrices COPPA).[201]

De igual manera algunas posiciones doctrinales critican la forma en que la COPPA trata de proteger la privacidad de los menores de 13 años, y alegan además el choque que puede producirse con el derecho a la libertad de expresión y opinión que reconoce en general la Primera Enmienda a la Constitución de los Estados Unidos. Tema recurrente a lo largo de la tensión que se mantiene entre la privacidad y los objetivos de las empresas (sobre todo de las grandes tecnológicas) en el manejo de los datos personales.[202]

[201] Lo que nos dice su política de privacidad: "Are Children Allowed to Use Amazon.com? Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian." Recuperado el 29 de julio de 2018: http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496

[202] Nos encontramos numerosos artículos de opinión sobre el tema por parte de Fundaciones o personas jurídicas relacionadas con la actividad de Lobby que hacen mucho hincapié en el asunto.
Un ejemplo de ello lo tenemos en el trabajo realizado por Szoka & Thierer (2009).
Más academica (pero no menos dura) encontramos la crítica como la que realiza Allen (2001) que tilda de "paternalista" y "autoritaria" la norma federal, y en general como un excesivo ejercicio de intervencionismo estatal.

3.2.3 Regulación legal de la privacidad en el marketing.

Veamos ahora la regulación jurídica del Telemarketing y la defensa de la privacidad del consumidor en las leyes federales estadounidenses de referencia.

Las dos principales normas regulatorias de la privacidad dentro del marketing a las que se ve sometido a diario el consumidor estadounidense se establecen en dos Leyes de los años 90: la "*Telephone Consumer Protection Act*" de 1991, y la "*Telemarketing and Consumer Fraud Abuse Prevention Act*", de 1994.

Además, junto a ellas, veremos en este apartado la *CAN-SPAM Act* de 2003 que viene a regular la prohibición de determinados correos no deseados, incluyendo también los que contienen contenido sexual implícito.

La primera se encuentra contenida en el Título 47 del U.S.C., bajo el epígrafe 227 con el título "*Restrictions on use of telephone equipment*". La segunda se ubica en el 15 del U.S.C., en su capítulo 87, que lleva por enunciado "*Telemarketing and consumer fraud and abuse prevention*", y va desde el parágrafo 6101 al 6108. La tercera también se encuentra codificada en el Título 15 (parágrafos 7701 a 7713), así como en el parágrafo 1037 del Título 18 del U.S.C.

Estas Leyes tratan de prevenir las consecuencias negativas que una actividad tan frecuente (como barata) para las empresas como el marketing a distancia o electrónico, pueda ocasionar a los consumidores y usuarios en Estados Unidos.

El concepto general de "Telemarketing" es conocido por todos. Es una propuesta comercial a través de comunicaciones telefónicas o telecomunicaciones. En general, en Europa y en América, es una práctica bastante impopular. Puede ser, y así se suele definir en las normas, o bien entrante (*inbound*) cuando es la actividad del usuario la que lo provoca; o externa o saliente (*outbound*) cuando se trate de comunicaciones realizadas al efecto desde centros de comunicaciones, a veces de manera automática. En general EE.UU. presenta la posibilidad de "opt out" en estas actividades, habiendo, incluso, habilitada para los usuarios una página a nivel nacional para optar por no recibir llamadas (la "Do not call registry web"), dependiente de la FTC. Así como a nivel estatal a través de las diferentes oficinas de los fiscales generales de los Estados.

Debemos apuntar que para la ejecución de las Leyes citadas son competentes distintas autoridades (la FTC para la *Telemarketing and Consumer Fraud Abuse Prevention Act*, de 1994 así como para la *CAN-SPAM Act* de 2003, y la Federal Communications Commission (FCC) para la *Telephone Consumer Protection Act* de 1991).

Pasaremos ahora a analizar las normas de referencia.

3.2.3.1 Telephone Consumer Protection Act (1991)

El contenido de la ley empieza con las definiciones de rigor (letra a)). En ellas se perfilan el sistema automático de llamadas o de marcación, el término relación de negocio, el de máquina fax, o el de petición telefónica referida a las archiconocidas y sufridas llamadas para vender algún producto o servicio. Y continúa la Ley en su carácter y objeto de intervención jurídica sobre las restricciones de la automatización de llamadas de marketing. Es su letra (b) ("*Restrictions on use of automated telephone equipment*") la que presenta el contenido jurídico-normativo esencial de la Ley, imponiendo las limitaciones oportunas a esta actividad comercial, sobre todo en lo que a privacidad se refiere.

Su primer apartado estipula las prohibiciones, siendo ilegal para cualquier persona en EE.UU. o llamando a EE.UU. lo siguiente:

- Hacer cualquier llamada utilizando el artilugio "*automatic telephone dialing system*" (es decir la llamada publicitaria de voz robótica y automatizada) a servicios de emergencia, a huéspedes de hoteles o de hospitales o residencias de ancianos o similares establecimientos, o a cualquier número de teléfono o servicio telefónico en el que se cargue la llamada al receptor.

- Hacer llamadas a ninguna línea telefónica particular sin previo consentimiento de su titular, a excepción de llamadas de emergencia.

- Utilizar máquina de fax u ordenador para mandar publicidad no solicitada a menos que esa publicidad no solicitada venga de una relación de negocio establecida.[203]

Y la última prohibición, la del sistema automatizado de llamada para una práctica múltiple.

Como ejemplo de elaboración jurisprudencial que tiene a esta Ley como principal protagonista podremos citar la decisión judicial de *Destination Ventures, Ltd. v. F.C.C.*[204] En este caso se nos presenta la prohibición de la TCPA del envío de faxes no solicitados que contengan publicidad, sobre los principios de la Primera Enmienda y la libertad de expresión. Siendo la empresa Destination Ventures una mercantil de agencias de viajes que se consideraba agraviada por esta prohibición legal. El Tribunal mantiene la prohibición por el objetivo de la Ley en prevenir el desplazamiento de los costes de la publicidad a los consumidores.[205]

El punto 2 de la letra b) también mandata las posibles reglamentaciones y excepciones, por mediación de la "Federal Communications Commission (FCC)" a la que dota para ser la autoridad en este campo de regulación del que se ocupa la ley. Y le encarga la elaboración e implementación de las recomendaciones y guías a seguir en desarrollo de la misma.[206]

---

[203] O en cuanto al fax, contando igualmente con esa excepción "de negocio" permitiéndolo también. (Véase que aquí sigue primando el interés comercial de las empresas en la ley sobre la mera evitación de perturbación no deseada o solicitada del consumidor).

[204] Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995).

[205] Según literal de la sentencia: "*…Destination does not contest the government's substantial interest in preventing the shifting of advertising costs to consumers. Instead, Destination argues that the FCC failed to sustain its burden of demonstrating a "reasonable fit" between this interest and the ban on fax advertisements. Specifically, it contends that the government has not shown that faxes containing advertising are any more costly to consumers than other unsolicited faxes such as those containing political or "prank" messages. According to Destination, Congress may not single out advertisements for regulation when other types of unsolicited faxes produce the same cost-shifting.*
We disagree. Because Congress's goal was to prevent the shifting of advertising costs, limiting its regulation to faxes containing advertising was justified…"

[206] Se lo encarga con el objetivo de que la FCC desarrolle reglamentos que permitan a las empresas poder evitar recibir llamadas mediante el aparato de "prerecorder" (A) sin consentimiento y el establecimiento de una delegación ejecutiva de categorización de gran importancia (letra B) que se encargará de una labor de intervención determinante :"(B) … may prescribe—
(i)calls that are not made for a commercial purpose; and
(ii)such classes or categories of calls made for commercial purposes as the Commission determines—
(I)will not adversely affect the privacy rights that this section is intended to protect; and
(II)do not include the transmission of any unsolicited advertisement;"

También se podrán realizar excepciones a la norma general por la FCC en llamadas a un teléfono móvil en las condiciones establecidas en sus órdenes o resoluciones, sin que esas excepciones contradigan sus propias reglamentaciones o reglamentos de privacidad en ejecución de la Ley. Y se permite a la FCC, además, "validar" alguna notificación de publicidad no deseada, siempre que se cumplan determinados requisitos (que sea clara y evidente, que establezca la posibilidad de no que no se reciban más en el futuro, y un conjunto de datos donde ejercitar esta posibilidad y el coste gratuito de la misma) (letras C y D).

Es una posibilidad de excepción importante y que traslada una capacidad de decisión a la agencia ejecutiva, que podría dar para el antiguo debate discrecionalidad-arbitrariedad. De contenido similar al anterior es la letra E para los faxes.

La letra G ofrece a la autoridad ejecutiva (FCC) la capacidad de limitar la duración de lo que se entiende por "established business relationship" (relación de negocio establecida), con unos requisitos previos de actuación administrativa, como la comprobación del número de quejas al respecto y sus características, una evaluación de los costes y la comprobación de que no exista sobrecarga injusta de costes para las pequeñas empresas con la decisión que se adopte (letra i minúscula puntos I a IV). Debemos tener en cuenta que esta determinación es importante porque hace operar muchas de las excepciones y salvedades a la norma general limitativa de la Ley.

El punto 3 ya nos ofrece la posibilidad del clásico recurso a solicitar la responsabilidad civil correspondiente (*Private right of action*) por infracción de lo estipulado en esta subsección de la norma (letra b). Es importante esta estipulación legal porque clasifica a la norma en aquellas que dejan a la acción particular la defensa de la privacidad, en contraste con aquellas en las que el papel de la autoridad ejecutiva es más activo e intervencionista, haciendo operar los derechos ciudadanos (como así ocurre con la FTC en la sección 5 de la FTC Act). Deja así, en este caso, a la Federal Communications Commission (FCC) en la mera (y no por ello menos importante) labor reguladora.

En este sentido podemos citar el caso *Gager v. Dell* donde se observa esta actuación individual contemplada en la Ley.[207]

Dell alegaba que la TCPA no preveía ninguna revocación del consentimiento previo (que la ciudadana había manifestado en la petición del crédito), si bien el Tribunal no opinó lo mismo estimando que una falta de plasmación legal expresa no significaba que el derecho a esa revocación no existiera.[208]

La tercera parte de la norma se establece con el título "(*c) Protection of subscriber privacy rights*", que entra en la protección general de los derechos de los usuarios, dando a la Comisión (FCC) el mandato de elaboración normativa de protección en el campo de la Ley y su procedimiento. Un auténtico mandato reglamentario con un plazo cierto de 120 días a contar desde el 20 de diciembre de 1991, que incluye toda una elaboración de políticas de protección para los titulares de las líneas telefónicas en su derecho a no ser perturbados por publicidad indeseada.[209]

---

[207] Gager v. Dell financial services, LLC 727 F.3d 265 (2013)
La señora Gager pidió un crédito para financiar la compra de su ordenador Dell, y metieron su número de móvil en un listado para publicidad, y Dell la llamaba continuamente a través de un sistema automatizado telefónico. A pesar de los esfuerzos (incluso a través de comunicaciones postales) de la consumidora para parar aquella situación, las llamadas automáticas continuaron (a un ritmo de 40 en un intervalo de 3 semanas), ejercitando al final su derecho de acción civil.

[208] *"…Therefore, the TCPA's silence as to revocation should not be seen as limiting a consumer's right to revoke prior express consent. Instead, we view the silence in the statute as evidence that the right to revoke exists (…)*
In sum, we find that the TCPA provides consumers with the right to revoke their prior express consent to be contacted on cellular phones by autodialing systems…"

[209] Esa protección y su proceso deben sustanciarse en 9 meses desde el 20 de diciembre de 1991 y además de una manera eficiente, efectiva y económica, sin carga adicional para los usuarios. Determinándose en el punto 3 las bases de datos de uso permitido. Se prevé la posibilidad de una gran base de datos telefónicos para listar quien se opone a recibir esta publicidad y quién no.
En el caso de que la Comisión decida sobre la necesidad de esas bases de datos la Ley establece los requisitos que deben contener las regulaciones que las ordenen. Las letras A a L de ese punto 3 establecen metodología, organización y criterios de funcionamiento a cumplir por esas regulaciones; que van desde la obligación de especificación del método y persona responsables del tratamiento de la base de datos hasta el establecimiento de prohibiciones específicas.
En cambio, el punto 4 podríamos observarlo como de matización del anterior estableciendo que se deberán tener en cuenta por la Comisión las características concretas mercantiles de los negocios afectados para la configuración y gestión de las bases de datos.
Al igual que anteriormente en esta Ley, el punto 5 establece la capacidad de acción legal individual ("Private right of action") para proteger los postulados de privacidad determinados en esta importante letra c.

La letra d) nos prescribe unos estándares técnicos y procedimientales, estableciendo la Ley además la prohibición legal de establecer comunicaciones que no reúnan esos requisitos técnicos o estándares normativos aprobados en los EE.UU. para estas comunicaciones. Y propugna también la necesidad de revisión periódica de esos procedimientos técnicos y estándares normativos. En este sentido dota de competencia a la Comisión (FCC) para la prescripción de esos estándares técnicos y de procedimiento.

Continúa la Ley en su letra e) con una conveniente prohibición.[210] En general se trata de la de las llamadas o telecomunicaciones no identificadas (ocultas) con fin defraudatorio, previendo o dejando libre la posibilidad de bloqueo por el usuario afectado. Establece y ordena igualmente la necesidad de producción regulatoria por la FCC de lo prescrito, y presenta además el ya habitual "feedback democrático" con el Congreso que se nos ofrece en determinadas partes de las leyes sobre privacidad americana y en este caso más concretamente sobre la necesidad de prohibición de llamadas sin la conveniente identificación.

Ofrece además la Ley una mayor prescripción sancionatoria de la habitual para las infracciones reguladas, y presenta la posibilidad de confiscación civil, (siempre determinada por la Comisión) para los infractores hasta un máximo de 10.000 dólares, pudiendo llegar hasta un millón de máximo en caso de reincidencia y violación continuada. Y establece ya una sanción pecuniaria de tipo penal de igual primer límite.[211]

El punto 7 de la letra e) es de corta redacción pero de importante repercusión, ya que establece un mayor límite al general prescrito en esta Ley que se pueda establecer en otras leyes y su ejecución, siempre que contengan necesidades de investigación, de protección o de actividad de inteligencia del país o de sus entes político-territoriales.[212]

---

[210] "(*e) Prohibition on provision of inaccurate caller identification information*".

[211] Habilita también como actores legales a los Estados en la ejecución legal de esta sección, que se relacionarán para ello con la Comisión (FCC)

[212] Incidiendo en la sacrosanta seguridad. *"(7) Effect on other laws*
This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."
El punto 8 por último nos aclara y define los conceptos clave que se aplican en esta sección legal.

Conviene resaltar la regulación que hace la Ley en su letra f la que abarca la relación territorial legal en este campo ("(*f) Effect on State law*"). Nos encontramos ante una Ley federal "de mínimos", mejorable por los Estados en su protección. Y circunscribe la posibilidad de uso de datos de los contenidos en las bases de datos nacionales a la parte incumbida a los respectivos Estados.

Así la Ley regula y empodera la actividad de los Estados en lo tratado en la Ley, estableciendo la autoridad en el fiscal general de cada Estado, que tendrá además derechos especiales ante la Comisión (FCC) así como capacidad investigatoria propia. En general reciben una legitimación especial.[213]

La última sección legal (letra h) establece informe necesario sobre los "junk fax" al Congreso así como sus requerimientos de contenido por la Comisión (FCC).

En resumen, podremos decir que las prohibiciones y reglamentaciones de la TCPA implican la prohibición del uso del automatismo de llamadas o voces grabadas con el objeto de venta en líneas de llamadas de emergencia, médicas, de habitaciones hospitalarias y hogares de ancianos o teléfonos móviles; así como la prohibición de ese telemarketing de voz pregrabada en general, a menos que se haya obtenido consentimiento previo, y la prohibición de los fax no solicitados ("junk faxes")[214]

El requisito de cumplimiento de la correcta identificación integral de los faxes y su envío también es una exigencia legal, y se reconoce además el derecho de acción individual y su reconocimiento ("*private right of action*").[215]

Destacaremos igualmente la acción necesaria y oportuna que se recomienda a la FCC en el ámbito regulatorio de protección[216]. Si bien uno de sus principales elementos como es la creación de una lista nacional de "No Llamar" no ha sido creada, estando dentro de sus atribuciones, y la acción de aprobación legislativa de mejora de la protección que se ofrece a los Estados como como objetivo interesante de los contenidos en la Ley.

---

[213] tal y como prescribe el primer apartado de la sección: "(*1) Authority of States*
Whenever the attorney general of a State, or an official or agency designated by a State, has reason to believe that any person has engaged or is engaging in a pattern or practice of telephone calls or other transmissions to residents of that State in violation of this section or the regulations prescribed under this section, the State may bring a civil action on behalf of its residents to enjoin such calls, an action to recover for actual monetary loss or receive $500 in damages for each violation, or both such actions."

[214] 47 U.S.C. § 227 (b)(1)(A)(i)-(iii), § 227 (b)(1)(B)) y § 227 (b)(1)(C)

[215] (47 U.S.C. § 227 (d)(1)(B)) y . § 227 (b)(3), (f)(1))

[216] (47 U.S.C. § 227 (c))

3.2.3.2 Telemarketing and Consumer Fraud Abuse Prevention Act (1994)

Contenida en el Título 15 del U.S.C. Capítulo 87, Parágrafos §§ 6101- 6108, el contenido de la Ley comienza con aclaraciones de diferenciación sobre la definición de "telemarketing". Importante es el punto 2 que se hace eco del problema del fraude en este ámbito y que justifica estas especies de exposiciones de motivos que son los preceptos bajo el enunciado "*Findings*" en las leyes estadounidenses. O el punto 3 que además cifra el problema en 40.000 millones de dólares al año de pérdida para los consumidores.[217]

En el siguiente precepto legal (*Telemarketing rules*), se prohíben en general las prácticas abusivas o fraudulentas de "telemarketing", dejando a la FTC (y no a la FCC como en la anterior TCPA estudiada) la elaboración e implementación de reglas para su interdicción y prohibición.

Se ofrece igualmente similar legitimación a los Estados analizada en la anterior norma de prevención contra los abusos del marketing a distancia. Pudiendo actuar a iniciativa de su Fiscal general estatal.[218] Y una similar legitimación de acción civil individual para las personas afectadas.

En el punto 6106 que se encarga de las definiciones presenta especial interés la definitoria de"telemarketing" que se ofrece en contenido amplio.[219]

La ejecución legal y, sobre todo, sus desarrollo, se determina en el siguiente artículo (§6107 "*Enforcement of orders*") y se observa la especial delegación en la autoridad ejecutiva de la FTC para su determinación a través de las reglamentaciones propias que sirvan para la ejecución legal. Podríamos decir que es casi una ley habilitante de

[217] "*Interstate telemarketing fraud has become a problem of such magnitude that the resources of the Federal Trade Commission are not sufficient to ensure adequate consumer protection from such fraud."* No es habitual ver fuera de la exposición de motivos en nuestra tradición jurídica y en el articulado de una Ley estas justificaciones. Llega así a la conclusión de que se tienen que adoptar medidas normativas. Tal y como hace su punto 5

[218] Letra a) del parágrafo 6104.

[219] "(*4)The term "telemarketing" means a plan, program, or campaign which is conducted to induce purchases of goods or services, or a charitable contribution, donation, or gift of money or any other thing of value, by use of one or more telephones and which involves more than one interstate telephone call…*"

delegación ejecutiva. También, incluso para el ejercicio de la iniciativa relativa a la responsabilidad criminal.

Esas normas de desarrollo reflejo de esa labor normativa delegada y que se articularán a través de Reglamentos de la FTC, las podemos encontrar compiladas en la codificación administrativa de la FTC siguiente: "T*elemarketing Sales Rule (TSR), 16 C.F.R. Part 310.*"[220]

En ella podemos observar una serie de restricciones que consiguen así perfeccionar el mandato y objetivo de la Ley. Destacaremos que los agentes de Telemarketing al comienzo de sus llamadas de venta deben proporcionar cierta información al consumidor, como el nombre del vendedor o el propósito de su llamada así como información de compra en el caso de que se produzca. Y deben también informar en caso de actividades de juego por teléfono a través de unas especiales comunicaciones como la probabilidad de ganar y el coste asociado a la participación (debemos tener en cuenta que las apuestas telefónicas es una actividad muy extendida en el mundo anglosajón).

Asimismo las llamadas de venta no podrán realizarse antes de las 8 de la mañana ni después de las 9 de la noche, según la franja horaria en que se encuentre el consumidor. Y los agentes de Telemarketing deben obtener autorización expresa y verificable para determinadas actuaciones (como pudiera ser una transferencia bancaria). Estos agentes deberán mantener además un fichero de datos, incluyendo uno de anuncios o publicidad, otro de ventas y otro de empleados en la actividad.

Debemos tener presente, por último, que estas regulaciones no afectan a determinadas actuaciones de marketing reguladas en su propia normativa como las llamadas de venta entre empresas, o la venta financiera o de seguros, como tampoco la publicidad o negocio propio de ONG´s.

[220] Recuperada en 30 de julio de 2018: https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-310-telemarketing-sales-rule-final-rule-amendments

3.2.3.3 The CAN-SPAM Act

Siendo su nombre completo "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", o en su abreviado "CAN-SPAM Act of 2003", la norma se nos ofrece a regular el problema de los incómodos Spam's o correos no solicitados que vienen "asaltando" con publicidad y reclamos a los consumidores que tengan una cuenta de correo electrónico. Suelen estar fijados en listas de reenvío automático, y además, es frecuente que contengan elementos dañinos para la seguridad de los ordenadores que los reciben en el caso de que sean abiertos, y que permiten detectar si su apertura se ha producido.[221] Además, debemos observar la diversidad de su doble atención regulatoria, prestando asimismo atención a los elementos de publicidad pornográfica que se pudieran enviar por este método de correos electrónicos no solicitados.

Es en diciembre de 2003 cuando el Congreso de Estados Unidos aprueba esta Ley[222]. Como en buena parte de las Leyes de protección del consumidor y su privacidad, aquí también se inviste de autoridad a la Federal Trade Comission (FTC), que además juega un papel especial en los correos de contenido sexual junto con los fiscales generales de los Estados.

Al entrar ya en su contenido el primer parágrafo legal (§ 7701 "*Congressional findings and policy*") es un artículo que nos presenta una serie de consideraciones justificativas realizadas por el Congreso de Estados Unidos para aprobar la ley. Como ya hemos comprobado en otras normas anteriormente estudiadas, se trata de una suerte de exposición de motivos.[223]

[221] Sobre el concepto de Spam son relevantes las explicaciones contenidas en Sorkin (2001) que expresa la problemática de una dotación clara del concepto en el que se entremezclan las consideraciones tecnológicas y jurídicas.

[222] Quedando codificada en el 15 del U.S.C. §§ 7701-7713 así como en el 18 U.S.C. §1037.

[223] "Findings", que a la traducción resulta llamativa, como si hubieran encontrado en la sociedad elementos para actuar jurídicamente en un especie de imaginario del derecho como arqueología social, que se sustancian en los doce puntos que contiene la letra a). Y que podremos resumir en la advertencia del poder legislativo sobre los usos del correo electrónico y sus efectos y repercusiones en la sociedad estadounidense, las amenazas que conlleva, y el problema del SPAM (correo electrónico no solicitado) y del tipo pornográfico en particular. Las consideraciones fijan asimismo su atención en que, a pesar de los esfuerzos legislativos de los Estados, una armonización estandarizada se presume necesaria desde la actuación federal (así como con la colaboración con otros países).

Sobre estas consideraciones de la letra a), el Congreso se decide a actuar plasmándose ello en la letra b) con políticas orientadas a esa protección de la privacidad y dirigidas a establecer la regulación para atajar el problema planteado, reconociendo la conveniencia del derecho a rehusar recibir este tipo de correos al usuario.

El segundo precepto (§7702 "Definitions") es el también habitual artículo que nos ofrece los perfiles definitorios de su objeto y sujeto de regulación.[224]

Merecen una mayor atención algunos conceptos que ayudan a configurar la regulación como tal, como son los de:

- Correo electrónico comercial. Siendo aquel cuyo propósito principal esté relacionado con la publicidad. Distinguiéndolo de los "mensajes transaccionales". Si bien encomienda a la FTC que perfile e interprete esta concepción. Advierte además que el mero hecho de contenerse en el correo electrónico referencias a empresas no pueden hacerlo considerar automáticamente como correo comercial.[225]

- Los términos "*iniciate*" y "*Procure*" tratan de distinguir el origen de los mensajes o a cuenta de quien se produce ese inicio de los mensajes. Otro término de interés y que podríamos traducir como transmisión rutinaria (*Routine conveyance*) habla del proceso de envío automático de correos electrónicos.

- Y se define además en la Ley la distinción entre la persona que envía, el "*sender"* (iniciador) y el "enviador". Separándose además las distintas líneas de negocio en este sentido que pudiera haber como "enviadores" independientes.

[224] La ley presenta unas categorías que definen la actuación de la ley, y van, desde el consentimiento afirmativo, hasta lo que podemos entender por mensaje de correo electrónico, cuenta de correo electrónico, Internet, servicios de acceso a Internet, dominio, o la FTC como la comisión encargada de esta regulación y de la aplicación de esta Ley. Esos conceptos no se plasman de manera inusual y no son interpretativamente problemáticos, no requiriendo mayor detenimiento.

[225] En ese mandato definitorio podemos observar de importancia el documento de regulación de la FTC (2008) y que atiende a esa orden legal. Contenido en la compilación administrativa de la FTC (16 CFR Part 316 "Definitions and Implementation Under the CAN–SPAM Act; Final Rule"). Este documento es producto de un proceso de información pública previo. Recuperado el 21 de agosto de 2015: https://www.ftc.gov/policy/federal-register-notices/definitions-and-implementation-under-can-spam-act-16-cfr-part-316

- Por último, el concepto de "mensaje transaccional" es de importancia en la Ley ya que es la diferencia básica con el SPAM. En los mensajes transaccionales hay un consentimiento previo de negocio. Es la relación telemática fluida y consentida entre el proveedor de servicios y el consumidor. No solo en la relación que dé origen al negocio jurídico, sino todos los mensajes aledaños y necesarios que impliquen esos contratos (envíos de garantías varias, informaciones de seguros asociados suscritos, cambios de las condiciones y en general toda la justificada por la relación comercial). En todo caso esta definición está sujeta a la labor interpretativa y supervisora de la FTC.

La tercera parte de la Ley (§ 7703 "*Prohibition against predatory and abusive commercial e-mail*") entra ya en la prohibiciones, y encarga a la "*United States Sentencing Commission*"[226] el cometido de llevar un seguimiento de los casos sentenciados, así como de las penas establecidas y su cumplimiento (sobre todo en lo que a pornografía y exposición a los menores se refiere); originadas por violación de lo establecido en la "CAN-SPAM Act".

Pero es en la parte separada de la codificación (18 U.S. Code § 1037 "*Fraud and related activity in connection with electronic ma*il") en la que tenemos que pararnos para ver la determinación de la actividad ilícita que prescribe la Ley.[227]

Así proseguimos con el parágrafo 7704 que nos ofrece una serie de protecciones adicionales relacionadas con el mal uso del correo electrónico comercial (jurídicamente hablando). En cuanto a la transmisión de mensajes de correo electrónico comercial (letra a) es ilegal su envío con información falsa o engañosa a ordenadores protegidos (ordenadores como hemos señalado, con funciones gubernamentales en general). Ya sea en su origen, encabezamiento, persona que lo envía etcétera.

Es ilegal también la inclusión de cuentas de correos electrónicos de respuesta con ese mismo ánimo engañoso a esos mismos ordenadores protegidos.

[226] Es un órgano independiente y que forma parte de la rama judicial del Gobierno Federal (siendo una especie de codificador de pronunciamientos judiciales)

[227] Debemos así, antes de continuar el estudio de la parte 15 del U.S.C., analizar la prohibición general de la Ley que fue sustanciada en la codificación en parte distinta; y que pudieramos resumir como el establecimiento de las coacciones legales ante el uso fraudulento del correo electrónico y del "Spam" en general.Concretamente en la letra a) del 1037.

Para el público en general sería igualmente ilegal para el caso de que hubieran manifestado su objeción a recibir este tipo de información comercial[228]

Por último, el punto 5 del mismo artículo abre la posibilidad al envío de esta publicidad a "ordenadores protegidos" en los casos excepcionados. Es decir, en los casos en que los mensajes sean "cristalinos" en todos sus términos (origen, propósito etcétera), y se dé la opción de poder no ser recibidos y que una identificación postal, física y válida del que envía sea presentada. Vemos por tanto una dicotomía de protección evidente entre los ordenadores de función gubernamental (*protected)* y los pertenecientes al público en general, en el tratamiento a la hora de recibir correos no deseados.

Continúa el precepto con la estipulación de un tipo de violaciones agravadas en el uso fraudulento del correo electrónico comercial. En general el envío a ordenador protegido desde cuentas de correo electrónico podríamos decir que "hackeadas", o usando sistemas automáticos de generación de cuentas de correo "posibles" por combinación. Así como la creación automática de cuentas de correo para ello o el envío desde ordenador protegido al que se ha tenido acceso no autorizado.

La Ley ofrece a posibilidad a la FTC de crear regulación supletoria sobre este tema y nos presenta la obligatoriedad de marcar o etiquetar los correos electrónicos que contengan contenido sexualmente explícito con los mismos criterios de separación en la protección anteriormente vistos entre ordenadores protegidos y público en general.[229]

Igualmente se presenta ilegal el envío de información falsa o engañosa con conocimiento y de manera voluntaria teniendo por objeto la promoción de productos o con ánimo de negocio, con afán o expectativa de lucro y sin evitación alguna (§ 7705).

El páragrafo 7706 ya determina la autoridad ejecutiva de la Ley. En general la aplicación de lo dispuesto en esta Ley es cometido de la FTC, siempre que nos encontremos ante una "unfair or deceptive act or practice", respetándose en el artículo la habitual competencia específica de otras agencias y organismos en sus atribuciones específicas (reguladores bancarios, financieros y de seguros principalmente). Respetando también la capacidad de actuación de los Estados a través de sus respectivos

[228] Punto 4 de la letra a)

[229] Prohibición para los primeros, y previo consentimiento para los segundos. Sancionando para la violación intencionada de esa prohibición la prisión de hasta 5 años y/o multa pecuniaria (letras c y d)

fiscales generales para atender posibles casos de responsabilidad civil por este tipo de hechos así como los derechos de los reguladores estatales de actuación, en coordinación con la FTC.[230]

Importante encargo se hace a la FTC en el parágrafo siguiente (§ 7708 "*Do-Not-E-Mail registry*") ordenándole la elaboración de un plan para la creación de un Registro nacional que contenga las limitaciones al envío de correos electrónicos comerciales.

Y seguimos con los efectos y evaluación de la norma, conteniendo el precepto el habitual establecimiento en la legislación estadounidense sobre evaluación de eficacia de la ley y de su puesta en práctica en forma de informe al Congreso; junto con información sobre los procedimientos de infracción por violaciones de la ley que debe realizar la FTC, y el mandato de desarrollo legislativo propiamente a la FTC para continuar los reglamentos sobre la Ley.[231]

Por último, y con intervención de la Federal Communications Commission (FCC), previa consulta a la FTC, se promulgarán normas de protección para las conexiones móviles en el sentido de protección que estipula la Ley.[232]

Como aportaciones críticas a la visión de la Ley citaremos algunos trabajos doctrinales como Lorentz (2011) en la que se proponen reformas de la norma, o Goldman (2006) en el que critica la actual legislación en tanto no se encuentra orientada a la satisfacción del consumidor en sus relaciones con el marketing, que no mejora y habilita la capacidad de estos para manejar esa información de publicidad en su beneficio.

En comparativa crítica con la Unión Europea señalaremos la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), siendo su

[230] Desarrollado ello en su letra *"(f) Enforcement by States*" si bien tendrá preferencia la FTC en caso de una actuación ya iniciada o pendiente por parte de esta y hasta que se vea sustanciada.
La Ley continúa (§7707) diciendo que nada de lo establecido en la misma podrá perjudicar lo establecido en leyes federales de tipo penal, principalmente las encargadas de perseguir la obscenidad o explotación sexual de menores. Estableciendo además en la prevalencia de esta ley federal sobre otras estatales que regulen esos envíos de correos electrónicos comerciales en lo que a fraude se refiere.
[231] Parágrafos 7709, 7710 y 7711
[232] Parágrafo 7712

última versión consolidada de 2009. Que referiremos en la "parte europea" de este trabajo y que refleja *a sensu contrario* en general un sistema de "opt- in" o de consentimiento expreso (al igual que otras legislaciones internacionales como las de Canada, Australia y Nueva Zelanda), y que se presentan en un corte más garantista que el propio de "opt-out" de la SPAM-ACT estadounidense.

Añadiremos además que dentro de la Unión Europea, el país que con mayor celo, ha profundizado de manera más restrictiva en la Directiva ha sido Alemania que ha establecido un sistema de "doble opt-in" o de confirmación posterior del consentimiento expreso.[233]

3.2.3.4 Otras Normas en la regulación del Telemarketing.

Existen otras Normas (Leyes y Reglamentos) de cierta importancia en la protección de la privacidad (si bien no en su principal objetivo) del consumidor en el mundo del Telemarketing que presentan garantías adicionales. Las dejaremos enunciadas aquí:

- The Telephone Disclosure and Dispute Resolution Act del año 1992, (contenida en el 15 U.S.C. Chapter 83 bajo el título "Telephone disclosure and dispute resolution") que puso en práctica la norma del número 900, para identificar y proteger la actividad de los consumidores en sus relaciones telefónicas con muchas empresas así como la mayor transparencia en el pago de esas llamadas.

-The Mail and Telephone Order Rule. Dentro de las actuaciones de reglamentación de la FTC y contenida y compilada en el 16 CFR Part 435.

[233] Contenida en el artículo 7 de la Ley alemana para la lucha contra la publicidad telefónica desleal y para la mejora de la protección de los consumidores ante determinadas formas de venta (Gesetz zur Bekämpfung unlauterer Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen)

3.3. La privacidad financiera en Estados Unidos

Premisa

Dentro de este bloque de protección de la privacidad en Estados Unidos analizaremos las normas que regulan, de manera más determinante, la misma en el ámbito bancario y financiero. Asimismo deberemos hacer una distinción básica entre las dos leyes (Statutes) que regulan la privacidad financiera con una carácter más general, y aquellas que lo hacen de manera vinculada a la interacción del Estado o del Gobierno, de los poderes públicos, conceptuadas más como una defensa ante los mismos, que como elementos de intervención normativa directa ante riesgos del propio mercado financiero.

Entre las primeras leyes estudiaremos la *Fair Credit Reporting Act* y la *Financial Modernization Act*, ("*Gramm-Leach-Bliley Act*"). Entre las segundas centraremos nuestra atención en la "*Right to Financial Privacy Act*" así como en la "*Identity Theft Assumption and Deterrence Act*". Compartimos por tanto, así, en esta parte del capítulo determinaciones de enfoque de las dos primeras partes del mismo, y del anterior donde estudiábamos el acceso a los registros públicos, e incidimos en esa diferenciación, ficticia pero práctica, de la actividad de protección del individuo estadounidense en su vertiente de consumidor (en este caso financiero) y de ciudadano en sus relaciones con las entidades de sector público. Es decir un ojo puesto en la protección de la privacidad financiera del consumidor y otro focalizado en la privacidad financiera ante la posible intromisión estatal.

3.3.1 Fair Credit Reporting Act.

A partir de los años 80 la financiación de los gastos domésticos (sobre todo vivienda y vehículos) se encuentra basada más en la obtención de crédito que en el mero ahorro personal; dándose esto sobre todo con particular incidencia en Estados Unidos. Este es el marco social en el que se aprueba esta Ley de regulación financiera.

La norma está dentro de las leyes que se encargan de la privacidad financiera. Y forma parte del "paquete" de defensa de la protección de datos en el ámbito financiero en EE.UU.

Dentro del entramado diseminado de normas sobre privacidad, debemos decir que, ni siquiera dentro de un mismo ámbito sectorial, como es el financiero, encontramos una regulación común y unitaria.

En este caso, la Ley se encarga de la privacidad para el tratamiento de la información personal ubicada y tratada por las "*Credit Reporting Agencies (CRA's)*" que, según definición del propio Gobierno americano, y ante la confusión habitual de que se trataran de agencias gubernamentales, las titula como empresas de servicios que aglutinan la información sobre la manera en que la gente maneja el crédito con objeto de hacer negocio con esa información. Siendo las mayores de estas empresas Equifax, Experian y Transunion.[234]

Un pronunciamiento jurisprudencial importante en torno al concepto de CRA's se da en la sentencia Spokeo.[235]

Spokeo es una empresa que reunía información de consumidores de una multiplicidad de fuentes, compilándola en perfiles personales coherentes que, además, destacaban en clasificaciones por hobbies, etnias, religiones o participación en redes sociales. Esos perfiles se vendían por Spokeo a través de suscripciones. En 2010 Spokeo cambia los términos de uso de su web, sin ser consciente de que actuaba (y su negocio era conceptuado) como "Consumer Reporting Agency" (CRA), obviando las exigencias que la FCRA establece al respecto. Es condenada por ello a una multa de 800.000 dólares y a una serie de obligaciones de adaptación a los dictados de la Ley. Con la mera defensa de la empresa de argumentar que ella no sabía que era una CRA, en un caso muy costoso de "ignoratio legis".

---

[234] En las preguntas frecuentes de la página web del Gobierno estadounidense nos informan de la siguiente manera: "A credit reporting agency (CRA) is a company that collects information about where you live and work, how you pay your bills, whether or not you have been sued, arrested, or filed for bankruptcy. All of this information is combined together in a credit report. A CRA will then sell your credit report to creditors, employers, insurers, and others. These companies will use these reports to make decisions about extending credit, jobs, and insurance policies to you." (Recuperado el 20 de septiembre de 2018): https://www.usa.gov/credit-reports
Su negocio, podríamos decir por tanto, es la información financiera en materia crediticia de los consumidores.

[235] *United States v. Spokeo, Inc. No CV12-05001 MMM (JHx) (C.D. Cal.2012)*

El texto de la Ley que data de 1970, y que ha sufrido numerosas modificaciones, es de una larga redacción, que hace coincidir sus estipulaciones con una clasificación casi coincidente con las letras del abecedario, haciendo así, una de las secciones (o articulados) más extensos del código americano.[236]

La principal motivación por tanto de la Ley es el establecimiento de la fiabilidad, veracidad y protección de la privacidad de esos informes emitidos por las "CRA's", y que de tanta importancia social y económica se venían revelando. En el texto legal estas Agencias pueden venir referidas igualmente como *credit bureaus* o *consumer reporting agencies*.[237]

Como órgano de ejecución legal tendremos que apuntar al organismo al que se suelen dirigir todas las miradas: la FTC. Si bien, y una vez creada por la Ley Dodd-Frank en 2010, la *Consumer Financial Protection Bureau* (CFPB) es ensalzada en esta tarea y sobre todo en esta Ley, por encima de la FTC. En este sentido, es importante el "memorandum of understanding" que los dos organismos firmaron en el año 2012.[238]

Nos encontramos así, ante la primera ley federal que regula en EE.UU. el tratamiento de datos personales en el negocio privado. Concretamente en el ámbito de las Finanzas.[239]

La Ley que entra en vigor el 25 de abril de 1971, sufrió una fuerte modificación en 1996 a través de la *Consumer Credit Reporting Reform Act* y en 2003 con la *Fair and Accurate Credit Transactions Act.*[240]

---

[236] Contenido en el 15 del U.S.§ 1681 et seq (1681-1681u)

[237] Una lista comprensiva de estas Agencias que operan en el territorio estadounidense la podemos encontrar en el siguiente enlace y documento de la página web de la CFPB (Consumer Financial Protection Bureau) (recuperado el 20 de septiembre de 2018):
http://files.consumerfinance.gov/f/201501_cfpb_list-consumer-reporting-agencies.pdf

[238] Recuperado el 30 de julio 2018:
http://files.consumerfinance.gov/f/2012/01/FTC.MOUwSig.1.20.pdf

[239] Como antecedentes de esta Ley diremos que este negocio tiene su primera gran compañía (agencia) dedicada a este menester en la "*Retail Credit Co*" en 1899. Estas compañías, (en cierta medida asimilables a las empresas de detección de morosos), entraron en la agenda pública a partir de 1960, cuando se empezó a crear controversia a su alrededor, debido a que algunas oportunidades de empleo, de negocio y de servicios se veían afectadas (o directamente denegadas) por los informes que emitían; resultando además los afectados sin posibilidad de acceder a sus propios informes, que, además, incluían de manera habitual datos concernientes a todo tipo de hábitos diarios y "estilos de vida" dimanantes de sus procesos de solicitud de crédito, con toda la indefensión que aquello suponía.

[240] En este sentido la página de la FTC desde un punto de vista institucional y de la EPIC, desde la percepción del tercer sector social, nos ayudan al estudio de la Ley y sus antecedentes. Recuperados el

3.3.1.1 Análisis de la Ley

La Ley en su primer precepto (§ 1681) nos habla de su necesidad, de su propósito y objeto. En la letra a) el Congreso llega a la conclusión del importante papel de la Agencias de Crédito (CRA's) en la vida de los consumidores. Más concretamente, para el tema que nos ocupa, su punto 4, cual es el de asegurar la imparcialidad y el respeto a la privacidad en los mismos. La alusión y determinación a los "recursos razonables" de la letra b) establece la necesidad de su equilibrio con la privacidad.

El subapartado a) entra ya en las definiciones. Particular interés revisten las definiciones de los informes, que, como comprobamos, son definidos en sentido amplio.[241]

También es de interés el término de informe de investigación sobre el consumidor. Es una categoría importante la de estos *investigative consumer reports, (ICR's)* ya que pueden incluir información sobre características personales y modos de vida así como reputación. Si bien como hemos visto, estos informes reciben mayor protección de privacidad por la Ley. La garantía de solvencia ("*Credit Score*") es clasificada en base a estos informes. Es decir, un informe agravado o especial. El término "*adverse action*" también es tratado profusamente, y se podría resumir en cualquier acción desventajosa motivada por el informe.

La letra o) relata las comunicaciones excluidas del tratamiento legal, que de manera directa o indirecta, implican un cierto consentimiento o se muevan en resultados

---

30 de julio de 2018:
https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act
https://epic.org/privacy/fcra/

[241] 1681 a) *"d) Consumer Report*
(1) In general. The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing,credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for
(A) credit or insurance to be used primarily for personal, family, orhousehold purposes;
(B) employment purposes; or
(C) any other purpose authorized under section 604 [§ 1681b]".

permitidos por las leyes. La letra q) entra a tratar el objeto legal definitorio para casos de fraude.

En cuanto al contenido de los informes se trataría fundamentalmente de información sobre responsabilidad o fiabilidad financiera de la persona de que se trate, incluyendo los balances de las tarjetas de crédito o información hipotecaria. Ese contenido es utilizado generalmente (y de ahí la susceptibilidad de lucro de esos informes) para evaluar la idoneidad de la asignación de créditos, la suscripción de seguros, el acceso a empleos, arrendamientos, el sostenimiento de los hijos, la capacidad de suscripción de seguros profesionales y por tanto de sus licencias, así como para cualquiera que el consumidor autorice.[242]

Descriptivamente los informes podrían dar información de identificación básica, como nombre y apellidos, dirección, número de seguridad social, estado civil, número de hijos, etcétera, así como información financiera, que puede contener los ingresos, el trabajo que se desempeña, números de cuenta, valor de las propiedades inmuebles o del coche o coches.

Igualmente se contempla la información que tenga carácter público por ley (como fianzas ejecutadas, impagos a bancos, situaciones de bancarrota), y las líneas de crédito (estados de las cuentas, que incluyen los datos de uso de las mismas); al igual que reclamaciones sobre pagos o mandamientos de no pagar determinados movimientos.

Asimismo entran temas afectantes a la capacidad financiera como el historial o vida laboral, así como el empleo actual y los requerimientos que se hagan de estos informes y su número, que revela evidentemente una información financiera. Así como la identidad de las personas que los solicitan. De igual manera se incluyen información de Salud e información interpretativa en los informes por parte de las entidades que los emiten.[243]

[242] Sobre el contenido de los informes y los objetivos de los mismos es muy interesante la información contenida en Hendricks (2004)

[243] Si bien hay información que se excluye por definición del informe de crédito. Esa exclusión vendría formada por la información de hábitos de consumo de bienes y servicios por el consumidor con su tarjeta de crédito. Además de añadir la opción "opt-out" a los clientes que no quieran verse contemplados en el informe. Habilitando además, tras la modificación ejecutada por la enmienda de la Ley del año 2003, la opción "opt-out" al consumidor en términos de marketing (temporalmente a 5 años ampliables por 5 más). También este cambio legal restringió mucho los datos a suministrar en los informes en cuanto a la información médica. Debe constar autorización expresa y por escrito y

Los informes, por tanto, están limitados en su uso a los propósitos establecidos en la Ley (FCRA). Las razones de uso que deberán esgrimirse son las solicitudes relacionadas con créditos o seguros o en materia de Empleo y su ámbito, que requiere consentimiento si implican decisiones de contratación laboral. También los mandatos judiciales y las necesidades propias del funcionamiento normal de las prestaciones de servicios empresariales, iniciados o buscados por el consumidor. De igual manera que los servicios profesionales, que incluirían las solicitudes bancarias para saber periódicamente los clientes que son interesantes mantener.

Los pagos de sostenimiento familiar y de hijos a cargo también son razones válidas así como todos aquellos accesos establecidos por las leyes.

Debemos resaltar que los usos con objetivo de publicidad y marketing no están permitidos ni incluidos en los usos de los informes de crédito.

Como ejemplo jurisprudencial de ello tenemos la sentencia preliminar que acabó por persuadir a Citigroup a aceptar un acuerdo e indemnización millonaria, ya que venía precedida de una actuación de la FTC con la que la gran corporación financiera no vino a estar de acuerdo. En ella se aducía por el órgano estatal que la compañía utilizaba los informes de crédito con propósitos de marketing.[244]

En cuanto a la notificación de estos informes se debe suministrar al titular de los datos si del mismo se pudieran inferir consecuencias crediticias negativas.[245]

Así la letra b) del parágrafo 1681 se remite a los propósitos legalmente válidos de los informes, que, con ánimo de síntesis, establece a aquellos a los que podríamos definir como con un interés legítimo (empleadores, acreedores, prestatarios etcétera).

Evidentemente, al igual que en otras estipulaciones, en materia de menores, o de necesidad de aplicación o ejecución de la ley por los órganos responsables (Agencias gubernamentales), los objetivos se encuentran igualmente matizados y previstos como

descriptiva de su uso (el del informe).

[244] FTC v. Citigroup Inc., et al, No. 1:01-CV-606-JTC (N.D. Ga. 2001).

[245] La "*Fair and Accurate Credit Transactions Act*" del año 2003, que modifica la FCRA, introdujo esta obligación en los casos que se pudiera ponderar en base a la media en términos de crédito, expresándolo así: "*materially less favorable than the most favorable terms available to a substantial proportion of consumers*."

legítimos. Se establece además, de manera separada, el tratamiento de los objetivos con motivación laboral y de empleo, siguiendo unos cauces de especial respeto procedimental, donde se trasluce el objetivo de no discriminación laboral, y requiriendo en general, un consentimiento expreso o tácito para esos usos de tipo laboral.

Una sentencia que entra a interpretar determinados preceptos de la Ley y concretamente esta letra b) es el caso *Smith* de 2003.[246]

Viene motivada por un préstamo para la compra de un coche y el acceso a determinados datos para comprobar la fiabilidad del prestatario. Debido a que se utiliza un previo acceso permitido para la compra de otro artículo de una marca perteneciente a la misma empresa (General Electric y General Motors) se accede esta vez de nuevo sin permiso renovado, y defendiéndolo la empresa en base a los usos permitidos del 1681b). Llega al final el Tribunal a la conclusión de que esos usos permitidos han sido sobrepasados, siendo así este caso, ejemplo importante de la aplicación doméstica y diaria del alcance de la Ley.

A partir del 11 de septiembre de 2001 podemos apuntar que muchos empleadores utilizan estos informes para conocer mejor los perfiles de sus empleados y de los aspirantes a serlo. También por tanto, debemos resaltar que en relación con los datos de antecedentes penales estos informes se topan con una maraña legal discordante entre las legislaciones estatales, ya que en algunos Estados se permite comprobación a efectos de empleo (siempre que la sentencia sea firme, y no solo un arresto), otros lo permiten en función de circunstancias muy determinadas.[247]

Las regulaciones del organismo competente en esta materia en EE.UU., el *Equal Employment Opportunity Commission (EEOC)*, advierten contra el mero hecho si no está directamente relacionado con el trabajo a desempeñar. En la misma linea se manifiesta la *Fair and Accurate Credit Transactions Act* del 2003, en su modificación de la FCRA, excluyendo categorías adicionales de investigación de los informes de crédito a efectos de empleo. Prohibe además, como hemos visto, la utilización de esos

[246] Smith v. Bob Smith Chevrolet, Inc. 275 F. Supp. 2d 808 (W.D.Ky.2003).
[247] Tal y como apunta la página de la EPIC. Ver nota 240.

informes por razones de empleo, si contuvieran datos médicos sin expresa autorización.[248]

A todo esto, y será un patrón que se repite como excepción legal, tenemos que añadir la aducida y motivada por razones de seguridad nacional, que establece la posibilidad ya apuntada de "opt- out" por el consumidor.[249]

Al igual que en los propósitos laborales, se establece una regulación diferenciada de los informes con contenido de datos médicos. Si bien aquí el carácter de protección es más implícito que el de simplemente cierta especialidad en lo referido a lo laboral. Aquí se habla ya de limitaciones.[250]

Es llamativa la falta de distinción en función de los datos (especialmente protegidos) de manera algo más débil que en la perspectiva jurídica europea.

El apartado c del largo precepto 1681 que analizamos establece en su letra a) la información que debe quedar excluida en los informes, y que queda regulada principalmente en una antigüedad de exclusión de 10 años para casos de fraude bancario y de 7 años para tipos generales de infracciones. Esta prescripción para la contemplación de hechos adversos, queda, sin embargo, exceptuada por lo que podríamos denominar "la fuerza del montante dinerario" del negocio de que se trate; viniendo a considerarse en mayores de 150.000 dólares para créditos y seguros de vida y 75.000 para salario anual del posible empleado. Se prima aquí la supuesta seguridad del negocio a la protección de la privacidad por hechos cometidos en el tiempo. Podría plantearse la tensión jurídica entre el principio reinsertivo y su necesidad social, así como la privacidad del individuo, frente a la fuerza (que aquí resulta ganadora) del "Business" como primer bien protegido, (o si se quiere, aquí también hay un protección explicita del capital frente al derecho individual).

También se nos habla de las alertas de fraude que deben estar presentes en las actuaciones de las agencias a la luz de la temática de la regulación.

[248] En este sentido advierte la EEOC a los empleadores en su página web. Recuperada el 30 de julio de 2018: https://www.eeoc.gov/eeoc/publications/background_checks_employers.cfm
[249] En su parte e) (subdivisión dentro de letra b) ("Election of consumer to be excluded from lists")
[250] Parte g) (también subdivisión)

Se dan aquí especiales prerrogativas de acceso a los expedientes por parte de los consumidores, vistos los posibles abusos a los que pueden verse expuestos con el robo de identidad. Se les ofrece así también una protección especial para las alertas prolongadas en el tiempo, dándoseles en ambos casos facilidades procedimentales y limitaciones en el uso de su información.

Es de destacar que debe darse un peligro cierto de delito contra la privacidad para que se dé una protección agravada; que entendemos debería reflejarse para el tipo de protección normal o estándar.[251]

La Ley establece previsiones al respecto del robo de identidad, en lo referido a los "credit reports", que, al igual que el robo de una tarjeta, pueden utilizarse para conseguir crédito de manera fraudulenta. Permite el bloqueo de los informes de las agencias para estos casos e incluye la gestión de "alertas de fraude" en el contenido legal. Alertas que tendrán un sentido integral y la que emita una Agencia podrá valer para las demás "CRA's", a las que se deberá notificar. La reforma de la FACTA de 2003 ofrece nuevos derechos a los usuarios que hayan sufrido este robo de identidad y prevé responsabilidades a los suministradores de información.[252]

En cuanto al procedimieno regulado en la Ley debemos resaltar que, en primer lugar, se comprueba que estamos ante un informe que cumpla criterios de conformidad (propósitos, requisitos, notificación etcétera). Se regula la divulgación o puesta en disposición de esos datos o informes a las agencias gubernamentales en el ejercicio de sus funciones, aplicando la excepción legal, así como la entrega de datos a los propios consumidores de su propio expediente y de sus fuentes de información o persona que lo recaba (con limitación temporal); y en general, con excepciones (como por ejemplo, referidas al propio fin del informe y sus resultados o si son agencias gubernamentales en el ejercicio de su función quienes los recaban).

El propio precepto regula el procedimiento y requisitos para recabar este informe propio junto con los derechos que deben respetarse en los mismos para el consumidor (obtener

[251] § 1681c-1
[252] 1681c-2

copia, frecuencia del acceso etcétera). Con especial atención, al igual que en lo visto anteriormente, a las posibles víctimas de fraude y de robo de identidad.

Entra a establecer además cuando es posible conocer los objetivos del informe de crédito (el "para que se recabó"). Y estipula los requisitos de forma y las condiciones de la puesta a disposición del informe a los consumidores, como serán, en general, su forma escrita y una identificación adecuada.[253]

También se tiene un acceso gratuito a los informes en caso de que se haya entablado por otra parte acción contraria contra el titular de los datos, en base a esos informes. De igual manera para personas desempleadas o afectadas por informes erróneos.

Ello se articuló con la reforma de 2003 operada por la *Fair and Accurate Credit Transactions Act*, en la que los consumidores adquirieron un derecho a obtener un informe de crédito anual gratuito a emitir por cada una de las tres grandes Agencias de crédito.

Hace así por tanto la Norma una distinción de derechos, en función de si los datos se ven tratados por una Agencia grande de ámbito nacional o por una menor o geográficamente limitada.

La Ley ofrece, además, el derecho a corregir la información incorrecta en los datos de los informes, reclamándose así a las "CRA's". Si la "CRA" no puede resolver la situación, la persona puede añadir una declaración al informe. La información incorrecta o no verificada debe ser eliminada en un plazo de 30 días. La investigación de ello ha de ser "razonable", según la modificación de la FACTA de 2003, si bien este parámetro es menor que el que se establece para la elaboración del propio informe. Es decir, la investigación solo es razonable en contraste con los requerimientos para la creación del informe.

[253] Se tiene por tanto legalmente ese derecho de posibilidad de acceso al expediente individual que lleven estas Agencias (CRA's) si bien las mismas pueden solicitar una contraprestación por ello.
(§ 1681e, f, g y h). La FTC lo ha establecido en 9 dólares con carácter general, si bien seis Estados (Colorado, Georgia, Maryland, Massachusetts, New Jersey, y Vermont) han elaborado y aprobado Leyes que obligan a las CRA's a expedir estos informes de manera gratuita a sus residentes. Otros Estados (Connecticut, Maine, Minnesota, California, y Montana) han establecido legalmente un precio reducido.

También opera ese derecho contra el suministrador de los datos, (algo que antes de la reforma de 2003 no era posible, enfocándose solo en las CRA's).

De ello se encarga la letra i del precepto, que regula el procedimiento en los casos de controversia en la exactitud de los datos del informe, y ofrece esa posibilidad de "reinvestigación" o de revisión en el caso de que el consumidor afectado encuentre inexactitudes en el mismo. Las obligaciones de advertir sobre este proceso a los destinatarios del informe recaen sobre las Agencias, si bien se le otorga a las mismas la facultad de decidir si esta reivindicación sobre la exactitud es "frívola o irrelevante". En ese caso deberá notificarse de manera motivada al consumidor afectado.

En ese supuesto de que se reconozca la pretensión de inexactitud, el precepto dispone una serie de actos que van desde la rectificación a la prevención para que esas inexactitudes no se den de nuevo. De todo el procedimiento y su resultado se notifica al interesado a su finalización.[254]

Asimismo se regulan las tasas por la emisión de informes, así como las excepciones a las mismas. Se establece para casos de empleo y en el caso de *public records* (acceso público), que las agencias también deben comunicar al consumidor que se está informando sobre ello, siempre que pudiera tener un efecto adverso para aquel, con estricta vigilancia de que el informe es correcto y está actualizado, y con la excepción habitual por razones de seguridad nacional.

En los "investigative consumer reports", no debe incluirse información adversa, a menos que haya sido verificada. La Ley se encarga de estipular los requisitos que deben observarse en los informes respecto a los consumidores afectados para el caso de que se puedan inferir acciones adversas contra ellos por la emisión de los mismos. Ello lo hace en el apartado de la letra m, importante y extenso artículo de corte garantista que contiene todas las precauciones consecuencia de los efectos perjudiciales de estos informes. Y ello exigiendo notificaciones, atemperando la información disponible en estos casos, o marcando las "lineas rojas" para las guías de actuación que los

[254]En todo este proceso se presume la vigilancia de la FTC, a la que se deberá dar cuenta, que a su vez deberá informar al Congreso en su documento anual informativo sobre las quejas y reclamaciones en este tema así como la responsabilidad acaecida en las Agencias (§ 1681i).

organismos gubernamentales con competencia en el asunto deben respetar, a la hora de formular esas reglamentaciones e instrucciones.[255]

Una sentencia que garantiza el derecho privado de acción contra los "proveedores de información" ("furnishers") es la sentencia Nelson en 2002, y que posteriormente incorporaría legalmente la FACTA en 2003 en su modificación de la FCR Act.[256]

3.3.1.2 Ejecución de la Ley y responsabilidad.

En cuanto a la ejecución de la Ley, las previsiones legales presentan diferentes ámbitos institucionales. Todas las Administraciones (Federal, Estatal y Local) pueden obtener información de identificación básica de la CRA's. Esa información es nombre, apellidos, dirección, empleo, etcétera.

Algunas Instituciones, por sus características, tienen acceso de mayor envergadura. El FBI en su función de llevanza de investigaciones criminales o las Agencias de espionaje, amparadas por la *USA Patriot Act* y con similar justificación, tienen ampliados accesos a estos informes de crédito.

En cuanto a su aplicabilidad tienen preeminencia o preferencia legal ("preemption") las leyes estatales en caso de mejora en la privacidad para el consumidor. Es por tanto la FCRA una ley de mínimos.[257]

La Ley entra también en horizontes temporales de mantenimiento de datos en estos informes (10años), y en la sección habitual de la Accountability (Responsabilidad), en su vertiente civil y penal.

Observamos además una figura legal de inmunidad para determinados supuestos contenidos en la norma.[258]

---

[255] § 1681 j, § 1681l y § 1681m

[256] Nelson v. Chase Manhattan Mortgage Corp., No. 00-15946 (9th Cir. 2002).

[257] Esta también es una aportación de las enmiendas operadas por la "Fair and Accurate Credit Transactions Act de 2003 (FACTA)"

[258] La llamada "qualified immunity provision". Aquí además tenemos el ejemplo de que no todas las modificaciones de la FACTA de 2003 fueron para mayor garantía de los usuarios.

Igualmente la Ley prevé la responsabilidad civil por daños resultantes de la no observancia de lo establecido en la norma, y producidos consciente o voluntariamente, marcando como separador de gravedad en el perjuicio en su valoración mayor o menor a 1.000 dólares. También para conductas negligentes.[259]

En cuanto al poder judicial, se establece la jurisdicción de los "United States district courts" (Tribunales estadounidenses) correspondientes, y establece plazos de prescripción para esa actuación en 2 años desde que se descubre la violación de ese derecho y en 5 desde que ocurrió esa violación jurídica. Se prevé además pena de prisión de 2 años en adelante para el que hubiere obtenido información bajo falsedad de pretensión, estipulándose igual plazo para empleados de las Agencias que revelen información de manera no autorizada o ilegalmente.[260]

Un perfecto ejemplo de aplicación judicial de la Ley y de la responsabilidad civil es el caso Sloane.[261]

En esta pieza jurisprudencial, si bien relacionada con el robo de información financiera del que se encargan más atentamente otras normas, se establece el caso de la consecuencia acaecida de ese robo de información que se mantiene en el tiempo en el expediente de Suzanne Sloane respecto al tratamiento de los datos por Equifax (otra de las grandes CRA`s).

[259] § 1681n y § 1681o

[260] § 1681p§ 1681q y § 1681r

[261] Sloane v. Equifax Information Services LLC 510 F. 3d 495 (4th Cir. 2007).
Tras más de 13 meses de infructuosas gestiones para modificar las incorrecciones e inconveniencias que el robo de su identidad financiera por parte de Shovana Sloan (empleada del hospital donde Suzanne dio a luz y que utilizó sus datos financieros para obtener créditos de manera fraudulenta) le estaba provocando; envió comunicación formal a Equifax. Tras una primera apariencia de solución, Equifax aumentó más el error, enviando una comunicación a la dirección de Suzanne a nombre de Shovanna Sloan pero con el número de seguridad social de Suzanne, en la que se contenía una advertencia a Shovanna de que era posible fuera víctima de robo de identidad por la ¡propia Suzanne! Además estos problemas continuados hacen mella en el matrimonio de Suzanne con Tracey, su marido, que debido a todos estos "problemas financieros" de su mujer tuvo que abandonar la idea de tomarse un año sabático en el Instituto donde trabajaba. Todos estos hechos probados se completan con habituales noches sin dormir y disputas y riñas matrimoniales (21 meses en total). El Jurado da por probada la violación de la FCRA por Equifax por actuación negligente.
Suzanne además ejerció su acción de responsabilidad civil, que fue apreciada por el tribunal en el daño emocional provocado, si bien este no aceptó la posible merma sobre su reputación que también demandaba. Todo ello se computó en una obligación pecuniaria de 150.000 dólares a favor de Suzanne Sloane.

A partir del apartado s) de la Ley se regula ya la ejecución administrativa de la misma por parte de la omnipresente FTC, así como por otras Agencias federales y por los Estados. Sigue en sus añadidos la regulación, de manera profusa, de la responsabilidad de los *furnishers* (o suministradores de datos para los informes), y la de la figura del *Affiliate sharing* o la de aquellos participantes necesarios en el tratamiento de datos; que por supuesto están excluidos de su uso para marketing, a menos que este claro que ese objetivo está permitido, estableciéndose la opción de "opt out".[262]

En este sentido, y sobre el perfil ejecutivo de la FTC, debemos retomar el informe de la FTC sobre sus guías de actuación en el que apunta a su principio rector "Transparency" como especialmente vinculado a la aplicación de esta Ley.

El principio que se mantiene en el informe (FTC, 2012, 60-64), si bien clarificado tras el procedimiento de información pública, es el de que las empresas deben incrementar su transparencia. Deben ser las notificaciones de privacidad más cortas, más claras y más normalizadas para permitir una mejor comprensión y comparación de las prácticas de privacidad. Y el acceso de los consumidores ha de ser proporcional y equilibrado con el uso que se pretenda hacer de esos datos por las empresas. Aboga por un equilibrio razonado y muestra la cara de la FTC, que venimos observando, de elemento de conjugación de la actividad económica en mayor medida que la de protector de los datos personales. Diferencia los objetivos de la *Fair Credit Reporting Act*, de los propósitos publicitarios y de marketing, y de otros más estrictamente relaciones con las necesidades profesionales, gozando de cierta protección especial los "credit reports".

Algunos tipos de negocios no encajan de manera clara con algunas de las dos categorías anteriores. En estos casos, la FTC utilizaría una especie de consideración nivelada en función del uso y sensibilidad de los datos.[263]

Las empresas deben, además, proporcionar acceso a los datos que mantienen de los clientes o consumidores de manera razonable, debiendo ser proporcionales dependiendo de la sensibilidad y naturaleza del uso de los datos. En la formulación última de este

[262] § 1681s con sus añadidos 2 y 3

[263] FTC (2012, 67): "*Finally, some businesses may maintain and use consumer data for purposes that do not fall neatly within either the FCRA or marketing categories discussed above. For these entities, the Commission supports the sliding scale approach…*"

principio hay bastante acuerdo entre la proposición de la FTC y las aportaciones de los actores en el proceso de información pública.

Se observan, ahora bien, especialidades que se tienen en cuenta a la hora de la formulación de las recomendaciones de privacidad, como pudiera ser el mecanismo de acceso especial para los "Data Brokers" (*Special Access Mechanism for Data Brokers*), que son empresas que se dedican a la recopilación de la información desde muchos ámbitos para después venderla. La falta de transparencia de estas empresas es motivo de preocupación de los participantes en el procedimiento de información pública, lo que queda plasmado en el documento (FTC, 2012, 67-68).

A partir de la actuación de la FTC estas empresas o su principal asociación crean una organización autorregulatoria. Además la FTC anima al Congreso a regular el derecho de acceso de los consumidores a sus datos que ostenten estas compañías. La *Data Accountability and Trust Act* prosigue sus trámites de aprobación en el Congreso. Recomienda además la FTC la creación por esa industria de una gran página web centralizada donde puedan ser identificadas por los consumidores, y en la que expliquen cómo recopilan y distribuyen o venden los datos, y a qué tipo de empresas. Asimismo en ella podrían explicar los derechos de acceso de los usuarios a sus datos así como otras opciones a los mismos (FTC, 2012, 69-70).

Si continuamos con la Ley, la *Preemptio*n estatal viene en ella establecida, y contempla las relaciones legales en el ámbito de esta ley federal con los Estados, básicamente asegurándose ser una ley "de mínimos" en sus preceptos y garantías.[264]

Finaliza la Ley con algunas consideraciones y regímenes especiales en la puesta a disposición de los datos para el FBI u otras agencias gubernamentales por razones de contrainteligencia.[265]

[264] § 1681t

Uno de los Estados con clara vocación de protección al consumidor en su legislación, superando ampliamente los mínimos de la FCRA, es Ohio que recoge todo un código de protección al consumidor, incluyendo una mejor protección de la privacidad financiera. Como ejemplo de ello podremos hablar de la *Credit Freeze Act* de 2008 que está contenida en el "*Ohio Revised Code*" (ORC) en su parágrafo 1349.52 y que requiere a las CRA's: "*to allow consumers to place a "freeze" on each of their credit reports to prevent opening new credit accounts in the consumers' names. The security freeze is designed to prevent credit, loans, and services from being approved in consumers' names without their consent*." Es decir, una auténtica acción de "congelación" de los informes de crédito para proteger la privacidad de los consumidores

3.3.1.3 Consideraciones

El resumen que podemos hacer de la ley, y a modo de recapitulación, está en relación con la dotación de derechos y responsabilidades a las personas involucradas en los Informes de crédito. Están los consumidores ("consumers") en este caso, las personas individuales, también las entidades que manejan la información ("furnishers") y la suministran a las CRA's, y por último los usuarios finales de esa información ("users") que reciben el informe. Son, por tanto, las CRA's las intermediarias en este "mercado de información crediticia".

Es una Ley que pone orden regulatorio a una actividad importante para el mercado de crédito y que define a los actores integrantes dotándoles de una capacidad y protección jurídica de la que antes de la Ley carecían.

Las CRA's, que se entienden en sentido amplio, son quizá el órgano cuya regulación se ha demostrado más relevante (dependiendo de la circunstancia, algunos tribunales han mantenido que incluso agencias de detectives o investigadores privados pueden ubicarse bajo el amparo de la Ley y tener esa consideración).

Además, un documento de tanta importancia como el Informe de crédito pasa a ser objeto de atención legal en el tráfico jurídico estadounidense. Si bien debemos observar algunas deficiencias en su integridad en lo que a privacidad se refiere. El ejemplo de la parte desgajada de los encabezamientos en esa protección es revelador. Y ello porque los encabezamientos de los informes parecen quedar fuera de protección de privacidad, de lo que entendemos una protección de datos parcial en estos documentos. Ya que esos encabezamientos conllevan también información personal si bien primaria o no especialmente protegida (nombre, dirección, sexo, número de la seguridad social...)[266]

[265] § 1681u y § 1681v

[266] Una de las recomendaciones de EPIC es acabar con esta distinción: "Congress should eliminate the distinction between the "credit header" and the actual credit report. In effect, Congress should move the credit header "below the line," so that it can only be used for permissible purposes under the FCRA"

Esos encabezamientos de crédito ("Credit headers") de los informes se empezaron a utilizar en este sentido después del caso (finalizado en acuerdo) de la FTC contra TRW (ahora Experian, una de las tres grandes CRA's), en el que se revisó y cambió su definición de "Informe de crédito" permitiéndose su uso y desprotegiendo su carácter de privacidad, considerándose por la FTC no formar parte (o constituir parte separada) del Informe de crédito.[267]

A pesar del avance regulatorio que supone la Ley en líneas generales, debemos fijar nuestra atención en unos importantes riesgos: los errores en los informes.[268]Como ejemplo judicial de ello y de la aplicación cotidiana de la Ley tenemos la sentencia Sarver[269]

Siguiendo esta línea crítica nos parece interesante la posición de Bils (2013) que pone su atención en las deficiencias de acción de los particulares para corregir las inexactitudes contenidas en los informes de crédito por parte de las Agencias, principalmente por parte de las tres grandes que elaboran la mayoría de los informes en América: Experian, TransUnion, o Equifax.[270]

La Ley sí que incluye un derecho de acción para el caso de intencionado o negligente incumplimiento. Sin embargo ello no se aplica para el caso de "inaccurate information". Solo lo tienen de manera mediata (§ 1681s-2(b)) a través de las Agencias. La razón de este sentido legal la establece el autor en la voluntad del Congreso de proteger a los proveedores de información ("furnishers") de demandas. Simple y llanamente, utilizan a

[267] Matter of TRW Inc. File Number 9810081(April 7, 1998).
El señor Sarver demanda a Experian (una de las tres grandes) por la información equivocada de uno de sus *credit reports* que le provocó no serle concedido un crédito por el Monogram Bank of Georgia. El informe contenía el error de una situación de bancarrota sobre el particular, y que venia referida a otra persona. Si bien el Tribunal en este caso no aprecia que se le hubieran provocado daños al señor Sarver.
[268] Según nos informa EPIC (recuperado el 22 de agosto de 2015), en 1998 un estudio del "US Public Interest Research Group" (US PIRG) daba a conocer el dato de que el 29 por ciento de los Informes de crédito contenían graves errores (enjuiciamientos falsos o falsos antecedentes penales por ejemplo) que pudieran denegar un crédito y un 70 por ciento algún tipo de error. Además de que al menos un 20 por ciento omitían información de solvencia que habría sido determinante para la obtención del crédito.
Igualmente a principios de los 90 TRW (ahora Experian) identificó como delincuentes fiscales a 3000 residentes de Norwich en Vermont y no consiguió subsanar el error antes de que los afectados identificaran el fallo masivo.
[269] Sarver v. Experian Information Solutions 390 F.3d 969 (7th Cir. 2004).
[270] Bils (2013, 228) El texto además anima al Congreso a un cambio legal que remueva esos grandes obstáculos a través del reconocimiento del derecho de rectificación individual directo. Aboga asi por la mediación agencial.

las agencias como "filtro antidemandas", que se viene a criticar como "poor public policy" (Bils 2013, 232)[271]

En el caso de que no se produzca la rectificación, el consumidor tiene derecho, como hemos visto, a demandar conforme a la FCRA. Pero en la práctica judicial gran parte de esas demandas se archivan por la falta de medios probatorios de que disponen los individuales en sus pretensiones. Siguiendo el estudio de la FTC (2013) al respecto, se pone el foco en que esa falta de efectividad sea de hecho más injusta con la gran recesión que sufrimos, no pudiendo rectificarse de manera efectiva esos informes con las repercusiones que para la concesión de crédito esto conlleva (o que paguen un 5 por ciento más por el producto de crédito o aseguramiento privado).

Otra línea de crítica a la Ley la presenta Murphy (2003) relacionada con la figura del *Affiliate sharing* (del 1681s-3), en la que se nos argumenta como se ha producido cierta desprotección legal de los datos de los consumidores y usuarios que, con la entrada en vigor de la enmienda de 1996 a la FCT Act, se ha hecho posible cederlos de manera desregulada entre las diversas empresas ("affiliates"), dentro de la red empresarial de la empresa matriz a la que se prestó el consentimiento originario, siempre con la posibilidad de "opt out". A partir de 2004 los Estados pudieron mejorar esta previsión legal aumentando las garantías en este sentido.

Esta referencia (Murphy, 2003), por tanto, nos sirve de análisis del artículo del parágrafo 1681, y como su modificación ha permitido un mejor control de los datos cedidos a los "affiliates". Igualmente pone de relevancia la posible confusión normativa de una recopilación asístemática de los aumentos o reducciones de exigencias en los derechos en función del sector normativo que se trate, aún dentro de una misma actividad jurídica (como es en este caso la financiera); teniendo en cuenta la divergencia de las previsiones normativas en este sentido de la "*Gramm-Leach-Bliley Act* "por un lado, y de la "*Fair Credit Reporting Act*" (FCRA) por otro (Murphy, 2003, 1-2).

Se hace eco también de las legislaciones estatales de mejora en estas previsiones. En las que se incluyen Alaska, Connecticut, North Dakota, y Vermont (Murphy, 2003, 4-5).

[271] Se establece como solución por el autor el reconocimiento del derecho de acción directa por los consumidores por parte del Congreso, modificando la FTC Act. Si bien con la concurrencia previa de reclamación a la "Consumer Financial Protection Bureau" que pueda alternativamente servir para filtrar pretensiones infundadas.

3.3.2. Financial Modernization Act of 1999, ("Gramm-Leach-Bliley Act")

Está Ley encargada de la regulación de ciertos asuntos financieros, es una de las leyes sectoriales importantes que incide en la regulación de la Privacidad en EE.UU., dentro del paquete de la "Financial Privacy". La ya estudiada Federal Trade Comission (FTC) es una de las 8 agencias de "enforcement" (ejecución legal) que tiene entre sus cometidos el de velar por esa "privacidad financiera" en lo regulado por esta Ley.

La Ley cubre el sector bancario y de inversión, y además el de seguros y la regulación de otra serie de compañías dedicadas al aseguramiento y comercialización de productos financieros.

Esta Ley rompe con la tradicional separación "rooseveliana" de la Ley Glass- Steagall de 1933, que separaba los bancos clásicos o de depósitos, de los de actividad de inversión financiera, Ley que tenía el objeto de evitar la especulación y no proliferaración de los bancos "demasiado grandes" (también para caer) o sistémicos. A partir de finales de los 80 y con la creciente acumulación de capital y de actividades extralimitadas de algunas entidades financieras americanas, como las del "Citigroup" que agrupaba multitud de servicios financieros de inversión y de aseguramiento, se plantea el cambio normativo que dio como resultado esta Ley de 1999 aupada bajo la Administración Clinton.[272]

3.3.2.1 Historia de la ley

Los riesgos para la privacidad que supuso la acumulación de actividad financiera nuevamente permitida por esta ley se pone de manifiesto a través de una serie de eventos (aparte deberíamos mencionar la avocación a la mayor crisis financiera mundial

[272] Varoufakis (2012) Resumen maestro se hace de estos cambios legales y económicos por el efímero ex ministro de finanzas griego antes de saltar a la fama. Ley que sienta las bases del estropicio económico que venimos sufriendo desde 2008 al confundir y desregular en gran manera las actividades financieras y mercantiles a un nivel de toxicidad inmanejable.

tras los años 30). Dos eventos principalmente, uno de corte internacional y otro nacional.

Internacionalmente el evento se produce en 1995 y se ocasiona en Europa con la aprobación de la Directiva de Protección de datos que requería que los datos de los ciudadanos europeos en sus transferencias internacionales tuvieran el mismo nivel de protección que los eb ella exigidos (o en la transposición de la misma realizada por cada Estado miembro). Lo que supuso una verdadera y obligada "puesta al día" en las empresas norteamericanas que se nutrían y gestionaban esos datos de ciudadanos europeos para alcanzar ese "estándar europeo" de protección. Debemos añadir que la Unión Europea estaba preocupada por la tendencia legislativa estadounidense hacia el "no hacer", es decir hacia la autorregulación por parte de las empresas en materia de protección de datos, y la falta de regulaciones federales al respecto. Todo ello fue generando el acuerdo de Puerto Seguro entre EE.UU. y la U.E. ("Safe Harbor" en sus términos de inglés americano) del año 2000 que, como veremos, permitía la autorregulación si bien bajo la vigilancia de la FTC. Pero el acuerdo (si bien ya también tocado) no contemplaba a la industria financiera en sus estipulaciones.[273]

A nivel interno, la privacidad se veía cada vez más amenazada, según opinión reflejada en estudios y encuestas realizados, además de la preocupación ciudadana que se venía generando sobre el tema. Y sobre todo en el ámbito del consumo financiero y en la falta de protección bancaria de la privacidad.

Más aún, este pulso social se fue acelerando con algunos asuntos sobre la venta de datos con propósitos de marketing y que incluían fraude y robo de identidad de los consumidores financieros.

A finales de 1997 el californiano *Charter Pacific Bank* de Agoura Hills en California vendió el número de millones de tarjetas de crédito a una web de contenido para adultos, que facturó a muchos de esos usuarios financieros servicios de pornografía "online" que no habían solicitado, algunos de ellos no habían encendido un ordenador en su vida.

[273] Con el pronunciamiento del TJUE de 6 de octubre de 2015 en el asunto Maximillian Schrems, y que veremos más detenidamente, el propio acuerdo de "Puerto Seguro" queda totalmente al descubierto y al tiempo que se escriben estas líneas parece abrir una etapa totalmente nueva en las relaciones de transferencias de datos entre EE.UU. y la Unión Europea.

La FTC, en su función de protectora del consumidor, ganó el juicio contra la empresa de pornografía, consiguiendo una indemnización para el público de 37,5 millones de dólares, si bien el banco mantenía que no había actuado ilegalmente por ese vacío legal, sí que dejo de mercadear con esos datos.

En 1998 el "Nations Bank" fue multado por violaciones en la seguridad de los datos que gestionaba, por compartirlos con sus empresas subsidiarias con ánimo de que estas realizaran negocios de inversión de alto riesgo con esos propios clientes, provocando grandes pérdidas entre ellos tanto en sus inversiones como en sus ahorros. La multa fue millonaria. Ya en 1999 el Fiscal general de Minnesota demandó al "U.S. Bankcorp" por la compartición de los datos de sus clientes, que gestionaba con terceros con ánimo mercantil, violando sus propias políticas de privacidad y sin autorización ni consentimiento. Igualmente se fue descubriendo que esta práctica era habitual y que esos datos y otros muchos eran vendidos y revendidos en un ciclo mercantilista entre grandes bancos (entre ellos Citigroup o Chase Manhattan) y los "Telemarketers".[274]

Ello hace incluir el asunto de la privacidad financiera y sobre todo en el Título V de la GLBA.[275]

3.3.2.2 Análisis de la Ley

La "Financial Privacy Rule" que nos ofrece la Ley se encuentra ubicada en el Título 15 del USC que viene dedicado al Comercio, y concretamente en su capítulo 94 en sus dos subapartados.[276]

[274] Seguimos el resumen de los antecedentes de la Ley que realiza EPIC, Recuperado el 30 de agosto de 2018: https://epic.org/privacy/glba/

[275] Estas previsiones de la GLBA fueron presentadas en el Senado por el Senador Phil Gramm el 28 de abril de 1999, bajo el informe 106 S. 900 y en el Congreso por el representante James Leach con el informe 106 H.R. 1. La ley se firma por el Presidente Clinton y entra en vigor como Public Law 106-102 (113 Stat. 1338) el 11 de noviembre de 1999. (Fundamentándose el redactado de la Ley en el informe de la Comisión del Congreso "Committee Reports 106th Congress (1999-2000)House Report 106-434")

[276] "Subchapter I - disclosure of nonpublic personal information (§§ 6801 to 6809)" y "Subchapter II - fraudulent access to financial information (§§ 6821 to 6827)"

El parágrafo 6801 es el precepto matriz que aporta la Ley en protección de privacidad financiera. Con el enunciado "disclosure of nonpublic personal information" establece la regla general de regulación sobre la puesta a disposición de los bancos de la información financiera de sus clientes.

Su letra a) establece la obligación de la llevanza de una política de privacidad a la entidades financieras. Y su letra b) se refiere a las obligaciones administrativas de las Agencias y Autoridades competentes para establecer los estándares necesarios para la correcta aplicación de esta obligación legal y la salvaguarda de la privacidad de los clientes (tanto en el plano administrativo, técnico y físico).[277]

Sobre la Ley, por tanto, podremos presentar algunos apuntes de relevancia. Son las instituciones financieras afectadas por la ley las que se someten en primera instancia a la legislación estatal, que en todo caso debe cumplir con los mínimos de la ley federal, (pudiendo mejorarlos), siendo importante la diferenciación que nos presenta la Ley entre "consumers" (consumidores) y "customers" (clientes) basada en la mayor relación de continuidad de estos últimos.

Así los clientes y consumidores tiene la opción de "opt out", es decir de que su información no sea compartida con terceros, y que se ofrece sobre todo a partir de la *Fair Credit Reporting Act*, que estudiamos anteriormente. Es de gran importancia la "Safeguard Rule" que hemos visto en letra b), que complementa a la obligación general, y que obliga a las instituciones financieras a disponer de un plan de acción para proteger la información y la privacidad de sus usuarios.

El Título V de la Ley es el que se encarga de la regulación de la privacidad en esta norma y en el ámbito sectorial financiero, y va de los artículos (o secciones) 501 a 527, que son coincidentes con su codificación en el Título 15 del U.S.C. (parágrafos 6801 a

[277] Las entidades financiera afectadas y sobre las que pondrán el foco las Autoridades se reparten competencialmente en el 6805(a) para su regulación y supervisión (bajo el título "Enforcement"). La división se da entre las Agencias no solo federales sino también entre organismos estatales en función del tipo de entidad financiera a supervisar. Las autoridades van desde la FTC hasta las autoridades estatales de control de las aseguradoras, o desde la "Bureau of Consumer Financial Protection" hasta los reguladores federales en función de la materia.

6827). Seguiremos la clasificación codificada tal y como hemos mantenido en el resto de estudio de las normas legales sobre privacidad estadounidense.

Se establece, como hemos visto, la obligación general, para las instituciones financieras, de protección de la información personal no pública. Se trata de una obligación continua a tener con sus clientes.[278]

Se establece además la regla general de no cesión de los datos a terceros, a menos que se haya notificado expresamente al consumidor afectado (no tiene por qué ser necesariamente un cliente).[279]

Podrá la institución financiera dar esa información no pública siempre que de manera clara y fehaciente[280] haya informado por escrito o telemáticamente, o bien en algunas de las otras formas permitidas por el artículo 6804, que esa información se va a ceder a un tercero. Que el tercero no se oponga de manera directa o más bien que le sea dada la oportunidad de oponerse de manera directa a esa cesión, y que, además, se le ofrezca una explicación a ese consumidor de cómo puede ejercer esa oposición.

Notamos aquí la diferenciación con Europa donde la situación de consentimiento es generalmente inversa, es decir, expresamente por el interesado ("opt in") mientras que aquí el "opt-out" es la norma general.[281]

La excepción con la que continua el articulo si se parece un poco más a lo estipulado en Europa: "que sea necesario para la actividad del principal, obligándose el tercero a mantener el nivel de confidencialidad"[282]

Se encarga, por tanto, la Ley de los límites de la reutilización de esa información por parte de ese tercero, que no podrá seguir la cadena de cesión de los datos para otro tercero. Y concretamente de las limitaciones en la compartición del número de cuenta

[278] § 6801.
[279] § 6802. Con la posibilidad de "opt out" de esa posible cesión previamente notificada. Siempre seguimos hablando de "Nonpublic Information" (información que no sea de acceso público)
[280] ("conspicuously") (notablemente)
[281] Apuesta por el "opt-in" que se desprende de la definición de consentimiento del apartado 11 del artículo 4 del Reglamento Europeo de Protección de Datos que nos dice "11) «consentimiento del interesado»:toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".
[282] Parecido razonable al artículo 13.2 e) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

con propósitos de marketing. La regla general se acompaña de una similar restricción a la comentada. Si bien estas restricciones generales tienen también sus excepciones generales, continuando el artículo con una enrevesada formulación jurídica de contraposiciones. Que hacen de estas extensas excepciones generales un debilitamiento importante de la regla general de la protección del "non disclosure" de esa información.[283]

Igualmente se ordena la necesidad de la divulgación o publicación de la política de privacidad de la institución financiera en forma de notificación clara y fehaciente al cliente, al menos de manera anual. Y se encarga de la regulación de las autoridades competentes para hacer cumplir la norma y la elaboración de sus reglamentaciones.[284]

Y se desarrolla asi una obligación a las entidades referidas a que colaboren y se pongan en contacto entre ellas para conseguir unas reglamentaciones armonizadas y coherentes entre sí. Reglamentaciones que, claro está, deben respetar el título 5 que se refiere a las agencias gubernamentales estadounidenses, sus responsabilidades y funciones y su régimen de personal (punto 3)[285]

Se distingue asimismo las autoridades en función de las entidades a vigilar. Y de las funciones a realizar Si bien la reglamentación está encomendada a unos órganos, la aplicación o ejecución se encomienda a otros (al igual que en el marco europeo, nacional y regional), si bien con el evidente protagonismo de la FTC que cumple un papel destacado en los dos niveles.[286]

En caso de verse afectados por la sección 8 de la *Federal Deposit Insurance Act* (Ley de Seguros) se va distribuyendo en función de la "entidad" (o importancia geográfica y cuantitativa) de la entidad.[287]

---

[283] Letras c d y e del artículo 6802

[284] Principalmente "*the Bureau of Consumer Financial Protection and the Securities and Exchange Commission*".

[285] Parágrafos 6803 y 6804.

[286] Parágrafo 6805.Se trata de una auténtica distribución competencial exhaustiva de los órganos competentes (federales, estatales y locales) en función de la institución cuya responsabilidad de privacidad se esté ejecutando.

[287] Como visión práctica diremos que "national banks, Federal branches and Federal agencies of foreign banks" (ejemplo: alguna sección de aseguramiento del Banco Santander en EE.UU.) la encargada será la "*Office of the Comptroller of the Currency*".
De la Letra B mayúscula del artículo a la D va estableciendo estos órganos regulatorios según la materia, entrando en juego por ejemplo la "Securities and Exchange Commission", para entidades de inversión (puntos 3, 4 y 5) y la FTC cuando entre en juego la "Federal Trade Commission Act" (como ya vimos

Si la autoridad estatal no ejercita sus competencias de adopción reglamentaria parece que no podrá hacer caso omiso de la regulación federal en su caso. Poderes absorbentes federales que pudieran tener cierta similitud con algunos de la U.E.[288]

La Ley no entra a enmendar las leyes y normativas estatales excepto en aquello que la contradiga. Es decir que nos encontramos ante una Ley de mínimos.Y establece como órganos de estudio de la información que comparten las instituciones financieras a "The Secretary of the Treasury", en conjunción con los reguladores federales en función de la materia, así como a la FTC.[289]

Termina la Ley en su primera parte (subtítulo a) con las definiciones de los sujetos y objeto de la Ley en materia de privacidad. Además de perfilar cada uno de las instituciones financieras con referencias normativas concretas, indicando su ubicación jurídica, dejando fuera a las entidades de crédito agrario. Por destacar algunos términos de definición que revistan mayor interés aludiremos al de información personal no pública, que utiliza la base de la PII (personal identifiable information) propia de la privacidad del consumidor, y la traslada al ámbito financiero, así como a la distinción entre "affiliate" y ''nonaffiliated third party'', que presenta también interés por la distinción jurídica en su tratamiento en la Ley respecto al uso de la privacidad que manejan.[290]

En la segunda parte de la Ley (subtítulo b) queda codificado la regulación del acceso fraudulento.[291]

---

anteriormente).
En la introducción de estándares podemos fijarnos la codificación administrativa la podemos encontrar en el 12 CFR 364.101 bajo el enunciado "Standards for safety and soundness."

[288] § 6805 letra c)
Estableciéndose las definiciones con las generales sobre bancos y sistema bancario establecido en el 12 U.S. Code § 1813 (según la letra d)) que son las establecidas en la *International Banking Act* de 1978.

[289] Parágrafos 6807 y 6808
Ese esfuerzo de estudio que recae sobre la Secretaria del Tesoro pone el foco en la compartición de información de las instituciones, y su potencial de riesgo para la privacidad, con consulta además a los órganos estatales de supervisión. De ello se informará al Congreso.

[290] Parágrafo 6809

[291] "Subtitle B—Fraudulent Access to Financial Information" y se sustancia en el 15 del U.S.C., que va desde el parágrafo 6821 al 6827.

Empieza encargándose de la protección de la privacidad de los clientes de las instituciones financieras. Y lo hace con una serie de prohibiciones, como son las de obtener información de los mismos por medios fraudulentos y falsas pretensiones, así como la petición a las instituciones financieras de esa información mediando esa falsas pretensiones (que se conoce como "Pretexting").

Si bien después comienzan las salvedades a esas prohibiciones generales, dejando fuera de estas cautelas a la Agencias de aplicación de la Ley ("Law Enforcement Agencies"), si con ello se pretende evitar el cumplimiento de esas leyes. Y también se excepcionan ciertos casos para las propias instituciones financieras, que serían casos para implementar la protección de la propia privacidad, para casos de investigaciones disciplinarias internas o para la recuperación de información que ya se recabó usando el filtro de protección de privacidad (propio o por terceros) exigible y exigido.

Igualmente para los tipos penales de fraude en seguros (e). Así como otros dos tipos de excepción para "ciertos tipos de clientes", o en temas relacionados con la averiguación financiera en juicios civiles para dilucidar pensiones a los hijos menores. (f) y (g)[292]

Continúa la Ley haciendo una división para la ejecución de las competencias administrativas, atribuyéndolas a los distintos órganos administrativos encargados de su aplicación. Parece adquirir protagonismo la FTC en la aplicación general, si bien se distinguen, al igual que lo visto con anterioridad, y en función de la entidad, agencias de ejecución especializadas.

Para los casos de fraude previstos en este subtitulo ya sí que juega y se deriva hacia el derecho penal tipificado, según lo contenido en el título 18 del U.S.C. (encargados de tipificaciones penales) con multa y penas de prisión de hasta 5 años. Para el caso de infracciones agravadas (es decir para los casos en los que se infrinjan además otras leyes, o que se parta de una actividad de delincuencia organizada) se pueden doblar las multas, así como la pena de prisión (hasta 10 años).[293]

[292] Parágrafo 6821
[293] Parágrafos 6822 y 6823

Al igual que lo estudiado con anterioridad, estamos ante disposiciones propias de una ley “de mínimos”, en su relación con los Estados y las leyes estatales, y que no deben ser contrarias a ella. Se encomienda a las respectivas agencias administrativas implicadas en la ejecución de la Ley, la labor de guía en este campo, con elaboración de recomendaciones y dictámenes. E impone la obligación y plazo para informar al Congreso. Y termina con las preceptivas definiciones normativas para la aplicación del subtitulo, en similar sintonía que lo referenciado en las definiciones de la primera parte de la Ley.[294]

3.3.2.3 Consideraciones sobre la Ley

La GLBA, por tanto, nace con la intención general de modernizar los servicios financieros con la técnica política y jurídica propia de los tiempos: la desregulación. Si bien ello ha presentado y acentuado una serie de riesgos con el acceso a una vasta información y datos que las entidades financieras pasan a disponer, y de la que generan un lucro permanente. Además de que ese uso de información se encontraba muy dispersado en cada empresa o compañía. La Ley, sin embargo, ha introducido, con ánimo sistematizador, algunos requisitos clave para la protección de datos de los individuales:

– Las entidades de crédito y de seguros han de mantener de manera segura los datos financieros de los que dispongan.

– Deben publicitar y dar a conocer sus políticas de privacidad.

– Deben ofrecer a los consumidores la opción de “opt-out” en caso de que vayan a “compartir” o usar los datos que les afecten.

La Ley solo regula instituciones financieras en sus diversas actividades, entre las cuales se incluye su actividad de protección de la privacidad. Una de las principales obligaciones es que las instituciones deben tener en aplicación un plan de privacidad como tal entidad, a todos los efectos.

[294] Parágrafos 6823 a 6827

En caso de que se vaya a pasar a tener la condición de cliente, se debe notificar la política de privacidad así como la política de compartición de esos datos e información al inicio de la relación mercantil, y de manera anual posteriormente a la primera suscripción contractual de cliente. Esta sería la segunda gran obligación.

Se da al consumidor financiero el derecho "opt-out" a esa puesta a disposición de sus datos con otras empresas, si bien para las empresas relacionadas ("affiliates"), no le asiste ese derecho a los consumidores (no clientes). Se observa asi que el consumidor no tiene el control sobre su "baile" de datos entre empresas pertenecientes al mismo conglomerado.[295]

Para el caso del "telemarketing" la Ley ofrece una mayor protección. Al fin y al cabo fue una de las actividades generadoras de la reacción que provocó la elaboración de la misma. Se prohíbe la divulgación con este fin. Por tanto, aunque no se produzca el "opt out" del cliente, esta actividad queda vedada en su ánimo mercantil.

En último lugar se regula la asimilación penal del "pretexting", que es, como aludimos, la forma fradulenta de recopilación de datos, con pretensiones falsas, es decir con propósitos distintos a los establecidos en su solicitud. Básicamente es el robo de información mediando engaño.

Debemos además tener presenta la problemática que presenta la Ley[296]respecto a la efectiva protección de los consumidores y la carga que soporta la parte representada por el consumidor en la relación comercial, y además la única cuyos derechos más íntimos se pueden ver afectados; en contraposición a una supuesta lesividad de tipo puramente pecuniario para las entidades financieras. Se trata de evitar esa supuesta lesividad mercantil a costa de la precarización de la protección del individuo consumidor en su

[295] No se nos puede escapar que en un país como EE.UU., y en su entorno global donde las grandes firmas mercantiles están formadas por una red de numerosas empresas, esta salvedad legal no solo provoca difuminación de la protección jurídica pretendida, sino una ventaja comparativa desleal que proporciona el uso de esos datos, proporcional al tamaño de la empresa.

[296] La web del "Electronic Privacy Information Center" se hace eco de una serie de problemas de la Ley al considerar que no se protege a los consumidores. Consideramos que la protección que otorga la Ley no se antoja suficiente, ya que traslada la carga "opt-out" para excluir el tratamiento de esa información a los propios consumidores con toda la desventaja que ello conlleva. Así alega EPIC (recuperada el 25 de agosto de 2015): "*It unfairly places the burden on the individual to protect privacy with an opt-out standard. By placing the burden on the customer to protect their data, GLBA weakens customer power to control their financial information*."

ámbito de privacidad. Y ello a través de la estandarización del sistema "opt out" a sus espaldas.

De ello se hacen eco de igual manera Janger & Schwartz (2002), que, además, hacen una crítica general a la Ley por no contentar ni a la industria financiera ni a los consumidores y defensores de la privacidad. Critican la mera opcion de opt-out contemplada en la ley como único aporte real de la misma, provocando insatisfacción general.[297]

Además de la confusión y límites a la transparencia que las políticas de privacidad de las empresas (habitualmente de las grandes) presentan para el cliente. Y en las que casi nunca se incluyen los términos y condiciones de cómo se utilizan y se utilizarán esos datos ni su destino. Evitándose la posibilidad de control por los consumidores de esos datos y anteponiéndose así la actividad económica por la GLBA a la privacidad. Se establecen las excepciones a la regla general como la auténtica regla general.[298]

El hecho de que en la Ley no se dote al ciudadano de un derecho individual de acción, y que solo se pueda ejercitar mediatamente a través de la intervención agencial pública es otro de las críticas que se pudieran realizar a esta norma legal.

Una diferencia que se ve es la mayor militancia de la sociedad civil en estos temas de protección de la privacidad en contraposición a la mayor institucionalización europea en esta vigilancia. En consonancia también con el sentido más liberal de aquella regulación americana a la hora de proteger el propio derecho.

Por último, debemos mencionar otros aspectos normativos vinculados a la Ley y que nos parecen reseñables siendo ejemplo el Acuerdo (Settlement) entre Citibank y el Fiscal General de New York, que pudiéramos ver como paradigma de acuerdo previo

[297] Janger & Schwartz (2002, 1230-1232) "… In other words, the GLB leaves the burden of bargaining on the less informed party, the individual consumer…"

[298] Recordando al silencio administrativo en el Derecho Administrativo español, si bien en este caso orientado para las grandes corporaciones estadounidenses y confirmando la imagen de su poder en América.
Algo que en mayor o menor medida todos hemos comprobado con letra de acuerdos de privacidad que marcamos con un "check" de leído y aceptado sin mucha más intervención previa, y con contenido difícil hasta para los más concienciados con sus derechos. Siendo la alternativa no poder acceder al servicio o producto de que se trate.

por posibles violaciones de la Ley, o bien ya el pronunciamiento judicial con actuación de la FTC también como paradigmático en el caso IRSG v. FTC.[299]

Además la Federal Deposit Insurance Corporation (FDIC) en su función ejecutiva, (y en similar manera a la labor estudiada en los casos de *Consumer Privacy* realizada por la FTC), establece un manual de desarrollo reglamentario de la Ley donde interpreta y desarrolla conceptos y procedimientos concernientes a la misma. El manual FDIC 2014 establece entre muchas oras normativas ejecutivas, un protocolo de evaluación del cumplimiento de la privacidad por parte de la instituciones financieras.[300]

3.3.2.4 Leyes estatales

Al encontrarnos ante una "ley de mínimos", los Estados podrían mejorar la Ley siendo el establecimiento del "opt in" la posibilidad de mejora más evidente.[301][302]

En cuanto a Leyes estatales reseñables en la mejora de las estipulaciones federales relataremos las siguientes:

- California es uno de los Estados de mayor avance sobre la GLBA en el panorama estatal. Aupado por una activa promoción de sectores de la sociedad civil (entre los que se pueden contar la Consumers Union, la American Association of Retired Persons o la American Civil Liberties Union) se puso en la agenda la mejora estatal de la privacidad financiera a partir del año 2002, con la intermediación política del Gobernador Gray Davis (que la estableció además en sus políticas de campaña).[303]

- Dakota del Norte también se vio abocada, por la presión de la sociedad civil, a incluir estipulaciones de "opt-in" en su agenda legislativa. Si bien en una forma contraria a la

[299] 145 F. Supp. 2d 6, No. 00-1828 (D.D.C. 2001)
[300] Y que viene siendo actualizado periódicamente. Recuperado el 28/03/2018: https://www.fdic.gov/regulations/compliance/manual/
[301] Es interesante en este sentido el informe de GAO (2012) sobre la introducción de esta opción (opt-in) en relación con los derroteros que toman los Estados en su aplicación.
[302] Nos son de utilidad las referencias contenidas en Solove & Schwartz (2015,779-780)
[303] Alguna dificultad de implementación en California de la opción "opt-in" hizo que algunos condados o entidades territorales inferiores al Estado plantearan sus propias ordenanzas en este sentido (como el San Mateo County o la Daly City) si bien impugnadas por las grandes compañías financieras como Bank of America y el Wells Fargo Bank para conseguir su anulación.

de California, ya que en principio la posición política de sus dirigentes era la de eliminar esa posibilidad. Grupos de presión como "Protect Our Privacy" y la ayuda de la American Civil Liberties Union (ACLU) iniciaron y financiaron una campaña para el mantenimiento de la opción “opt-in” en contra del posicionamiento de las principales instituciones financieras de la zona. Así se llegó a una consulta popular o referéndum que avaló la tesis del “opt-in” de manera abrumadora. Y convirtiéndose en un buen ejemplo de democracia participativa en el ámbito de la privacidad para conformar políticas públicas de protección.[304]

- En Vermont, Estado tradicionalmente progresista (o liberal/libertario en el sentido de la terminología política americana), la conformación del “opt-out” fue distinta y de mayor “facilidad institucional” que en el caso anterior. El propio Gobierno opta por esta determinación en la configuración de las normas de privacidad financiera.[305]

- En otros Estados se ha introducido de una manera u otra cierta opción “opt-in” en la privacidad financiera antes de que se compartan esos datos.[306]

3.3.3 The Right to Financial Privacy Act de 1978

Es una de las Leyes dentro del conjunto normativo de la privacidad financiera que se enfoca a la regulación de la cesión de la misma a los poderes públicos, más que a la propia regulación general de la misma. Es, por tanto, una Ley de las establecidas como de control al Gobierno en su uso de información más que una norma general de privacidad en el ámbito financiero (como si lo son la FCRA y la GBA) en esa relación de consumo.[307]

Esta ley protege la privacidad de la información personal de tipo financiero, de cuya desprotección legal se tuvo conciencia a partir del pronunciamiento judicial del Tribunal

[304] Votando a favor del mantenimiento de esta opción de privacidad el 73 por ciento de los votantes.
[305] “Privacy of Consumer Financial and Health Information State of Vermont Regulation”.
[306] Los citaremos juntos con la reseña de la ubicación en sus Códigos Alaska (Alaska Stat. § 06.05.175), Connecticut (Conn. Gen. Stat. Ann § 36a-42), Illinois (205 Ill. Comp. Stat. Ann. 5/48.1), y Maryland (Md. Code Ann. § 1-301).
[307] La Ley se encuentra codificada en el título 12 del U.S.C., Capítulo 35, bajo el enunciado “Right to Financial Privacy” (§§ 3401 – 3422).

Supremo de EE.UU. de 1976 "United States v. Miller", en el cual se establecía esa falta de derecho expreso en la ciudadanía estadounidense. Todo ello amparado con el respaldo constitucional de la Cuarta Enmienda.[308]

Este es el asunto fundacional que da paso a la Ley (que es de motivación jurisprudencial), tratándose de un pronunciamiento del Tribunal Supremo estadounidense que interpretaba la ausencia del derecho a la privacidad financiera por parte de los clientes de los bancos. En la sentencia se establecía que los ficheros eran propiedad del banco, y no podían presumirse de ellos expectativas de privacidad en base a la Cuarta Enmienda, y a la legislación reguladora del momento (la "Bank Secrecy Act").[309]

Se observó entonces un riesgo claro para la privacidad de los consumidores financieros con esta aseveración judicial.

La propuesta original de la Ley se basaba en tres pilares que requerían regulación como eran en primer lugar el derecho a ser notificado por el Gobierno antes de la divulgación de sus datos por entidad financiera. En segundo término el derecho a enfrentarse y disentir sobre la puesta a disposición de su información, y por último, el derecho al seguimiento de la revelación o puesta a disposición de su información. Es decir una auditoria de cómo y de qué hace el Gobierno con los datos financieros.

Esta ley está enfocada y solo afecta a las Autoridades o Agencias gubernamentales y no se regula el traspaso de información en los negocios privados, que como ya hemos visto, se regula por otras leyes en el ámbito financiero.

La Ley tuvo oposición por parte del mundo del empleado público federal que alegaba que esta Ley facilitaba las cosas para el crimen de "cuello o guante blanco" según percepción anglosajona o latina.[310]

---

[308] United States v. Miller, 425 U.S. 435 (1976).
En California Bankers Association v. Schultz, 416 US 21 (1974) el Tribunal Supremo tuvo un pronunciamiento similar, contándose así ya con precedente.

[309] Sentencia que no debe ser confundida con otra de mismo nombre pero de 1939, si bien relacionada también con los bancos, en este caso y muy propio de la época, con el robo a los mismos.
Una crítica a la sentencia la podemos ejemplificar en el artículo de Nicol (1976).

[310] EPIC apunta al respecto que: "Much of the opposition to the RFPA has been by federal law enforcement officials who are concerned that the proposed privacy protections would impede federal authorities in their investigation and prosecution of white-collar and organized crime..."

3.3.3.1 Contenido de la Ley

Arranca el estipulado de la Ley definiendo a las instituciones financieras sometidas a la misma en sentido amplio. Importante es la definición del objeto cuya privacidad se regula en la Ley. Es decir del archivo o información financiera. Es importante igualmente la del sujeto al que se le dota del derecho, el cliente o consumidor financiero.[311]

Particularmente importante es la definición de institución financiera. El concepto de institución financiera que establece la Ley es amplio, abarcando no solo a los clásicos bancos o entidades de crédito, sino también a negocios relacionados con la prestación dineraria a crédito no habitual en la acepción común de entidad financiera, y que llega a abarcar al Servicio Postal o a los casinos.[312]

Es de destacar la importancia de esta definitoria normativa porque es una Ley que entra en juego en función de los sujetos que manejan esa información financiera (las instituciones financieras) y no asiste, como es habitual en el fragmentado derecho estadounidense a la privacidad, a derechos subjetivos de alcance general para los ciudadanos, activándose su protección con la ubicación de la actividad jurídica de que se trate.

La prohibición general y las excepciones a esa prohibición[313]ocupan buena parte del contenido de la norma. Las previsiones de la Ley en este sentido se pueden resumir en una prohibición de acceso por parte del Gobierno a los registros financieros de los

[311] § 3401 ("Definitions") En el punto 2 del artículo nos dice que:" *"financial record" means an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution". Y en su punto 5: " "customer" means any person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person's nam*e".

[312] Incluso a "cards clubs" o entidades de viaje con tarjetas al efecto.

[313] Contenidas en el § 3402 ("*Access to financial records by Government authorities prohibited; exceptions*"). Y desarrolladas en los parágrafos 3404 a 3408.

particulares a menos que los mismos sean razonablemente identificados y además se de alguno de estos casos:

- Que el cliente autorice el acceso.

- Que haya una correcta notificación o citación administrativa.

- Que haya una garantía cualificada para esa petición.

- Que haya un requerimiento judicial.

- Que haya un apropiado requerimiento por escrito de alguna autoridad o agencia estatal.

La acción gubernamental debe acompañarse de una notificación al particular avisando del requerimiento que está haciendo el Gobierno o Autoridad Pública a la entidad financiera de que se trate, con copia de lo solicitado. El particular puede, o bien prestarse a colaborar, dando él mismo la información, o bien en plazo dado (10 o 14 días) enfrentarse u oponerse a esa revelación que se solicita.

Las excepciones al derecho contenido en la Ley son tan abundantes como relevantes, en las que las posibilidades de revelación de información están permitidas sin autorización o mandamiento judicial:[314]

- Excepción de de primer tipo: Las divulgaciones que no identifiquen al cliente o consumidor[315]

- Excepción de segundo tipo (necesidad de su ejercicio de supervisión por las autoridades financieras de control): Divulgaciones que sean de interés de la institución financiera incluidos los motivados por asuntos de seguridad, o prestamos del Gobierno o garantías y seguros de préstamos, así como aquellas puestas a disposición al Gobierno por posibles violaciones legales. Éstas últimas están limitadas al nombre del titular de la cuenta y condicionadas a la entidad del posible delito.

- Excepción de tercer tipo: Divulgaciones motivadas por investigaciones de supervisión financiera.[316]

[314] Desarrolladas en el § 3413 ("Exceptions")
[315] En este sentido es interesante la sentencia Donovan v. National Bank of Alaska, 696 F.2d 678 (9th Cir. 1983).

- Excepción de cuarto tipo: divulgaciones amparadas por las previsiones de privacidad tributarias, pudiéndose solicitar información al banco por la Autoridad pública sin necesidad de aviso al contribuyente-cliente. Ello en base al "Internal Revenue Codes", los códigos tributarios estadounidenses que están dotados de sus propias normas de protección de privacidad.

- Excepción de quinto tipo: divulgaciones amparadas por las previsiones de otras Leyes, bien administrativas o judiciales, que impliquen labor de supervisión e inspección.

- Excepción de sexto tipo: divulgaciones motivadas por razones de emergencia o las necesarias para la labores de inteligencia o contrainteligencia.[317]

Habría que ver si estas excepciones no hacen a la Ley una aventura programática más que una eficaz atribución de derecho.

La Ley propugna, como uno de sus elementos relevantes, la confidencialidad de los documentos financieros, estando prohibida su libre puesta a disposición a las autoridades gubernamentales. Si bien acto seguido se establece la misma prohibición pero ya con una salvedad importante: a menos que la autoridad gubernamental certifique por escrito a la institución financiera que ha cumplido todos los requisitos legales contenidos en esta norma para esa solicitud.

Y ello sin perjuicio de que la entidad financiera suministre información a la autoridad gubernamental que sea relevante en previsión de posible infracción normativa. Además estando exentos de responsabilidad en caso de, digamos, que esta previsión fuera errónea. Incidiendo en particular en concreto suministro relevante con las mismas previsiones[318]

---

[316] Ejemplo del caso en que la "Securities and Exchange Commission" quiera investigar a un banco nacional por actividades sospechosas y operaciones posiblemente ilícitas.

[317] Es la excepción recurrente que recorre las Leyes de privacidad de EE.UU. En agitación del fantasma del riesgo a la seguridad. En este caso el ejemplo lo pondríamos en la puesta a disposición de datos bancarios por una entidad fi nanciera al Gobierno por sospechas de acciones terroristas.

[318] § 3403 "Confidentiality of financial records"
La letra c) del precepto ofrece esa inmunidad por responsabilidad civil a las entidades financieras por las derivaciones de tipo penal que pudieran provocarse de sus informes (en lo que se denomina el "Suspicious Activity Report (SAR)" con el departamento de persecución de delitos financieros ("Financial Crimes Enforcement Network (FinCEN)"), lo entendemos desde una perspectiva pragmática donde prima la persecución del delito; si bien pueden generar unos daños particulares (en casos de informes

Se pueden entender, en cuanto a privacidad se refiere, las cautelas en la determinación de este derecho con el ánimo de persecución de posibles delitos fiscales o conductas antijurídicas relacionadas, si bien se observa lo que podríamos denominar "horadación progresiva" del derecho a la privacidad financiera que llega casi a convertirlo en un núcleo jurídico programático. Rasgo que se observa en buena parte de la legislación de la privacidad financiera estadounidense.[319]

Se regula, en entrando en el procedimiento regulado, la autorización directa del titular del derecho para la posible petición de información por la acción gubernamental y su puesta a disposición. La autorización tiene una vigencia que no puede exceder de 3 meses. Puede ser revocada antes de que la información sea puesta a disposición, debe identificar los datos concretos ("financial record") que se autoriza a conocer, y debe especificar el objeto para ello y la autoridad gubernamental al efecto; así como cumplir con los derechos que la Ley protege. No se puede autorizar con ánimo de negocio y el cliente o particular siempre tiene derecho a conocer la información revelada bajo su autorización.[320]

La Ley estipula la acción gubernamental y cuando puede pedir el poder público esta información financiera, así como la regulación de la notificación o petición administrativa o los casos así establecidos por la ley en forma y fondo, y según las determinaciones del artículo.[321]

---

erróneos) que trasladarían la carga de la responsabilidad civil al sector público en vez de a los originarios de esas lesiones (los bancos o entidades financieras).
Básicamente esta modificación de la Ley de 1992 dio al departamento del Tesoro a través de la "Annunzio-Wylie Anti-Money Laundering Act", potestad para adoptar los requisitos para estos "SAR's" que establece unas determinaciones a partir de las cuales las entidades financieras pudieran entender actividad sospechosa de sus clientes en el blanqueo de capitales, estableciéndose el umbral mínimo para "poner la lupa" en las transacciones de al menos 5.000 dólares.

[319] En la sentencia Anderson v. La Junta State Bank (US App. LEXIS 12345 (10th Cir. 1997), (y con la RFPA ya en vigor), entendemos por qué se entra en la consideración de forma de cómo "no seguir" la Ley, siendo la revelación oral de la información financiera igualmente condenable y condenada.

[320] Parágrafo 3404 ("Customer authorizations")
Siempre se habla en la Ley de "customer" o "consumer" y no de ciudadanos (o personas con derechos de categoría más directa). Observándose una privacidad mediata, a través del consumo o la condición de cliente, en estos casos financiero.

[321] §3405 ("Administrative subpena and summons")
Los requisitos formales y de contenido se expresan de una manera bastante descriptiva y pedagógica en

Continúa la Ley con la regulación de las pesquisas criminales, la petición judicial y la forma del requerimiento gubernamental en lo regulado por su objeto jurídico, observándose también una excepción (de mayor lógica por la prevención penal) con autorización judicial, debiéndose informar posteriormente al interesado (o investigado) no más tarde de 90 días o 180 días.[322323]

Para la notificación referida, debemos resaltar otra "horadación" formal en el ejercicio del derecho que establece la Ley, como es el que la misma puede ser demorada siempre que el presidente de una autoridad judicial lo decida y en los casos tasados. Se sigue el criterio de prevalencia de protección de posibles investigaciones penales, pero aquí se da ya por buena también la demora notificativa para el caso de que aquella posible "razonabilidad" se haya hecho plausible por decisión judicial.[324]

El artículo regula todos los aspectos formales de esta demora en la notificación, ya que, al fin y al cabo, es una modificación importante en la formalidad del ejercicio del derecho contemplado. Regula además otra excepción de notificación, cual es la derivada del acceso al "financial record" por razones de emergencia, estableciendo eso sí, la obligación de un histórico de tramitación de estas notificaciones de excepción.[325]

Por último, procedimentalmente la Ley regula la posible "reacción" del consumidor ante esa "horadación" de su derecho. Es la regulación un derecho de revisión a los ejercicios de excepción de su derecho originario.[326]

---

el artículo. Traslada la carga del "opt out" al consumidor. El concepto "razón para creer" ("reason to believe") abre una liberalidad de actuación totalmente discrecional. Y los requisitos para hacer valer el derecho se trasladan a la actuación del individuo, que casi se revela en un derecho proclamado por la adversidad de su ejercicio efectivo.

[322] Parágrafos 3406 a 3408.

El requerimiento judicial ("Judicial subpena") sigue los mismos parámetros que lo visto en parágrafo 3405 para la petición administrativa. Con similares formalidades para las peticiones gubernamentales

[323] En Fisher v. United States, 425 U.S. 391 (1976), tenemos un ejemplo de interpretación constitucional del Tribunal Supremo (en este caso sobre la aplicación de la Quinta Enmienda constitucional) sobre la producción de ficheros con información personal financiera en los procesos judiciales.

[324] §3409("Delayed notice").

[325] Seguimos viendo como la Ley ocupa buena parte de su texto en excepcionar el derecho que genera más que en desarrollarlo.

[326] § 3410 ("Customer challenges").

Se nos presentan aquí sus posibles recursos en favor a su derecho. En un plazo dado de 10 o 14 días ya sea si lo contamos desde la realización o la notificación del acto que se recurre (es decir de la acción judicial o gubernamental de recabación de la información financiera) ("administrative summons or judicial subpoena").

Llama la atención la falta de diferenciación en el ejercicio del derecho en EE.UU. sin atender tanto a la instancia administrativa o judicial, contemplándose jurídicamente de forma más individual que institucional.

En el recurso se debe establecer declaración jurada de ser el afectado o cliente de la institución financiera y dar sus razones o alegaciones, explicando por qué no son relevantes esas informaciones financieras que le conciernen para la legítima ejecución legal de que se trate, o por qué esa puesta a disposición de información no cumple con los requisitos legales.

Si el recurso cumple los requisitos, el tribunal encargado del asunto ordenará a la autoridad gubernamental que responda al mismo, y deberá decidir en 7 días desde esa respuesta. Si el recurso no cumple con los requisitos, el tribunal desestimará el recurso (aquí no se entra tanto en archivo de actuaciones, desestimación o declaración de invalidez del derecho a recurrir. Simplemente si no se cumplen los requisitos del recurso se deniega la pretensión).

En caso de que el tribunal estime el recurso, éste puede, o bien anular la acción, o bien pedir a la autoridad gubernamental contestación escrita.

La decisión denegatoria puede ser blandida en su favor por el consumidor si se ve encausado en base a esa información financiera. Digamos que partiría de un “vicio sustancial” al haber sido recabada contrariando lo establecido por el tribunal que la denegó. En 30 días se debe notificar al interesado por la autoridad que recabó la información, que ninguna acción va a ser entablada contra él en base a esa información para el caso concreto. Si no se hace esto en 180 días, un funcionario de la autoridad de que se trate deberá certificar lo propio (ninguna acción entablada) al tribunal que dictaminó la denegación.

En los preceptos finales la Ley obliga básicamente a las instituciones financieras a tener preparados y a disposición los “financial records” que con validez legal le pida la autoridad pública respectiva.

Regulando el uso permitido con la información recabada. No se pueden transferir los datos a otras agencias gubernamentales a menos que legalmente les sean necesarios para

la ejecución de sus competencias o para casos de inteligencia o los de prevención del terrorismo previstos legalmente.

De ello se debe notificar al cliente financiero o particular cuyos datos se ven transferidos, en un plazo de 14 días y poniendo de relieve la autoridad y para qué se transfieren.Todo ello sin perjuicio de la necesidad de investigación penal y judicial que requieran esa información a las instituciones financieras o Agencias sin más publicidad como es obvio al investigado.[327]

Se encarga La Ley también de los procedimientos especiales. Se sigue el camino de la regulación de las especialidades que afectan al ejercicio del derecho de la Ley. Principalmente razones de seguridad nacional e Inteligencia e investigaciones del FBI, y separadamente casos de emergencia.[328]

Igualmente la letra d) establece en esta misma linea ("Prohibition of certain disclosure") y para esta misma justificación normativa que con carácter discrecional el Director del FBI o delegado por él tengan la posibilidad de prohibir a la institución financiera cualquier comunicación sobre la petición de información

La Ley contiene además la obligación de abonar a la entidad financiera los costes de la colaboración exigida por su estipulado estableciendo la Jurisdicción competente. Contempla además las posibles responsabilidades civiles de autoridades e instituciones financieras por incumplimiento de la misma, así como por daños y perjuicios.[329]

[327] Parágrafos 3410 y 3412

[328] § 3414 ("Special procedures")
El artículo constituye una verdadera regulación especial. Aquí se observa una difuminación acusada de la protección de la privacidad del ciudadano, y ya se observa simplemente un "toma y daca" jurídico entre los servicios de Inteligencia, el FBI y el comité antiterrorista del Congreso, con la obligada colaboración de las instituciones financieras. La justificación legal es para el caso de peligro para seguridad nacional: "a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person"

[329] Parágrafos 3415, 3416 y 3417

3.3.3.2 La RFPA y los Estados.

No se contiene en la Ley determinaciones expresas sobre la aplicación de la misma en los Estados ni sobre la intervención de los Estados en su aplicación. De hecho, no se hace referencia al poder estatal y local en la Ley, ni se considera su aplicación a esos poderes. Tratándose de una Ley que solo afectaría por tanto, a los organismos e instituciones federales.

Lo que sí podremos hacer es un listado de aquellos Estados que tienen una regulación similar a lo estipulado en la RFPA para los órganos federales. Los Estados que han optado por una protección en igual sentido son: Alabama, Alaska, Connecticut, Illinois, Louisiana, Maine, Maryland, New Hampshire, North Carolina, North Dakota, Oklahoma, Oregon, Utah y Vermont.

Florida y Massachusetts se han dotado de legislaciones de protección adicional a la establecida en la RFPA ya que entran a regular en mayor calado los sistemas de transferencia financiera electrónica.[330]

[330] Observamos aquí una indeseable asíntonía de derechos en privacidad financiera y en sus relaciones con el poder público, dependiendo de la Autoridad con la que el ciudadano estadounidense vea gestionados sus datos. Discordancia que en Europa no se produce, ya que, si bien en la figura de la Directiva pudiera darse temporalmente por falta de trasposición (sometida a sanción), la asunción en Reglamento de la protección de datos, impide de manera definitiva esa discordancia observada en el derecho de privacidad financiera estadounidense. Donde por ejemplo los ciudadanos de un Estado tan importante como California o de otro como Minsesota, se ven en una protección inferior ante sus autoridades estatales y locales.

3.3.4 Identity Theft Assumption and Deterrence Act de 1998.

Es una de las Leyes, junto con la RFPA, que se encarga de la protección de la privacidad financiera desde el prisma de la defensa contra la intromisión gubernamental en la misma, y se encuentra contenida en el título18 del U.S.C., parágrafo 1028 bajo el enunciado *Fraud and related activity in connection with identification documents, authentication features, and information*.

Los que con conocimiento falseen de alguna u otra manera la identificación de otra persona (en forma de documento o firma supuestamente auténtica), la roben, la transfieran, trafiquen con ella o la posean con intenciones ilegales (cinco o más de estas identificaciones), estarán bajo su ámbito subjetivo de actuación.

En estos supuestos la norma hace distinciones en función del objetivo que persigan esos posibles infractores, ya sea el de fraude en los Estados Unidos, o bien el de la producción de documentos falsos o en los casos en que se prevea sean utilizados en eventos de especial significancia nacional o para violar una ley federal.[331]

Las circunstancias (letra c) en que debe producirse la actuación ilegal referida, nos habla de aquella identificación en la que parezca jugar el poder público americano, sin llegar a afirmar que se traten solo de casos de falseamiento de documentos públicos. O bien se trate de una ofensa de la que pueda causar fraude a los Estados Unidos (punto 4 de la letra a), o bien que afecte al comercio interestatal o extranjero, o implique la utilización del correo.[332]

Los castigos a estas ofensas van desde multas hasta penas de prisión de hasta 30 años (con escalas en 5, 15 y 20 años y reservada la mayor para aquellas falsificaciones que hayan podido facilitar actos de terrorismo).[333]

[331] Letra a) que se encarga de establecer los sujetos de la Ley en base a las circunstancias de la letra c)
[332] Creando un tipo agravado de comportamiento ilegal en la esfera del fraude público
[333] Letra b del precepto.
Distinguiendo del tipo de documento objeto de falsificación (documento de identificación, certificado de nacimiento...), así como del hecho de la infracción (falseamiento, transferencia, posesión), su número (más o menos de 5) o el fin para qué se hayan utilizado.

La letra d) se encarga, por último, de ofrecer claves definitorias para la aplicación de la Ley.

Vemos una Ley que está dentro de la esfera de la defensa de la privacidad, pero que es una auténtica disposición penal para la persecución de falsificación de documentos personales o actos de manifestación de voluntad personal, de suplantación de la personalidad al fin, y que lleven implícitos el "respaldo" público de la autoridad estadounidense.[334]

En este sentido conviene recordar el Acuerdo entre la Unión Europea y los Estados Unidos relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la financiación del Terrorismo (*Terrorist Finance Tracking Program*), conocido como "Acuerdo SWIFT" (Santos Vara, 2012), y que resumidamente diremos que permitía la entrega a los EE.UU. de los datos de mensajería financiera sobre transferencias financieras almacenados en el territorio de la Unión Europea por los proveedores de servicios de mensajería financiera internacional. Este Acuerdo ha sido suspendido por el Parlamento Europeo, poniendo de relieve la incidencia político-jurídica que las revelaciones de Edward Snowden pusieron sobre el tablero en las relaciones Europa-Estados Unidos.[335]

[334] En este sentido es de interés el artículo de Solove, (2003: 12-16). En el cual se realiza un análisis crítico sobre el acercamiento al problema desde la mera perspectiva sancionadora, siendo más bien un problema de construcción y de "arquitectura" en el diseño del sistema de privacidad que provoca vulnerabilidad y facilita el robo de identidad. Proponiendo un "sistema arquitectónico" de mejores y más justas prácticas y políticas de privacidad.

[335] En este sentido ver la Resolución del Parlamento Europeo, (2013), sobre la suspensión del Acuerdo TFTP a raíz de la vigilancia de la NSA (2013/2831(RSP)), siendo de especial interés su considerando J punto 5 en el que el Parlamento Europeo: " *Insiste en la necesidad de que todos los acuerdos sobre intercambio de datos con los EE.UU. se basen en un marco jurídico para la protección de datos coherente que ofrezca normas para la protección de datos personales que sean jurídicamente vinculantes, en particular en lo que se refiere a la limitación de los fines, la reducción al mínimo de los datos, la información, el acceso, la corrección, la supresión y la reparación* ..."

CAPÍTULO TERCERO

LA PRIVACIDAD Y SU ENCAJE CON EL *LAW ENFORCEMENT* Y LA SEGURIDAD NACIONAL.

La relación tensa entre privacidad y seguridad es una constante que se da en las sociedades democráticas occidentales de manera persistente. EE.UU. no solo no es una excepción sino quizá uno de los más ilustrativos ejemplos de esa complicada relación, que es, al fin, la pugna ente ejercicio de un derecho y sus límites.

En este apartado de la parte americana del trabajo analizamos cómo se soluciona en el Derecho estadounidense el encaje de la privacidad con las exigencias de la ejecución de la Ley y la actuación de la autoridad pública (concepto que el idioma inglés en su gran virtud de concreción lingüística resume en "Law Enforcement"), así como el engranaje de aquella en las determinaciones de la Seguridad Nacional y los asuntos de "Inteligencia Extranjera".

Al igual que en el estudio de la relación de la privacidad con el consumo, y que forma la otra gran relación jurídica de esta en EE.UU. (si bien en aquel con el enfoque en el mercado y el poder privado y empresarial), en este otro gran pilar de matización y limitación de la privacidad individual nos adentramos en el sentido "orwelliano" de la misma, pasando a estudiar como el "Big Brother" estatal (o federal) vigila a los estadounidenses (y a los que no lo son), y el derecho que se esgrime en estos casos. Es decir, dentro de las vertientes ficcionadas pero pragmáticas que hemos creado en la diferenciación de defensa de la privacidad estadounidense, esta sería la vertiente que le corresponde al estadounidense como ciudadano (en su exposición al poder público como garante del orden público y de la vigilancia que ello conlleva).

En esta sección debemos distinguir, por un lado las estipulaciones constitucionales generales al respecto, como es la previsión constitucional de la Cuarta Enmienda (y también en menor medida de la Quinta), que se utiliza y se puede utilizar para la defensa de la privacidad ante la intromisión del poder público; y por otro lado, la construcción legal (*Statutory Law*) en varias importantes normas de tal rango que determinan la privacidad en este ámbito. Además de una construcción jurisprudencial que se imbrica en el desarrollo e interpretación de ambas, y que en este caso cobra especial relevancia (a la habitual americana) siendo, por tanto, germen y molde de este sistema de protección de la privacidad.

1. La previsión constitucional

1.1 La protección de la Cuarta Enmienda

La Cuarta Enmienda a la Constitución de los Estados Unidos tuvo en su creación, y tiene por objeto en su actual ejecución, la defensa del ciudadano ante intromisiones injustificadas del poder público en su persona, casa y efectos personales. Es el derecho a la Intimidad personal en su acepción general, y es la norma constitucional que limita y rige el poder de investigación del Gobierno y de sus funcionarios y empleados públicos.

Su redacción es la siguiente: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*" Es la vieja acepción jurídica de "la casa de cada hombre como su "castillo"".[336]

Debemos tener en cuenta que la comparativa europea se ve en este caso alejada propiamente del Reglamento Europeo de Protección de Datos de 27 de abril de 2016, que no recoge en su objeto la intimidad personal como derecho regulado en sentido amplio y propiamente, sino la gestión y protección de los datos personales de los europeos. No está por tanto en su ámbito de aplicación material el tratamiento de datos personales en el ámbito de la seguridad pública. En este caso la norma europea de

[336] En su traducción (propia) "El derecho del pueblo a estar seguro en sus personas, domicilios, papeles y efectos se hallen a salvo de registros y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con precisión el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas."

referencia comparativa es la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016.[337]

La Cuarta Enmienda, y seguimos aquí a Solove & Schwartz, (2015, 260-264) se divide en su estudio jurídico en tres partes:

1. La de su aplicabilidad, es decir la respuesta a la pregunta de cuándo opera.

2. La de la determinación de cuando es razonable "a search or seizure", entrando aquí en juego la doctrina de la "causa probable" y la garantía judicial.

3. Y la de cómo se hace efectiva, siendo aquí determinante la doctrina conocida como "Exclusionary Rule", o la de no hacer valer la prueba obtenida en su violación.

En cuanto a la aplicabilidad, la Cuarta Enmienda se aplica a todos los funcionarios y empleados públicos. A todos los agentes del Gobierno (no solo a la policía), cuando ejerzan esas tareas sobre las personas, documentos o cosas. Por lo que deberemos responder a qué se refiere en su objeto jurídico, es decir que se entiende por "search" y por "seizure" (las investigaciones y las incautaciones o requisas). Para ello, la construcción jurisprudencial ha sido vital, estableciendo "la prueba de expectativa de privacidad razonable".

Por "causa razonable" básicamente se entiende aquella que aprecie un Juez mediante una orden judicial ("warrant") entendiendo que los "indicios razonables" de la policía se puedan transformar en mandato judicial.[338]

Incluso obteniendo esas órdenes ("warrants"), algunas intromisiones pueden considerarse como "no razonables", como así establece el Tribunal Supremo en

[337] En su artículo 2. 2 letra d) "El presente Reglamento no se aplica al tratamiento de datos personales:
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."
Siendo la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[338] En este sentido las sentencias del Tribunal Supremo Brinegar v. United States 338 U.S. 160 (1949) y Wong Sun v. United States 371 U.S. 471 (1963)

"Winston v. Lee 470 U.S. 753 (1985)". Además, los objetivos y personas de esas órdenes judiciales han de ser circunscritas y no amplias y generales, siguiendo la literalidad de la Cuarta Enmienda. Si bien y en sentido contrario, hay pesquisas en las que se puede excepcionar esa necesidad de "warrant" debido a las circunstancias. Como para aquellos casos que pudieran hacer inútil o impracticable el mandato judicial. Sería la excepción de las necesidades especiales ("Special Needs"), construida igualmente por la Jurisprudencia del Tribunal Supremo.[339]

Para su efectiva aplicación tenemos básicamente la "Exclusionary Rule" y la posibilidad de solicitar indemnización por responsabilidad civil. La incapacidad de utilizar la prueba obtenida ilegalmente en los procesos penales ("Exclusionary Rule") se manifiesta judicialmente a principios del siglo XX por el Tribunal Supremo en "Weeks v. United States 232 U.S. 383 (1914)", con el objetivo de impedir que los empleados públicos contravengan la Constitución, así como en los años 60 en "Mapp v. Ohio 367 U.S. 643 (1961)", en la que se añade que aquella prueba que traiga causa de la originalmente ilegal también se suprimirá como tal. En lo que se conoce como la doctrina "de la fruta del árbol envenenado." La segunda forma para su aplicación es la de la indemnización civil, siguiendo lo establecido en la codificación americana para esa posibilidad.[340] (Solove & Schwartz, 2015, 263-264)

[339] O'Connor v. Ortega 480 U.S. 709 (1987) y Terry v. Ohio 392 U.S. 1 (1968)

[340] Título 42 del USC en su parágrafo 1983.

Debemos añadir por último la distinción procesal entre "Subpoenas" y "Cort Orders" en esos mandatos judiciales y que son diferentes de las "warrants". Algo así como diferencia entre una citación y una orden (en las formas respectivas) que son dos maneras adicionales (además del mandamiento de la "warrant"), en que puede autorizarse al Ejecutivo por el Poder judicial estadounidense.

La diferencia entre ellas es que en el caso de "warrant" el mandato judicial se fundamenta directamente en la Cuarta Enmienda, y requieren de "probable cause" y tienen prevalencia. Mientras que los "Court orders" han de venir avaladas y contenidas en un precepto legal sin que sea necesario ese estándar de "causa probable", y se dan en aquellas situaciones en que no se aplica la Cuarta Enmienda. Las "subpoenas" o citaciones se utilizan para las testificaciones o la obtención de documentos, teniendo además una versión puramente administrativa, si la Ley otorga esa capacidad a las agencias federales respectivas.

1.2 La interpretación jurisprudencial de la Cuarta Enmienda

Debemos partir de que al tiempo de aprobarse y promulgarse la Cuarta Enmienda, la intromisión en la privacidad (intimidad) era principalmente violenta y por mediación de fuerza más bien física. Los elementos de escucha se consideraban anecdotarios, y el objeto de la adición constitucional era principalmente evitar intromisiones en los domicilios privados y la aprehensión de efectos personales.

Sería con la invención del telégrafo en 1844 y la del teléfono en 1876 cuando las comunicaciones empiezan a conformarse en el sentido en que nos llegan hasta nuestros días, así como en sus implicaciones para la privacidad. Así, el uso de instrumentos y artilugios para la captación de comunicaciones de telégrafo se dio por primera vez en EE.UU., durante su guerra civil, y la efectuada por la policía en 1890. Y ya entrado el siglo XX se generaliza este tipo de investigación, sobre todo para controlar protestas y acciones obreras en los centros industriales, el control interior durante la Primera Guerra Mundial, o la persecución del contrabando de alcohol durante los años de la Prohibición. Observamos aquí como se va perfilando el marcado carácter de control social que este tipo de actuaciones conlleva, y cómo, ya en sus inicios, se observa el mismo criterio que se consolidaría con los años (Lane, 2009).[341]

Es por ello que la continua interpretación jurisprudencial será el elemento determinante que va construyendo la aplicación de la Cuarta Enmienda en torno a la privacidad individual estadounidense.

Así, analizaremos las principales sentencias que tienen contenido esencial en este sentido.

[341] Para la perspectiva histórica de la evolución del derecho recomendaremos a Smith (2004).

1.2.1 Limitaciones de la Cuarta Enmienda. Ejemplos.

Citaremos dos célebres sentencias del Tribunal Supremo estadounidense que nos sirven de paradigma en la limitación de la Cuarta Enmienda para entrar a prestar un juego válido general de protección a la privacidad, como son el caso Olmstead v. United States y el asunto Hoffa v. United States. Ambas curiosamente relacionadas con la persecución de las actividades del hampa.

En la primera[342] se nos presenta la historia del señor Olmstead, que era un conocido traficante de alcohol de la costa oeste (conocido como "Rey de los contrabandistas") durante los años de la Gran Depresión, cuya actividad salió a la luz en base a unas escuchas policiales por parte de los agentes especiales designados para su persecución. Las captaciones se hicieron desde los postes de teléfono que se encontraban en el exterior de la propiedad de Olmstead, que reclamaba su nulidad. El Tribunal Supremo en un controvertido pronunciamiento no expande la protección de la Cuarta Enmienda a los cables telefónicos y elementos situados fuera de la casa del individuo, estableciendo que se requería un pronunciamiento legislativo del Congreso para establecer esas escuchas. De esta sentencia, por tanto, surge buena parte de la legislación que veremos en este bloque, al requerirse por el Supremo esta específica habilitación legal, y al no operar así en estos casos plenamente la protección de la Cuarta Enmienda.[343][344]

Hablamos de controvertida sentencia por el famoso voto particular contenido en ella del no menos famoso Juez Brandeis, coautor del artículo que inicia el estudio de la protección jurídica de la privacidad en EE.UU., y que 40 años después vuelve a cobrar protagonismo. En su voto disconforme advierte de manera premonitoria de los peligros que en el futuro acecharán sobre la privacidad de los ciudadanos por parte de los

[342] Olmstead v. United States 277 U.S. 438 (1929)
[343] Ver Hamm (2010)
[344] Nos lo dice así la sentencia "…*Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials by direct legislation and thus depart from the common law of evidence. But the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment*…"

poderes ejecutivos, asumiendo que la protección de la Cuarta Enmienda es mucho más amplia que la interpretación que de ella hace la sentencia.[345]

Es por tanto consecuencia directa de esta sentencia la aprobación legal en 1934 del parágrafo 605 de la *Federal Communications Act* que incluía las escuchas sin autorización como crimen federal. Y que es anticipo y precedente legislativo de las leyes que veremos en esta sección del trabajo.

En la segunda sentencia[346] se da un caso de tipo y con resultado contrario al anteriormente visto en "Olmstead". En este caso un informante de la policía revela contenidos de conversaciones mantenidas con el famoso capo (conocido más por Jimmy que por James) en su antigua y habitual relación de amistad. El Tribunal establece que en este caso no opera la Cuarta Enmienda ya que, a pesar de que se encontraban en el domicilio habitual de Hoffa (la suite de un hotel), la información que revela se produjo con una previa invitación a entrar en la habitación y dirigida a él. Es decir, que no estaba escuchando, por así decirlo, escondido en un armario y habiendo entrado a la habitación por la fuerza o sin permiso (en este caso además no hay grabaciones o elementos de captación de por medio)[347]

[345] Voto particular que primero diferencia los tiempos de la Enmienda y de la sentencia "*…But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet…*"
Y luego los tiempos que están por venir, así como la más amplia validez de la Cuarta y Quinta Enmienda: "*…The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth…*"

[346] Hoffa v. United States 385 U.S. 293 (1966)

[347] Otro caso similar se da en Lewis v. United States 385 U.S. 206 (1966) para el caso de un traficante de drogas.

Vemos así que estas dos sentencias (Olmstead y Hoffa) excluyen de la aplicación de la Cuarta Enmienda al interés de privacidad mantenido en el entorno de "lealtad entre amigos".

Siendo de utilidad para este caso la reflexión al respecto en Amsterdam (1974, 407) cuando nos dice que "la única diferencia es que estar bajo vigilancia electrónica uno tiene miedo de hablar en la oficina o por teléfono mientras que estar bajo un sistema "espía" uno tiene miedo de hablar con cualquiera".

1.2.2 La evolución jurisprudencial oscilante y la importancia de los votos particulares

El Tribunal Supremo ha ido elaborando una serie de pronunciamientos con la Cuarta Enmienda y la privacidad como protagonistas que han oscilado en cuanto a su proyección de protección, y que no han dibujado una línea clara de seguimiento (atendiendo más al caso juzgado que a la construcción de una protección general sobre privacidad). Línea sobre esa protección de la privacidad y su conexión a la Cuarta Enmienda que sí podemos entrever más coherente en sus votos particulares, recurrentemente manifestados por algunos jueces con una visión pertinaz al respecto.

En este apartado podemos empezar con la sentencia López v. United States[348], en la que el señor López es juzgado debido a unas escuchas tomadas desde una grabadora que llevaba en el bolsillo un agente del departamento de Hacienda, al que trataba de sobornar. El alto Tribunal estadounidense, en otra controvertida sentencia, establece que el riesgo del demandante al ofrecer un soborno, incluía el riesgo de que ello fuera reproducido ante un Tribunal por el funcionario, también en manera de grabación mecánica.[349]

[348] López v. United States 373 U.S. 427 (1963)

[349] Dice el Tribunal: *"…We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording…"*

Y hablamos de controversia por sus disentimientos que, como en el caso Olmstead, ofrecen una visión de protección de la privacidad y su extensión constitucional, mayores que las de la sentencia.

Así el Juez Brennan, secundado por los Jueces Douglas y Goldberg, critica que esta protección sea tan variable en función de la forma, y sobre todo, que se asimile a una conversación normal ya que ese posible riesgo de creer ser grabado implicaría estar callado en todo momento.[350]

Argumentándolo de manera profética ya que el riesgo no es igual en caso de que entren en juego elementos de grabación o electrónicos o no.[351]

Por tanto en esta sentencia se produce un cambio de postura del Tribunal con respecto al pronunciamiento Olmstead, (más garantista), que si bien se sigue reivindicando en estos votos particulares de la propia sentencia.

Otro asunto es el de Katz v. United States,[352]sentencia clave en esta conexión de la privacidad con la Cuarta Enmienda, en la que unos agentes del FBI consiguen, a través de escuchas electrónicas que se utilizan como prueba, la condena del acusado en un tribunal californiano. El señor Katz apela, y el caso llega al Supremo. Su apelación se basa en que aquellas pruebas fueron captadas en una cabina telefónica y la determinación si ese lugar se puede considerar un "área protegida constitucionalmente" o no y su consiguiente invasión de privacidad en base a la Cuarta Enmienda.

En la sentencia el Tribunal hace algunas consideraciones previas sobre el carácter de la Cuarta Enmienda y su carácter trascendente al derecho de privacidad. La conciben

---

[350] *"…It is the risk that third parties, whether mechanical auditors like the Minifon or human transcribers of mechanical transmissions as in On Lee—third parties who cannot be shut out of a conversation as conventional eavesdroppers can be, merely by a lowering of voices, or withdrawing to a private place—may give independent evidence of any conversation. There is only one way to guard against such a risk, and that is to keep one's mouth shut on all occasions…"*

[351] *"…The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak. But as soon as electronic surveillance comes into play, the risk changes crucially. There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy.*
(...) Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny…"

[352] Katz v. United States 389 U.S. 347 (1967)

como una previsión constitucional de interdicción de la intromisión de los gobiernos, sin que ello tenga que ver necesariamente con temas de privacidad o protección de datos. Así como la consideración de su carácter federal.[353]

La sentencia continúa en un hito de superación de otros precedentes judiciales (como la sentencia Olmstead) para establecer que aquella doctrina del "traspaso" de la propiedad estaría superada (sobre todo en base a la discusión en torno a la cabina telefónica y su carácter). Y ello para ubicar la atención en si las pesquisas e incautaciones han seguido los criterios constitucionales. Asume, y de ahí gran parte de su importancia, la era electrónica en la vigilancia estatal.[354]

Tiene en cuenta que esas interceptaciones se hicieron por agentes no judiciales y sin la aprobación de un Juez, y no cumplieron el criterio de "razonabilidad de privacidad", cuya prueba es la principal aportación de la sentencia para la historia jurídica de la aplicación de la Cuarta Enmienda en materia de privacidad.[355]

Tiene así desarrollo esta "prueba de expectativa razonable de privacidad" en la opinión concurrente del Juez Harlan presentada a la sentencia. Que se basa, primero, en que una persona ha de manifestar una expectativa real de privacidad (como lo era el estar en una

[353] Así lo estipula la sentencia: "…*We decline to adopt this formulation of the issues. In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy -- his right to be let alone by other people is, like the protection of his property and of his very life, left largely to the law of the individual States..."*

[354] "*We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.*
The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards."

[355] "*…Over and again, this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well delineated exceptions*".

cabina), y segundo, en que esa expectativa ha de observarse como "razonable" por la sociedad.[356][357]

En el caso de United States v. White[358] se trata de dilucidar si la Cuarta Enmienda suprime la prueba obtenida del testimonio de unos agentes del gobierno que informan de ciertas conversaciones que se dieron entre el señor White y un informante del gobierno, Harvey Jackson, a través de captaciones de radiofrecuencia, de las que cuatro de ellas, tuvieron lugar en la casa de Jackson y con el consentimiento del mismo.

En esta ocasión volvemos a aquellos "riesgos" del que comete actividades ilegales del caso López. Así como la situación de privacidad en los entornos de amistad de aquel pronunciamiento. Utiliza en mayor medida este precedente que el anterior de Katz e implica la sentencia una vuelta del péndulo hacia la prevalencia de la seguridad.[359]

En esta sentencia vuelve a tomar relevancia la voz del Juez Harlan (garante de la parte del péndulo en su lado de la privacidad o intimidad), esta vez con una voto particular o disidente, abogando por un sistema de protección de la privacidad ciudadana integral que requiera siempre de mandato judicial.[360]

---

[356] "*MR. JUSTICE HARLAN, concurring (…) As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."*

[357] Igualmente y en la misma línea sigue a este pronunciamiento Katz la sentencia del Tribunal Supremo Berger v. New York 388 U.S. 41 (1967), si bien poniendo más el foco jurídico en la necesidad de un mandato judicial ("warrant").

[358] United States v. White 401 U.S. 745 (1971)

[359] "…Our problem, in terms of the principles announced in Katz, is what expectations of privacy are constitutionally "justifiable" -- what expectations the Fourth Amendment will protect in the absence of a warrant. (…) Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end, or never materialize.(…)
Considerations like these obviously do not favor the defendant, but we are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question."

[360] "*The critical question, therefore, is whether, under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement (…)*
Interposition of a warrant requirement is designed not to shield "wrongdoers," but to secure a measure of privacy and a sense of personal security throughout our society.
The Fourth Amendment does, of course, leave room for the employment of modern technology in criminal law enforcement, but in the stream of current developments in Fourth Amendment law, I think it

La sentencia Smith v. Maryland[361]resulta importante por establecerse en ella la doctrina conocida como "The Third Party Doctrine", que se caracteriza por mantener que el hecho de dar información a terceros de manera voluntaria deja escapar las "expectativas razonables de privacidad". La sentencia, que se apoya mucho en su justificación en la anterior del caso Katz, es reflejo del oscilante, y poco homogéneo (al igual que en la Ley escrita) parecer del Tribunal Supremo en su consideración de la privacidad en su relación con las exigencias de la seguridad, y que venimos observando.

Autores como Bellia (2004) ponen de relieve la contradicción y conflicto entre las sentencias que estamos estudiando.

En este caso se presenta la instalación de un "pen register" para grabar los números y conversaciones mantenidas por Michael Lee Smith, un ladrón que entró en casa de Patricia McDonough y a la cual realizaba llamadas intimidatorias con el objeto de que no prestara testimonio de haberlo identificado. La policía ordena a la compañía de teléfono las escuchas y empieza nuestro caso.

La sentencia va justificando su apartamiento de la de Katz en los distintos medios empleados en ambas, quitando las "oficinas telefónicas" de la prueba de expectativa razonable" dentro del ámbito de protección constitucional.[362]

Si bien en este pronunciamiento judicial vuelven a ser también sus votos discordantes de más interés, para el estudio de la protección de la privacidad, que el resultado del mismo. Los Jueces Stewart, secundado por el incasable Brennan, y Marshall, igualmente secundado por Brennan, presentan sendos votos particulares, advirtiendo de los peligros de la falta de mandato judicial para estos casos. Critican esa "asunción de riesgo" que se traslada a las conversaciones telefónicas con terceros.[363]

---

must be held that third-party electronic monitoring, subject only to the self-restraint of law enforcement officials has no place in our society…"

[361] Smith v. Maryland 442 U.S. 735 (1979)

[362] *"…This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial…"*

[363] *" …The crux of the Court's holding, however, is that whatever expectation of privacy petitioner may in fact have entertained regarding his calls, it is not one "society is prepared to recognize as reasonable.'". In so ruling, the Court determines that individuals who convey information to third parties have "assumed the risk" of disclosure to the government (…)*

The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those

La doctrina ofrece extensivas interpretaciones de las repercusiones de esta sentencia y de la "Third Party doctrine". Entre las que nos parecen más interesantes hablaremos que, por causa de ella (y también por el caso Miller) Solove (2002) lo fija en la pérdida de capacidad de la Cuarta Enmienda para limitar la recopilación de información de las empresas por parte del Gobierno. Con todas las enormes implicaciones que ello está conllevando.

Por último citaremos la sentencia California v. Greenwood,[364]llamativo caso en el que se trata el asunto de los objetos abandonados o expuestos al público y sus implicaciones de privacidad.

La familia Greenwood deja en los contenedores a las afueras de su casa su basura, algo bastante habitual. Si bien en una de las bolsas, que además es transparente, se encuentran restos de droga por parte de unos agentes, que para este caso se ganaron a pulso el apelativo de "sabuesos". Esos policías, tras rebuscar y encontrar aquello en la basura, consiguieron una orden judicial para registrar la casa.

Los Greenwood acuden a los Tribunales y acaba pronunciándose el Supremo sobre su reclamación a la Cuarta Enmienda. El resultado no les fue satisfactorio estableciendo la sentencia la legalidad de las búsquedas de los agentes en la basura. Se interpreta que la familia había "expuesto" lo suficiente su basura al público, en un área muy adecuada a esa inspección pública, como para reivindicar la garantía constitucional.[365]

Ahora bien, también en esta sentencia lo que nos parece más interesante para la protección de la privacidad son sus votos particulares. Y de nuevo el del Juez Brennan apoyado en esta ocasión por el Juez Marshall. Expresándolo poéticamente, al decir que el "escrutinio en basura ajena es contrario a las comúnmente aceptadas nociones de

---

with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."

[364] California v. Greenwood 486 U.S. 35 (1988)

[365] "*…Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection…*"

comportamiento civilizado.” Y cita el precedente de un caso similar (Caso Jacobsen) en el que la diferencia estaba en la opacidad de las bolsas de basura, impugnando de manera respetuosa el contenido de la sentencia.[366]

1.2.3 Últimos pronunciamientos relevantes.

A finales del siglo pasado y a lo largo de este podremos destacar algunas sentencias relevantes sobre la privacidad y la Cuarta Enmienda, que siguen sin marcar un criterio claro y uniforme de protección, si bien nos ofrecen una imagen última de esa evolución.

Así en la sentencia Florida v. Riley[367]a finales de los 80 en el condado de Pasco en Florida, el Sheriff sospecha de las actividades que se pueden estar cometiendo en el interior de una casa. Principalmente sospecha del cultivo de marihuana en su interior, debido a que hay un invernadero en ella, cubierto por plásticos que hacen imposible la visión de su interior desde la calle. En su investigación utiliza un helicóptero para conseguir captar pruebas desde arriba y ve, a simple vista (desde 400 pies), que se trata de una plantación de marihuana. El señor Riley (jardinero e inquilino en esta historia) reclama su derecho reconocido en la Cuarta Enmienda sin que el Tribunal Supremo se lo conceda. Ya que no podía esperar “razonablemente” que su cultivo no fuera visto desde el aire por agente de policía. Sin grabaciones, sin molestias o ruidos indebidos

[366] *“…“Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior. I suspect, therefore, that members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public (…)*
Our precedent, therefore, leaves no room to doubt that, had respondents been carrying their personal effects in opaque, sealed plastic bags -- identical to the ones they placed on the curb -- their privacy would have been protected from warrantless police intrusion. So far as Fourth Amendment protection is concerned, opaque plastic bags are every bit as worthy as "packages wrapped in green opaque plastic" and "double-locked footlocker[s]”.
Respondents deserve no less protection just because Greenwood used the bags to discard, rather than to *transport, his personal effects. Their contents are not inherently any less private, and Greenwood's decision to discard them, at least in the manner in which he did, does not diminish his expectation of privacy…”*
[367] Florida v. Riley 488 U.S. 445 (1989)

relacionados con su hogar. No encontrando así violación de su derecho contenido en la Cuarta Enmienda.[368]

Y volvemos de nuevo a nuestros conocidos disidentes en pos de la privacidad. El Juez Brennan acompañado de Marshall y esta vez además junto al Juez Stevens, vuelven a disentir del pronunciamiento desde posiciones defensivas de la privacidad. Hablan de que la sentencia ignora la verdadera esencia del asunto Katz, atacando la interpretación de sus compañeros de órgano. Y reclaman la libertad ante esa seguridad omnipresente. Recurren directamente y expresamente al "Big Brother" de Orwell, siendo citado literalmente el autor británico y su libro 1984 (en consonancia con el momento y década en que se dictó la sentencia)[369]

La sentencia, y sobre todo sus disentimientos, tienen especial validez y actualidad a día de hoy. En mayor medida al pensar en el mundo de "drones" que se está desarrollando o en el control omnipresente de las cámaras de seguridad o vigilancia que pueblan la casi totalidad de los espacios públicos urbanos, que llegan ya a sistemas de reconocimiento facial.

Por otro lado, en la sentencia Kyllo v. United States [370]sigue la atención jurisprudencial del Supremo en temas de vigilancia. Y aquí, volvemos a un asunto de plantación de marihuana en el interior de una vivienda. Es conocido, según la sentencia, que el cultivo interior de esta planta requiere lámparas de alta intensidad, que producen un calor anormal. Así la casa del señor Kyllo fue "escaneada" termalmente por la policía, desde el asiento del copiloto de un coche de los investigadores, situado enfrente del domicilio

[368] *"…Riley could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft..."*

[369] *"…The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use. I hope it will be a matter of concern to my colleagues that the police surveillance methods they would sanction were among those described forty years ago in George Orwell's dread vision of life in the 1980's:*
"The black-mustachio'd face gazed down from every commanding corner. There was one on the house front immediately opposite. BIG BROTHER IS WATCHING YOU, the caption said. . . . In the far distance, a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows."
G. Orwell, Nineteen Eighty-Four 4 (1949)
Who can read this passage without a shudder, and without the instinctive reaction that it depicts life in some country other than ours? I respectfully dissent."

[370] Kyllo v. United States 533 U.S. 27 (2001)

y durante pocos minutos. De ello surgió la comprobación de que en algunas zonas de la casa el calor era muy intenso, aprobándose una orden judicial para entrar a la casa, que al final, albergaba más de 100 plantas de marihuana.

El señor Kyllo reclamó con las mismas motivaciones que hemos vistos en anteriores sentencias su derecho a la Cuarta Enmienda, y al contrario que en otra sentencia con este tipo de vigilancia operando (Dow Chemichal Co. v. United States 476 U.S. 227 (1986)), se considera que el uso de esta "vigilancia térmica" sí comprometía el derecho contenido en la Cuarta Enmienda. Lo considerán, por tanto, "a search" que requería mandato judicial previo (sobre todo por los medios utilizados no comunes ni accesibles).[371]

La sentencia, sin embargo, no se libra de votos disconformes que ofrecen una interpretación más garantista y protectora de la privacidad que la del alcance del fallo, a pesar de reconocer éste la violación de la Cuarta Enmienda. Se da por el Juez Stevens al que se unen los Jueces Rehnquist, O'Connor y Kennedy. Critican que la sentencia habla de adoptar una postura mirando al largo plazo, cuando la realidad del uso de la tecnología va superando esa visión tan rápidamente mientras se va haciendo accesible al gran público, siendo esta vigilancia realmente característica de una "desnudez ciudadana" (comillas mías) sin garantías.

Por último citaremos la sentencia de 2012 United States v. Jones[372] en la que se viene a dar la razón de la violación de la Cuarta Enmienda al señor Jones, propietario de un club nocturno al que se le investigaba por asunto de drogas y al que se le instala un GPS en su coche. De esa investigación resulta culpable de un delito de tráfico de estupefacientes, si bien su vehículo se muestra como un efecto personal indudable para el Alto Tribunal. La autorización judicial para la instalación de GPS lo era por 10 días y para el Estado de Columbia, resultando la prueba obtenida en el undécimo día desde la aprobación de la instalación y en el Estado de Maryland.

[371] *"…Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant…"*

[372] United States v. Jones 132 St. 945 (2012)

En otras sentencias el Supremo se va pronunciando abiertamente sobre los temas relacionados con la aparición de nuevas tecnologías y su uso generalizado como es el caso del "Global-Positioning-System" (GPS), y su relación con la Cuarta Enmienda. Ejemplo de ello lo tenemos en esta sentencia *Jones* donde se presentan de especial interés algunas consideraciones y reflexiones jurídicas manifestadas en votos concurrentes por sus Jueces.

La de la Jueza Sotomayor viene a expresar con fino acierto la matización y condición de la privacidad del ciudadano medio en el uso extendido de esas tecnologías, como la de los "GPS".[373]

Pero sobre todo se presenta de gran altura jurídica las palabras del Juez Alito secundado por los Jueces Ginsburg, Breyer y Kagan, que reflexionan sobre esas teconologías, como los smartphones y similares.[374]

La sentencia, además, parece ofrecer un nuevo sentido al péndulo de la interpretación jurisprudencial del Supremo sobre la relación de la privacidad y la Cuarta Enmienda, ofreciendo una nueva consideración sobre la posibilidad de que "la expectativa razonable de privacidad" pueda reconocerse en los lugares públicos.

---

[373] Citaremos algunas palabras*:" I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.*"

[374] Nos lo dicen así: "*Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.*
Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements."

1.3 La protección de la Cuarta Enmienda cuando vienen implicadas actividades protegidas por la Primera Enmienda.

Debemos en este punto hacer una distinción para resaltar y distinguir aquella construcción jurisprudencial sobre la aplicación y protección de la Cuarta Enmienda de la privacidad cuando venga implicada en situaciones que refieren y evoquen la Primera Enmienda constitucional estadounidense. Seguimos en el debate de los límites entre derecho y necesidades de la realidad, o en este caso concreto, con la libertad de expresión en el foco de atención, en el debate de las limitaciones entre derechos y libertades y sus respectivos ejercicios.

La Primera Enmienda nos dice literalmente que: "El Congreso no podrá hacer ninguna ley con respecto al establecimiento de la religión, ni prohibiendo la libre práctica de la misma; ni limitando la libertad de expresión, ni de prensa; ni el derecho a la reunión pacífica de las personas, ni de solicitar al gobierno una compensación de agravios."[375]

La Primera Enmienda recoge, por tanto, los derechos constitucionales clásicos de la Libertad de Creencias y Religión, así como el de Libertad de Expresión, de Prensa o al Derecho de Asamblea o Reunión y el Derecho de Petición.

Por lo tanto, podemos inferir que existen muchas actividades concernientes a la privacidad que vienen protegidas por la Cuarta Enmienda para sus pesquisas e incautaciones, que pueden implicar una intromisión añadida a las previsiones de garantía que establece la Primera Enmienda.

Así, muchos de los actos que puedan llevar a cabo los poderes públicos en base a una válida orden judicial de investigaciones, pesquisas o incautaciones, pueden conllevar la revelación de creencias de los afectados o pueden afectar a su libertad de expresión u opinión.

[375] En su original en inglés "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*."

Solove (2007) nos dice que, en aquellos casos de recopilación de información por el Gobierno (válidamente establecida por un Juez), y especialmente la que implica el acceso a ordenadores personales o el uso de Internet, llevan casi siempre implícita una intromisión y revelación de datos afectantes a la ideología, creencias, escritos políticos o información sobre el ejercicio del derecho de asociación del sujeto en cuestión o de su religión.

Otros autores como Richards (2013) critican la "vigilancia", porque puede ser dañosa para las libertades civiles, y por tanto también las contenidas en esa Primera Enmienda, haciendo crítica del efecto que puede tener en lo que llama la "privacidad intelectual" ("intelectual privacy").

El origen de esta distinción lo podemos encontrar en algunos casos de la Historia del Derecho estadounidense, que se produjeron antes de la independencia americana y que fueron de especial trascendencia para los colonos. Existía entonces en aquellas posesiones de la Corona Británica y en su Common Law el delito conocido como "seditious libel", un tipo de difamación de sedición que se utilizaba permanentemente contra los colonos, cuando se ofendía a la Corona de la Metrópoli, y que coartaba su libertad de expresión. (McInnis, 2010)

Así, hubo dos pronunciamientos de especial interés en este sentido, y que serían el origen histórico de esa Primera Enmienda en su relación con la privacidad individual, y que dejamos apuntados aquí, más como establecimiento de origen histórico preconstitucional, que como elemento actual jurisprudencial.

Uno fue el caso Wilkes v. Wood 19 Howell's State Trials 982, (C.P 1763), y el caso Entick v. Carrington 19 Howell's State Trials 1029 (C.P. 1765), y en ellos se empezó a ganar esa esfera de libertades civiles en el sentido que nos ocupa. Y que después explosionarían de una manera política y estatal histórica, tras la guerra de independencia (Ku, 2002).

Siguiendo el modelo del epígrafe anterior pasaremos a ver dos ejemplos jurisprudenciales característicos en esta elaboración jurídica, donde se ve afectada además la Primera Enmienda, en la construcción jurisprudencial de defensa de la privacidad estadounidense.

El primer caso es el de Stanford v. Texas,[376] que se entiende en el marco y contexto de la Guerra Fría. En base al punto 9 del artículo 6889-3ª de las Leyes Civiles del Estado de Texas (*Revised Civil Statutes of Texas*) aprobado en 1955, se ilegalizaba el Partido Comunista en Texas y se creaban algunos tipos penales, con penas de prisión de hasta 20 años. Además se autorizaba la expedición de órdenes judiciales y su solicitud policial para la investigación e incautación de documentos, libros, materiales y soportes de todo tipo que fueran en la línea "ideológica" de violación de la Ley.

Así, con la orden del titular de la jurisdicción del distrito competente, se autorizaron este tipo de investigación e incautación en el domicilio del señor Stanford. Tras cuatro horas de inspección del domicilio los agentes, acompañados de dos ayudantes del Fiscal General de Texas incautaron una gran cantidad de documentos, que iban desde libros de Karl Marx, Sartre y Fidel Castro, hasta ejemplares de Juan XXIII y del Juez del Tribunal Supremo Hugo L. Black. Además de numerosos documentos y papeles privados, que incluían su certificado de matrimonio, facturas y correspondencia personal, entre otros.[377]

Para pasar más adelante en la sentencia a recorrer esa significación de la Cuarta Enmienda en la historia jurídica estadounidense. Compara el efecto de esa actuación gubernamental, con aquellos que sufrían los colonos de la Corona Británica, y poniendo explícitamente como ejemplo los casos históricos referidos anteriormente de Wilkes v. Wood y de Entick v. Carrington.[378]

[376] Stanford v. Texas 379 U.S. 476 (1965)

[377] Todo ello nos lo va relatando la sentencia para concluir de manera meridiana y clara que nos encontrábamos ante el paradigma del tipo de actuación gubernamental que se pretendía proteger con la aprobación de la Cuarta Enmienda: la prohibición del uso general de una orden judicial (warrant).
"*…For we think it is clear that this warrant was of a kind which it was the purpose of the Fourth Amendment to forbid -- a general warrant…*"

[378] Y lo hace de una manera contundente y con ánimo trascendente sobre las palabras de la Cuarta Enmienda: *"…These words are precise and clear. They reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever "be secure in their persons, houses, papers, and effects" from intrusion and seizure by officers acting under the unbridled authority of a general warrant. Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists…*"

Y termina comparando los efectos de la "caza de brujas" de aquellos años con los de las veleidades de la Corona Británica[379], en una conclusión que, de manera enfática, se centra en la reivindicacón de esa conquista jurídica.[380]

El segundo caso es el mucho más cercano en el tiempo de Gonzales v. Google,[381]en el que se produce un pronunciamiento del Supremo en un litigio entre el Fiscal General del Estado, Alberto Gonzales, y Google ante las reticencias de la compañía a proporcionar al Gobierno un gran número de búsquedas y consultas realizadas en su buscador, por parte de sus usuarios, durante una semana determinada.

El caso, que tuvo gran repercusión mediática, fue quizá uno de los primeros procesos judiciales que nos advirtieron sobre la vigilancia masiva que sufrimos a través del uso de buscadores y la presión del Gobierno estadounidense para la obtención de esa información.

El Supremo se pronuncia sobre la razonable expectativa de privacidad que los usuarios deben tener en el uso del buscador, no considerando razonable la petición de pesquisa general del Gobierno. Si bien tampoco considera razonable una expectativa de niveles altos de privacidad de los usuarios de Google, y la repercusión (aún de tipo comercial) que para la compañía pudiera tener acceder a esa petición. Sin que tampoco aprecie el Tribunal que pueda entrar en juego la *Electronic Communications Privacy Act (ECPA)* para esa petición masiva de búsquedas de los usuarios.[382]

---

[379] "*…But while the Fourth Amendment was most immediately the product of contemporary revulsion against a regime of writs of assistance, its roots go far deeper. Its adoption in the Constitution of this new Nation reflected the culmination in England a few years earlier of a struggle against oppression which had endured for centuries…*"

[380] "*Two centuries have passed since the historic decision in Entick v. Carrington, almost to the very day. The world has greatly changed, and the voice of nonconformity now sometimes speaks a tongue which Lord Camden might find hard to understand. But the Fourth and Fourteenth Amendments guarantee to John Stanford that no official of the State shall ransack his home and seize his books and papers under the unbridled authority of a general warrant -- no less than the law 200 years ago shielded John Entick from the messengers of the King…*"

[381] Gonzales v. Google 234 F.R.D. 674 (N.D. Cal. 2006)

[382] En este sentido debemosrefereciar el Asunto Google contra la AEPD y Mario Costeja del año 2014 y que será objeto de atención más detenida en la "parte europea" de este trabajo, con origen en cuestión prejudical planteada por la Audiencia Nacional y que el TJUE sustanció en lo que ha venido a conocerse como "el derecho al olvido". Sentencia TJUE. Asunto C-131/12 Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, de 13 de mayo de 2014.

1.4 La Cuarta Enmienda y la seguridad nacional ("The Keith Case")

No hay unanimidad ni consenso en el derecho sobre privacidad estadounidense en cuanto a si la protección de la Cuarta Enmienda se aplica de igual manera para la seguridad nacional, que para las investigaciones criminales interiores. Es por ello que le dedicamos un epígarfe diferenciado a la principal interpretación jurisprudencial sobre esta aplicación en temas de "inteligencia extranjera": el caso Keith.

Ya en la sentencia Katz, como vimos, se introdujeron estas dudas de aplicación en un pie de página a la misma donde se infería que posiblemente no hiciese falta una orden judicial ("warrant") para situaciones donde entrara en juego la seguridad nacional. Tema en el que, en aquella sentencia, también opinan el Juez White y los jueces Douglas y Brennan.[383]

Al final se hubo de afrontar por el Alto Tribunal americano una decisión que fue tomada en 1972 con el caso United States v. United States District Court, conocida como sentencia Keith, por ser el nombre de un Juez de esa demarcación judicial (Damon Keith).

La sentencia United States v. United States District Court[384]se ubica en los siguientes hechos: tres miembros fundadores del grupo denominado "White Panthers" pusieron una bomba en una oficina de la CIA en Michigan. Dentro de las pretensiones de este grupo estaba la abolición del dinero y la "libertad para todo el mundo", siendo además simpatizantes de los "Black Panthers", conocido grupo relacionado con la lucha radical por los derechos de los negros en EE.UU durante los años 60, y que tenían a Malcom X como referencia.

Al investigar los sucesos, el Gobierno intervino las llamadas del teléfono de uno de los miembros del grupo. Y lo hizo sin una orden judicial ("warrant"). La Administración "Nixon" argumentaba que al ser un caso que involucraba a la seguridad nacional, tenía facultades para la vigilancia sin una orden judicial. Si bien el Tribunal Supremo no estaría de acuerdo con esa visión ejecutiva, en una sentencia histórica, que marcaba las próximas líneas a seguir y rompía con la prerrogativa presidencial de actuar de esa

[383] Resulta interesante Wagner & Finkelman (2015) sobre ese impacto en la seguridad nacional.
[384] United States v. United States District Court 407 U.S. 297 (1972)

forma en temas de vigilancia que afectasen a la seguridad nacional. El Tribunal es consciente, desde el primer momento, de la relevancia de fondo del caso que están juzgando.[385]

Y así, pasa a interpretar la legislación de vigilancia del momento, consistente principalmente en la *Omnibus Control and Safe Streets Act* de 1968 (ley que se vería modificada más tarde por la ECPA), para, primero reconocer los poderes especiales del Presidente en tiempo de guerra y de ataques de potencia extranjera, y segundo argumentar la puerta abierta dejada en el caso Katz para establecer que esos reconocimientos no implican una "bienvenida a la vigilancia electrónica del Gobierno."[386]

Reconoce el Tribunal la especialidad que presentan los casos de seguridad nacional y las implicaciones que en ellos tienen la Cuarta y la Primera Enmienda, si bien advierte de los peligros que supone para la "disidencia política" que el Gobierno pueda actuar en base a criterios "tan vagos"; así como las amenazas implícitas a la constitucionalmente protegida libertad de expresión. Reconoce que el precio de esa disensión política no puede ser la sujeción a un poder de vigilancia sin equilibrios ni garantías.

Pasa después la sentencia a centrarse, tras esas consideraciones generales, en el estudio de esa aplicación de equilibrio jurídico al caso concreto que se juzga. El papel que debe jugar el Presidente de EE.UU. se reconoce en la sentencia así como el de la Administración en la seguridad del país, si bien cree el Tribunal que debe hacerse compatible con las exigencias constitucionales de la Cuarta Enmienda. Y reconoce la capacidad de los Tribunales para intervenir, a pesar de tratarse de "investigaciones complejas" como alude el Gobierno.[387]

---

[385] *"The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion*."

[386] *"…But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development -- even when employed with restraint and under judicial supervision…"*

[387] *"… We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case, we*

Aunque también enfatiza que esta decisión se da para los casos "internos" de seguridad nacional y hace hincapié que no está refiriéndose a aquellas situaciones en las que se vean involucrados "potencias extranjeras o sus agentes."[388]

Y pone el foco en la necesidad de que el Congreso considere una legislación que establezca los "estándares de protección" para estos casos distintos a los propios de las investigaciones criminales comunes y que fueran compatibles con la Cuarta Enmienda de la Constitución.

En conclusión de ello, debemos decir que consecuentemente el Congreso recogió el guante lanzado por el Supremo con esta sentencia, y en 1976 un Comité liderado por el senador Frank Church, investigó de manera exhaustiva los poderes y actuaciones de vigilancia del Gobierno en materia de seguridad nacional, concluyendo en la constatación de numerosos y extendidos abusos por parte del Gobierno, que habían resultado en una gran impunidad. Unas primeras palabras del informe dicen: "*too many people have been spied upon by too many Government agencies and too much information has been collected…*"[389]

Este informe tuvo una gran influencia en la posterior redacción de la FISA (que estudiaremos seguidamente), que es el principal instrumento normativo resultante de esta situación y de su constatación constitucional y jurisprudencial por el Supremo en el caso Keith.

---

hold that this requires an appropriate prior warrant procedure.
We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases…"

[388] *"… We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents…"*

[389] Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975-76 (Church Committee) (1976)

1.5 Limitaciones razonables a la privacidad y la cláusula "necesario en una sociedad democrática" del CEDH.

Tras el análisis de las implicaciones constitucionales sobre la privacidad estadounidense y sustanciadas a través de las diversas sentencias referidas en las que se va delimitando el ejercicio del derecho por los ciudadanos, nos parece oportuno traer a colación la tesis del profesor García San José (2001) en este estudio, y que trata precisamente este tipo de limitación en el ámbito del Convenio Europeo de Derechos Humanos de 1950.[390]

Este estudio, por tanto, podemos relacionarlo con las limitaciones que a la protección de la privacidad observamos en las regulaciones estadounidenses, así como en los pronunciamientos judiciales, que vienen motivadas principalmente por la defensa del orden público y por razones de seguridad nacional, (normativizadas como veremos de manera clara en las leyes ECPA y FISA).

La tesis de García San José (2001) se nos presenta en el estudio de este concepto jurídico indeterminado presente en el Convenio como es el de "necesario en una sociedad democrática", y que sirve de razonamiento jurídico de estas limitaciones.

Nos dice el trabajo del profesor (2001, 21) que para supuestos de guerra, (medida también y lógicamente alegada en las regulaciones americanas para su excepción como veremos), el derecho del artículo 8 del CEDH puede ser derogado, si bien sometido ello al parecer del TEDH, en virtud del artículo 15 del Convenio.

Hemos visto que en Estados Unidos la labor de los Tribunales, y principalmente la del Tribunal Supremo, es oscilante en el sentido de determinar la calificación de injerencia en la privacidad. Conectando con ello nos fijamos en que el profesor nos dice que “de un lado, la noción de sociedad democrática se emplea en estos artículos como límite corrector de los derechos humanos para la propia supervivencia de la sociedad democrática. De otro lado esta cláusula está delimitando la facultad de las autoridades

[390] Y ello precisamente para la restricción, limitación de las condiciones y ejercicio de determinados derechos contenidos en los artículos 8, 9, 10 y 11 del mismo. Es especialmente interesante para esta comparación el artículo 8, dedicado a la protección de la intimidad de la persona, y donde se encuentra, de manera más general, incluido el más concreto de privacidad.

del Estado de restringir el ejercicio de estos derechos y libertades...” (García San José, 2001, 26)[391]

En el análisis del concepto se nos dice que la necesidad de la cláusula “no puede ser establecida en términos absolutos”, distinguiéndose la “necesidad en abstracto” de la “necesidad en concreto” (García San José, 2001, 68 y 72-73).

Y se asegura que “el fin de proteger la seguridad nacional justifica, en términos genéricos, la necesidad de una injerencia” para después pasar a la necesidad en concreto de la injerencia (García San José, 2001, 72).

Hasta aquí parece que las determinaciones de excepción que viene recogiendo mucha de la jurisprudencia estudiada y que después será también norma de excepción, como veremos, en las leyes FISA y en la ECPA, aguantan los criterios de análisis de lo necesario en una sociedad democrática (partiendo de que EE.UU. lo es por definición).

García San José (2001) avanza ya en el test de proporcionalidad[392] de la injerencia al fin perseguido como siguiente premisa de control de apreciación, con la exigencia de no imponer restricciones más allá de lo estrictamente necesario y el deber de mantener un justo equilibrio de los intereses en juego, para pasar a analizar la interacción entre necesidad social imperiosa y principio de proporcionalidad. Ello viene complementado además en el estudio, por el análisis de la justificación de las injerencias en los contornos de ser relevantes y suficientes.

Se nos dice que “las razones relevantes y suficientes han de ser interpretadas como relativas tanto a la valoración de la existencia de la necesidad y a su alcance, como a la elección de los medios para llevar a cabo la injerencia (…) se refieren tanto a la necesidad social imperiosa como al test de proporcionalidad (...) De este modo el sentido de las razones suficientes ha de verse, con relación al examen concreto a la luz de las circunstancias particulares del caso, de la valoración del alcance de la necesidad y de la proporcionalidad de los medios empleados al fin legitimo perseguido...” (García San José, 2001, 74 y ss.)

[391] En ese sentido enlaza con el concepto de razonabilidad y sus expectativas para la privacidad a la que se alude en buena parte de las sentencias estadounidenses vistas. Ver como ejemplos las sentencias Smith v Maryland o United States v Jones.

[392] Numerosos autores han tratado este tema. Citaremos aquí a modo de ejemplo el trabajo de Bindi (2016) por el carácter integral y actualizado de su visión sobre el concepto.

Y entra en la distinción entre las razones relevantes y las razones suficientes: "Las primeras se refieren al dato de si la injerencia en principio se justifica en abstracto, sin entrar a conocer las circunstancias concretas del caso y sin tomar en consideración el margen de apreciación del Estado (…) En segundo lugar, al analizarse las razones suficientes ha de verse también si los medios empleados son proporcionales al fin perseguido (…) han de mantener un justo equilibrio entre los intereses en presencia, el interés general y el derecho lesionado (…) hay dos cuestiones diferenciadas: de un lado la necesidad ha de estar suficientemente justificada; de otro, la injerencia ha de ser proporcional al fin legitimo perseguido..." (García San José, 2001, 88 y 89).

Así, entendemos la labor de los Tribunales americanos vista en ese pulso de equilibrio sobre la clave de las "expectativas razonables de privacidad", que se asemeja en esa matización general del CEDH en su clausula "necesario en una sociedad democrática".

Ahora bien, respecto a las estipulaciones legales americanas (que veremos principalmente en la FISA por encargarse de la excepción para la seguridad nacional), en sus excepciones persistentes parecen ir cumpliendo al principio los criterios de justificación del análisis de la tesis del profesor, para la cláusula "necesario en un sociedad democrática". Hasta que nos centramos en las determinaciones concretas del caso y así, en las razones suficientes. Parece que es ahí donde el análisis de justificación encalla para las Leyes americanas desde nuestra humilde opinión, y se para en la relevancia de la excepción del derecho (como es la prevención del terrorismo o la evitación del delito, y que es claramente relevante), pero la excepción legal estadounidense hace en términos generales, tabla rasa sin especificación de concreción (como con los "warrants" plurijurisdiccionales).[393]

[393] Si bien la USA Information Act de 2015 ha hecho, como veremos, un esfuerzo de mejora en este sentido, intuimos que este asunto no conseguiría superar un test de proporcionalidad serio y riguroso, ya que si bien el fin perseguido es relevante (lucha contra el terror) resulta tan abstracto y, sobre todo, los medios son tan desproporcionados (la escucha y vigilancia masiva de datos de millones de personas a lo largo y ancho del planeta); que en una comparativa y utilizando la tesis de referencia, parece que no encontraría justificación, al no ser proporcionales ni de razón suficiente, las limitaciones impuestas por las regulaciones estadounidenses al derecho de privacidad de los ciudadanos.
Ello, claro está, si Estados Unidos estuviera bajo la jurisdicción del Tribunal Europeo de Derechos Humanos.

2. La previsión legal de la privacidad americana en el *Law Enforcement* y la seguridad nacional.

Una vez analizada la principal jurisprudencia sobre la aplicación de la protección de la Cuarta Enmienda en materia de Privacidad, y los pronunciamientos del Tribunal Supremo sobre ello, así como la alusión al equilibrio entre seguridad y privacidad, pasaremos a estudiar las principales leyes federales que regulan esta intervención de intromisión o limitación por parte del Estado en la privacidad de los ciudadanos estadounidenses; y que, en su mayoría, son regulaciones que provienen de una respuesta (más o menos adecuada) a esa interpretación judicial durante el último siglo.

Para ello vamos a distinguir las Leyes encargadas de la vigilancia de las comunicaciones de los ciudadanos, de aquellas también encargadas de la vigilancia pero que contienen elementos de dimensión exterior en su ámbito jurídico. Entre las primeras veremos la *Electronic Communications Privacy Act (ECPA)* de 1986 como norma principal, y la *Communications Assistance for Law Enforcement Act* de 1994, complementadas con algunas alusiones jurisprudenciales de incidencia normativa. Entre las segundas veremos principalmente la *Foreign Intelligence Surveillance Act (FISA)* de 1978, y en segundo lugar la *USA Patriot Act* de 2001 acompañadas de observaciones sobre el caso Snowden, con sus importantes consecuencias jurídicas y reacciones jurisprudenciales.

Por todo ello, y aunque veremos en apartados distintos las normas vigentes de mayor calado como son la *Electronic Communications Privacy Act (ECPA)* de 1986 y la *Foreign Intelligence Surveillance Act (FISA)* de 1978, en los dos planos de seguridad interior y exterior; primero debemos realizar un pequeño comentario sobre las dos leyes previas que fueron sus precedentes y que regularon, durante un importante periodo de la historia americana, estas vigilancias de los poderes ejecutivos federales. Y que afectan a estos dos planos.

Así en 1934, y como reacción del poder legislativo a la decisión del caso Olmstead, se promulgaba la *Federal Communications Act* (FCA) que en su sección 605 se encargaba de la prohibición de interceptación de las comunicaciones sin consentimiento o autorización del remitente, así como de la divulgación y publicación de esa información.[394]

La norma tenía sus limitaciones, ya que las leyes de los Estados podían seguir utilizando pruebas que se hubieran "saltado" la Ley federal, y solo se aplicaba a la comunicación por cable. El "bugging" o escuchas por radiofrecuencia no estaban incluidas.

Así, esta ley, y teniendo en cuenta que su cobertura abarcó buena parte de lo más determinante de la Guerra Fría, (incluida la auspiciada en Estados Unidos por el senador McCarthy, y gestionada por el arbitrario Director del FBI J. Edgar Hoover), podemos afirmar que fue aplicada a verdaderas personalidades como fueron John Steinbeck, Ernest Hemingway, Charlie Chaplin, Marlon Brando, Muhammad Ali, Albert Einstein, John Lennon; así como a otros muchas, incluidos miembros del Congreso y del Tribunal Supremo. Especial relevancia se dio en su aplicación con el reverendo Martin Luther King, ya que el contenido de esas escuchas incluyeron las comprobaciones de un "affair" extramatrimonial que le fueron enviadas a su mujer, así como a él mismo con la sugerencia de que el suicidio sería una buena salida. Conociendo los hechos posteriores de su muerte y la animadversión que Hoover le profesaba, podemos hacernos una idea de lo poderosa e inquietante que puede ser la maquinaria del Estado en su vigilancia al ciudadano por motivaciones políticas o ideológicas, aún en las sociedades y estados democráticos (Solove & Schwartz, 2015, 350).

La otra norma legal de precedencia es la *Omnibus Crime Control and Safe Streets Act* de 1968 que fue promulgada en respuesta al resultado del caso Katz, y que vino a modificar en su momento la FCA de 1934, arriba referida.

Esta ley se modificaría profundamente por la ECPA de 1986 y por ello las referencias a la misma en lo relativo a privacidad aluden al "Titulo III"; que es el Título que

[394] *"…no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person…"*

introducía aquellas previsiones por la ECPA en esa norma de 1968, y que además, coincide con la primera parte de la ECPA conocida como "The Wiretap Act"; y que analizaremos a continuación, junto con las otras dos partes de la ECPA, el Título II "Stored Communications Act (SCA)" y el Título III "Pen Register Act". Debemos destacar que la sustantividad propia de cada una de las partes de la ECPA hace que se aluda a ellas como "Act", aún perteneciendo a una misma Ley (si bien coincidente en su primera parte, como decimos, con la tercera de la modificada Omnibus de 1968)[395]

[395] En esta alusión el Departamento de Justicia estadounidense resume esa interrelación legal con la entrada en vigor de la ECPA, en el siguiente enlace (Recuperado el 1 de agosto de 2018): https://it.ojp.gov/privacyliberty/authorities/statutes/1285

2.1 Regulación legal en el plano interno.

2.1.1 Electronic Communications Privacy Act of 1986 (ECPA)

Contenida y codificada en el Título 18 del U.S.C., en sus capítulos 119, 121 y 206 para cada una de sus partes. La ley surge, en su principio, y como hemos apuntado, para actualizar la ley de escuchas de 1968, que no preveía las nuevas tecnologías acaecidas y se limitaba a señalar las líneas telefónicas y de comunicación de la época, sin entrar, como es obvio, a regular la realidad digital ni electrónica. Después, la propia ECPA se ha visto tratada, al igual que ella en su original propósito, por numerosas modificaciones y puestas al día, y sobre todo a partir de la focalización en la seguridad tras el año 2001 (la omnipresente "USA Patriot Act" es el más vivo ejemplo de ello).

La Ley se divide en tres grandes previsiones legales, de enjundia tal que enmarcan preceptos propios en la codificación americana: la Wiretap Act (que como ya hemos referido actualizaba el Título III de la *Omnibus Crime Control and Safe Streets Act*), la *Stored Communications Act* y la *Pen Register Act* que conforman los tres pilares del enmarque normativo. Titulos I, II y III de la ECPA respectivamente.

Según se establece en sus fundamentos, la Ley aspiraba a crear un justo equilibrio entre "las expectativas de privacidad de los ciudadanos y las necesidades legítimas de la aplicación de la Ley"

La Ley se divide en esas tres regulaciones diferenciadas, coincidiendo con sus tres títulos. Y debemos subrayar que su protección opera de manera independiente a la protección establecida en la Cuarta Enmienda constitucional.[396]

[396] Incluso con procedimientos más exigentes para la obtención de una orden judicial en comparación con las peticiones basadas en la previsión constitucional. Por ejemplo cualquier agente encargado de la ejecución legal respectiva puede solicitar una orden judicial ("warrant") en base a la Cuarta Enmienda, si bien en base a la "Wiretap Act" solo determinados agentes encargados, como son los fiscales que lleven la investigación.

La regulación de la *Wire Communication Act* viene básicamente referida a conversaciones telefónicas sin expectativa de que sean escuchadas por terceras personas. La regla general de la Ley es la prohibición de las escuchas y de la interceptación por otro particular, así como su mantenimiento y divulgación. Estas requerirían mecanismos ("devices"), y no simplemente un mero "poner la oreja". Evidentemente, y como es habitual, hay excepciones, que están previstas en la Ley.

La *Stored Communications Act* (Título II) protege la información almacenada. Que en el contexto actual viene referido fundamentalmente a los correos electrónicos que no se encuentren en tránsito.

La *Pen Register Act* entra en juego cuando también lo hacen estos mecanismos de captación. Por la información que pueden contener estos "devices", el título que regula su utilización en relación con la privacidad resulta menos restrictivo que los anteriores. Ya que, a pesar de que la Ley los prohíbe de manera general, la irrupción de la *USA Patriot Act* los puso otra vez en licitud, incluso dentro de los "softwares".[397]

2.1.1 a) Wiretap Act

Este Título primero[398] de la ECPA se nos desarrolla desde el precepto 2510 hasta el 2522.

Su primer parágrafo establece una definición esencial para delimitar el objeto de la Ley distinguiéndose entre "Wire communication" y "Oral communication"[399]

Para la comunicación artificial ("Wire") se requiere siempre algún tipo de artilugio ("facilities") de captación de la comunicación. Es decir, artilugio de captación manejado o controlado por persona interesada. Comunicación oral sería, en cambio, toda aquella

[397] Como apunta muy bien EPIC (Recuperada el 1 de agosto de 2018) no hay una determinación legal que excluya como norma general (y que así opere) las situaciones en que el Gobierno use de manera ilícita estos "pen registers" o "trade devices".
[398] Recogido en el 18 U.S. Code capítulo 119 con el enunciado "Wire and electronic communications interception and interception of oral communications".
[399] Parágrafo 2510 ("Definitions")

fuera de la comunicación electrónica emitida por persona en circunstancias que no son sospechosas de producir esa captación.

El territorio ("State") es el propio de EE.UU. y por la acción ("intercept") se entiende aquella que requiera el uso de mecanismo ("device") para esa interceptación de cualquier tipo de comunicación (oral o electrónica). Por estos "devices" se conciben todos los artilugios para ese fin de interceptación, menos el uso individual y común del aparato telefónico y el oído.

La definición de persona es todo lo amplia que podría caber. Persona natural o jurídica, pública o privada, incluyendo Estados y personal a su servicio. Por "Investigative or law enforcement officer" se refiere al funcionario (también el fiscal) encargado del asunto.

Otras definiciones del precepto no merecen mayor comentario, estando dentro del habitual jurídico conocido. Como los contenidos de la comunicación (punto 8) (referido a lo sustancial, no a lo formal), Juez competente (punto 9), y persona agraviada (punto 11) partícipe de la conversación captada.

Un comentario más extendido merece el punto 12, que define la comunicación electrónica fuera de la establecida por cable o de la "susurrada por el viento" por voz humana, fuera también de los "buscas" ("tone-only paging device"), y de los dispositivos de escucha móviles (utilizados con autorización judicial y pobladores del imaginario cinematográfico o novelesco colectivo de investigaciones policiales). También se dejan aparte las transferencias financieras, afectadas, como ya comprobaremos, por la específica "Financial Privacy".[400]

La definitoria del punto 17 nos determina que se entiende por almacenamiento electrónico, también en sentido amplio y relacionado con la captación. Y la definición 18 que llega a entrar en esas "palabras llevadas por el viento" en el concepto de "aural transfer". El punto (19) "foreign intelligence information", sigue la definición de la FISA y el punto (20) "protected computer", se refiere a los ordenadores

[400] Las definiciones de los puntos (13) "user", (14) "electronic communications system", (15) "electronic communication service", y (16) "readily accessible to the general public" (de fácil acceso público) no plantean mayores problemas de interpretación, siempre teniendo en cuenta los anteriores definitorios sobre comunicaciones de la Ley. (Por ejemplo "readily accessible to the general public" respecto a comunicación por radio, significa que no se encuentre encriptada o en frecuencias restringidas). De ahí el carácter algo obsoleto o de no amplia cobertura jurídica de la Ley, vistas la altura de las comunicaciones hoy.

gubernamentales con información estratégica o de especial confidencialidad. Ya en los orígenes de la ley había este tipo de "computers", pero ello no va referido a los ordenadores personales. El punto 21 "computer trespasser", define al que "traspasa" los límites de la Ley en el acceso no autorizado a los ordenadores protegidos del párrafo anterior.

La regla general de prohibición se ecuentra en el precepto 2511 ("Interception and disclosure of wire, oral, or electronic communications prohibited"), que marca la pauta general de regulación de la Ley, con las habituales excepciones.

La larga primera parte de este precepto se encarga de desmenuzar y especificar la prohibición general de la Ley con la advertencia de sanción, para toda aquella persona que intercepte o intente interceptar cualquier comunicación por cable, oral, o electrónica (en el sentido de las definiciones ya vistas), o bien use para sí o para otra persona mecanismos de captación intencionadamente; o bien revele a otra persona, con conocimiento, el contenido de lo captado de manera autorizada por la ley, sabiendo que es información relacionada con una investigación criminal.[401]

El punto 2, de mayor extensión, establece la larga lista de excepciones a esa prohibición y amenaza de sanción general. No serán ilegales así:

- Esas acciones en el transcurso normal de la prestación de servicios por el empleado público encargado de los mismos. O si las mismas son exigidas en el marco de la "Foreign Intelligence Surveillance Act (FISA)", y avaladas por mandato judicial o certificación del Fiscal General. Evidentemente con obligación de no revelar ese mandato legal recibido que pudiera afectar a la investigación por la que se lleva a cabo esa vigilancia.

- Tampoco para los empleados de la *Federal Communications Commission* en el ejercicio de sus funciones amparadas por la Ley.

[401] En este sentido guarda relación con la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Concretamente citaremos su Artículo 31 bajo el título "Comunicación de una violación de la seguridad de los datos personales al interesado"

- O si es parte de la comunicación interceptada y lo hace "under color of law". Es decir, siguiendo un aparente poder de legalidad de actuación, o bien cuando alguna de las partes de la comunicación ha dado su consentimiento previo para esa interceptación.

- Lo anterior pudiera ser obviado (para el caso de que no se actuara "under color of law") y no ser ilegal, para el caso de que esa comunicación se haya interceptado con objeto de evitar la comisión de acto criminal o contrario a las leyes.

- También se excepciona la ilegalidad para los funcionarios y empleados públicos en el ejercicio habitual de sus funciones, que conlleven tareas de vigilancia en el marco de la FISA.[402]

- Tampoco lo será la interceptación que venga de fuentes de acceso público o de alguna fuente que pudiera estar causando interferencia dañosa con el solo objeto de identificarla.

- Utilizar un "pen register" o "trace device", en los términos de este título o entre proveedores de servicios de comunicación para protegerse de fraude o uso abusivo del servicio.

- Tampoco será ilegal actuar "under color of law", para interceptar comunicaciones electrónicas o por cable de un "computer trespasser", si el propietario del ordenador protegido ("protected computer") lo autoriza, o si la persona que así actúa ("under color of law") está amparada legalmente por una investigación. O bien crea razonablemente que el contenido de ese ordenador "traspasado" será relevante para la investigación y ello no implique adquirir comunicaciones más allá de las que se transmitan desde el ordenador que intenta ese acceso.

Todas estas últimas serían excepciones de participación activa de la sociedad en la aplicación de la Ley.

Habrá multa proporcional o prisión de hasta 5 años para los incumplimientos de esta Ley (punto 4). El punto 5 establece una jurisdicción de ámbito inferior al federal para temas de solo visionado o escuchado sin mayores implicaciones criminales, siguiendo

[402] Por si este marco de excepcionalidad no fuera suficiente, la letra f) del precepto establece un blindaje general de excepción para lo que de esta Ley afecte a la adquisición por el Gobierno de EE.UU. de información o comunicación de potencia extranjera.

una serie de requisitos (principalmente que no sean comunicaciones encriptadas o protegidas).[403]

La ley establece igualmente la importante regulación de los aparatos de interceptación y las autorizaciones para esa interceptación.[404]

Sanciona así la distribución de los mecanismos y artilugios diseñados para este tipo de captación de comunicaciones. Y lo hace con multa, o bien con prisión de hasta 5 años. Se está refiriendo a distribuciones fraudulentas o ilegales, es decir, al "mercado negro" de estos aparatos.[405]

La Ley continúa con la posible autorización de estas interceptaciones de las comunicaciones, que bien puede prestar el Fiscal General o sus subordinados o delegados especialmente designados por él al efecto, dada al FBI o la agencia competente de la investigación de que se trate para el caso de ofensas criminales que se listan pormenorizadamente; teniendo todas unas consideraciones graves en su tipificación y reproche penal. También tienen esta capacidad autorizadora los fiscales de los Estados o de "subdivisión política inferior" en su ámbito jurisdiccional en búsqueda de pruebas en averiguación de delitos graves o muy graves. Acabando por permitir la autorización por parte de cualquier Fiscal para la aportación cualquier prueba en el caso de "federal Felony" o similar para delito grave federal.[406]

En cuanto a la regulación del procedimiento de interceptación[407]la solicitud debe hacerse siempre por escrito, bajo juramento, al juez competente y por la autoridad

[403] Siendo también las multas y penas menores. Fundamentalmente de responsabilidad civil y con un mínimo general de 500 dólares.

[404] Aspecto de la Ley, y este título en su conjunto que se ve muy gráficamente reflejada en la más laureada serie de televisión de los últimos tiempos, conocida precisamente como "The Wire" y que da una idea muy ajustada de estas autorizaciones de escuchas.

[405] Indicándose en el punto 2 del artículo que no se considera ilegal la distribución normalizada en la relación de negocios usual de estos aparatos, o dentro de la actividad pública oficial del Gobierno y gobiernos estatales o locales de EEUU. Establece la capacidad de confiscación de esos aparatos y la imposibilidad y prohibición de su utilización probatoria (parágrafos 2512, 2513 y 2515).

[406] Diferencia la Ley la puesta a disposición de datos en investigaciones criminales distintas, y entre los funcionarios y Administraciones encargados de su ejecución, y obtenidos con previa autorización válida (preceptos 2516 y 2517).

[407] El artículo 2518 "Procedure for interception of wire, oral, or electronic communications" es el precepto que nos relata el procedimiento a seguir.

habilitada para ello, con una completa relación de la identidad de los agentes y de la persona o personas cuya comunicación se pretende interceptar, así como de su tipo, los hechos detallados y la identificación del proceso de investigación criminal y su periodo de tiempo y demás detalles de interés. Pudiendo el juez pedir información adicional y prueba documental para ello. El juez puede ampliar a parte interesada la solicitud de interceptación cuando se aprecien circunstancias de ilícito penal grave, o que puedan ayudar a avanzar en una investigación criminal de ese tipo que esté, digamos, "empantanada".[408]

Toda orden debe ser expedita, no debiendo enfrentarse a trabas, obstáculos o dilaciones por parte de las parte implicadas (principalmente los proveedores de las comunicaciones). Tampoco la orden podrá excederse de lo necesario para la consecución de sus objetivos, estableciéndose el plazo temporal de 30 días como tope legal general desde el comienzo de las interceptaciones, pudiendo extenderse con nueva orden justificada. El juez será informado de manera permanente sobre los avances en las escuchas.

Una excepción procedimental se da, como suele ser habitual, para casos de emergencia, debiendo apreciar, el Fiscal competente según el caso, que las mismas concurren razonablemente.[409]

Hay, como es habitual, una serie de garantías sobre estas actuaciones como la necesidad de que sean grabadas y conservadas por un periodo de 10 años, su custodia bajo responsabilidad judicial y el archivo de actuaciones para las denegadas, o de plazo vencido así como un registro normalizado de las mismas.

Toda interceptación ilegal o sin autorización judicial suficiente o en disconformidad con la autorización, deberá ser destruida por la autoridad que la realizó con las responsabilidades que proceda dilucidar por el órgano judicial.

---

[408] El punto 4) establece el contenido que debe observar la orden judicial así como sus requisitos.

[409] Estableciendo qué se puede entender por casos de emergencia las letras a y b del punto 7 del precepto. Estos mandatos de emergencia deben ajustarse al dictado de supuestos de esta Ley y debe ser validada por una orden en el plazo de 84 horas.

Prosigue la norma con los necesarios informes que se deben expedir sobre estas interceptaciones en el procedimiento. En enero de cada año los jueces deben informar de todos sus mandatos judiciales (con sus contenidos principales) de interceptación de comunicaciones a la *Administrative Office of the United States Courts*.Y en marzo de cada año será el Fiscal general o los fiscales que lo hayan ordenado, los que lo hagan a ese mismo órgano.[410]

Se prevé además por la Ley la reparación de los daños civiles que se puedan provocar por intromisión injustificada o violación de esta ley en las comunicaciones de los particulares, principalmente con reparaciones pecuniarias y con plazo de prescripción de 2 años. Igualmente regula la previsión del régimen disciplinario administrativo para aquellos empleados públicos que resulten responsables de estas violaciones.

Por último, se recoge el requerimiento típico de protección por fiscal competente así como el encargo de incidir legalmente en la aplicación de la ley, sobre todo enfocado a los proveedores de estos mecanismos.[411]

2.1.1 b) Stored Communications Act

Esta segunda parte[412] de la ECPA regula el acceso a la parte almacenada de las comunicaciones electrónicas y su privacidad. Empieza estableciendo lo que se entiende por ofensa a lo protegido por esta parte de la ley. Básicamente se conceptuará el acceso intencionado sin autorización o excediendo de la misma a través de instalación en las comunicaciones electrónicas; y obtener, alterar o evitar el acceso autorizado, previendo su castigo, en multa o prisión de 5 a 10 años. Y de multa o prisión de hasta 1 año para el

[410] Aquí la precisión no es tan exigente como en la obligación anterior de los jueces, ya que se habla de números aproximados en un informe general, con informe también de sus resultados de investigación y de las consecuencias jurídico penales (parágrafo 2519).

[411] Y se establece multa civil en caso de no atención a la misma (de hasta 10.000 dólares cada día de no obediencia).Parágrafos 2520, 2521 y 2522.

[412] Esta parte de la norma se encuentra contenida y codificada en el 18 U.S. Code, capítulo 121 bajo el título de "Stored wire and electronic communications and transactional records access" que incluye desde el parágrafo 2701 hasta el 2712.

resto de las motivaciones.[413]Las excepciones son las propias de la prestación del servicio y permitidas legalmente.

Sigue la Ley con la regla general de uso de esta información, y las excepciones a la misma. Se establecen así las prohibiciones de divulgación de la información almacenada electrónicamente, por la personas (naturales o jurídicas) encargadas de la prestación del servicio, bien sea con motivo de esa prestación o con destino a entidad gubernamental. Y además se encarga de las excepciones a esa prohibición de divulgación o puesta a disposición de las comunicaciones.[414]

Evidentemente se excepciona la prohibición al destinatario de servicio, a personas autorizadas legalmente o con el consentimiento del destinatario del servicio, a empleados autorizados, y para lo que sea necesario para la prestación del servicio o protección de los derechos o propiedad del prestatario del servicio.[415]

Continúa el precepto encargándose de las excepciones a esa prohibición de divulgación o puesta a disposición de los archivos de los clientes ("customer records") repitiéndose las excepciones anteriores. Con algunas notables diferencias como la del punto 6[416] de la letra c, pareciendo que la persona "no gubernamental" es mucho más digna de confianza que el aparato que ejecutivamente funciona en su nombre a nivel de conjunto. Y no estableciéndose aquí lo estipulado en la letra b) anterior, antojándose así, que en estos casos ("costumer records"), la regulación está más centrada por la propia naturaleza del tratamiento de datos (no habiendo aquí persona empleada para la prestación del servicio).

---

[413] Parágrafo 2701 "Unlawful access to stored communications"
"for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State."

[414] Precepto 2702 letras a y b.

[415] Esto se puede perfilar como una concesión a las empresas en detrimento de la Privacidad.
También resulta excepcionado "the National Center for Missing and Exploited Children", en el perfil de atención al menor, así como la excepción importante y transversal para las agencias gubernamentales, para los casos de implementación legal o en el ejercicio de sus funciones, y con los requisitos que introduce razones de emergencia. Dejándose la percepción de la emergencia (algo sorprendentemente) a la buena fe del suministrador del almacenamiento de las comunicaciones. Ya que lo son por motivaciones de prevención criminal.

[416] (*"6) to any person other than a governmental entity*."

También se regulan para estos casos las divulgaciones o puestas a disposición de emergencia, y su informe de control democrático a la Cámara de Representantes y de periodicidad anual.

La Ley trata también de la divulgación o puesta a disposición obligada o necesaria de las comunicaciones almacenadas. Lo regula para el almacenamiento electrónico y para el almacenamiento remoto. Para el almacenamiento electrónico, prevé la posible petición por entidad gubernamental por un máximo de 180 días para casos amparados por el Estatuto de enjuiciamiento criminal y a autorizar por la jurisdicción competente. Para el almacenamiento remoto se regula igual que en el anterior, diferenciándose en la necesidad de notificación previa o no a la entidad que presta el servicio. Para el remoto no se requiere esa notificación previa para los procesos criminales.[417]

Se establece una lista de los casos en que una entidad gubernamental puede solicitar a un proveedor de servicios de almacenamiento de comunicaciones electrónicas (también remoto) sus registros o archivos. Básicamente resumida la posibilidad en que venga con obtención de orden o citación judicial o el consentimiento del responsable del fichero o su titular; o bien como motivo de investigaciones criminales y contra el fraude.[418]

Para los casos de solicitud judicial, se establecen claramente los requisitos para su aceptación y que pivotan principalmente sobre los "hechos razonables" que apreciará el juez competente. Siguiendo los dictados de este precepto, los proveedores de este almacenamiento están libres de posible causa judicial contra ellos por este motivo.[419]

Además, se contempla la posibilidad de que la entidad gubernamental solicitante, pida una creación de copia "de respaldo" de esos contenidos. Igualmente sin necesidad de notificación al cliente afectado, la empresa suministradora de estos servicios puede realizar tal copia dentro de su actividad habitual con el fin de tener cumplida esta

[417] Si que se exige notificación previa para el caso en que solo se esgrima notificación administrativa de autoridad estatal o federal o se obtenga orden judicial. O bien cuando se actúa de parte del titular o por motivos de mantenimiento del servicio de almacenamiento.Parágrafo 2703 "Required disclosure of customer communications or records". En sus letras a y b respectivamente para el almacenamiento electrónico y remoto.

[418] Especificándose que el contenido que se puede poner a disposición (siguiendo siempre la notificación administrativa o judicial), y que incluye una serie de datos personales relevantes. (Letra c))

[419] Estableciéndose además los requisitos mínimos para hacer valer las posibles pruebas que surjan y que se contengan en esos ficheros afectados por orden judicial, debiendo realizar los proveedores "los pasos necesarios" para su preservación. Su retención será por un máximo de 90 días. (Letras d), e) y f))

posible obligación. Una comunicación de esa petición deberá hacerse al interesado por la entidad gubernamental solicitante en un plazo de 3 días desde la confirmación de la realización de la copia.[420]

También se regulan los requerimientos que se les pueda exigir cumplir al cliente o suscriptor del servicio así como sus posibilidades de actuación en contra de esta puesta a disposición.

En 14 días desde la notificación gubernamental se puede recurrir la orden judicial o administrativa que solicita esa copia al servidor, debiendo contener su identificación como afectado en esos contenidos y sus razones para estimar que esos ficheros no son relevantes para la ejecución legal que se trate. El tribunal con la jurisdicción correspondiente decide, valorando los medios de prueba a su alcance.

Se prevé el pago por los costes que esta "intromisión necesaria" del Gobierno provoque en los clientes-suscriptores y en las empresas-prestadoras del servicio. Y la acción civil para el caso de perjuicios surgidos contraviniendo lo establecido en esta norma, estipulándose además el posible juego del régimen disciplinario administrativo.[421]

El parágrafo 2709 es una secuela más de la gran excepción "mainstream" en la lucha contra el terrorismo, y que atraviesa toda la norma en materia de privacidad estadounidense. En él se establece una regulación "paralela" para los casos en que entre en juego la "necesidad" de la contrainteligencia estadounidense. En este artículo se habilita una regulación distinta, y por esta causa, para las investigaciones del FBI, que entra dentro de esa gran excepción de la norma escrita en la protección de la privacidad

[420] La copia deberá ser mantenida durante el tiempo hasta que sea suministrada o hasta el final de los procedimientos para los que se solicita. Se establecen 14 días de "cortesía" para poner a disposición de la entidad gubernamental la copia, una vez que haya comprobado que el cliente no ha contestado al Gobierno para ello y no ha iniciado los pasos tampoco. Se prevé asimismo una especie de proceso de realización de copia de respaldo de emergencia, si existe la razón para creer que esas pruebas o posibles pruebas dimanantes pudieran ser destruidas o falsificadas. Se establece la posibilidad de que esta última notificación sea retrasada hasta 90 días si hay apreciación del Juzgado de un posible "resultado adverso" de esa notificación. Posibilidad igual existe para las notificaciones de las autorizaciones administrativas. De ello se debe informar a los clientes o suscriptores interesados. Se entiende por "resultado adverso" en su punto 2 aquellos peligros para la vida o integridad física de las personas, la posibilidad de escapar de la acción de la Justicia, o la destrucción de pruebas, coacción de testigos u otros peligros que amenacen la investigación o la acción de la Justicia. Para el caso de no existiera esa necesidad de notificación sobre el acceso gubernamental, el procedimiento sería al contrario, debiendo solicitar la autoridad pública de que se trate al Juzgado una orden expresa sobre la notificación.
(Preceptos 2704 "Backup preservation") y 2705 "Delayed notice").

[421] Parágrafos 2706 y 2707.

estadounidense, y que solo pudiera ser matizada caso por caso por una posible futura jurisprudencia.[422]

Establece la obligación de provisión en la figura del Director del FBI sobre sus requerimientos. De la que se deberá dejar certificación con todos los extremos "pedidos" por el FBI y puestos a su disposición. Si bien se trata de acotar la puesta a disposición de cierta información, prohibiendo aquellas situaciones de divulgación que puedan suponer un peligro para personas o para la seguridad nacional, entre otras. Semestralmente se deberá informar al Comité de Inteligencia de la Cámara de Representantes. Todo lo anterior se pudiera resumir, así, en una posibilidad abierta para espiar, si bien con cuidado y advertencia sobre las implicaciones diplomáticas y la discreción interna.

La Ley se fija de manera especial en la no divulgación por los proveedores del servicio de "video tape" (cintas de video) sobre la información de los clientes y sus datos concretos.[423]

Por último acaba esta parte de la Ley con un precepto dedicado a las definiciones y aclaraciones aplicables para este capítulo legal y otro dedicado a acciones de responsabilidad civil contra los EE.UU.[424]

2.1.1 c) Pen Register Act

Esta parte de la Ley se encuentra ubicada y codificada en el título 18 del U.S.C., capítulo 206 bajo el enunciado "Pen Registers and Trap and Trace Devices". Su redacción abarca desde el parágrafo 3121 hasta el 3127.

[422] "Counterintelligence access to telephone toll and transactional records"

[423] El hecho regulado está muy circunscrito al antiguo hábito de pertenecer a un "video club" que podría almacenar ficheros sustanciosos sobre la práctica de alquiler y los gustos en las cintas de video de los clientes-suscriptores. Está contenido en el Precepto 2710 ("Wrongful disclosure of video tape rental or sale records"). Esta determinación viene introducida en 1988 por la *Video Privacy Protection Act* que hemos tratado en el bloque de "Consumer Privacy". En definitiva, se establece la prohibición general con las consiguientes y habituales excepciones, y con la posibilidad de acción civil por daños y perjuicios que el incumplimiento pudiera generar. Este establecimiento parece mantenerse por el servicio de videoteca que habitualmente se suele establecer por muchos proveedores de comunicaciones.

[424] En general, por cualquier persona agraviada por la violación de la correcta aplicación de este capítulo legal, por un importe en daños de al menos 10.000 dólares (parágrafos 2711 y 2712).

Se abre este título con la general prohibición de utilización de estos artilugios sin autorización judicial. La excepción se encuentra acto seguido en el precepto 3121, que en realidad son tres tipos de excepción, y pudiéramos resumirlos en: el uso relacionado con la protección de los derechos de propiedad del proveedor, los usos necesarios para la protección de los usuarios o los usos consentidos. Ellos, en general, con vistas a proteger más bien al ámbito empresarial o prestador del servicio que a la privacidad.

Además, se establece la limitación de su uso a las agencias gubernamentales autorizadas para ello, sobre todo en sus contenidos. Con la posibilidad de multa sobre la violación de la prohibición.

La Ley regula la solicitud de autorización, que debe realizar un fiscal para el Gobierno sobre la instalación al juez competente. También se habilita a funcionarios estatales, a menos que una ley estatal lo prohíba. Debe contener, como requisito, la identificación del solicitante y la certificación razonada de que es necesaria para una investigación criminal. Estipula también el procedimiento para la emisión de una orden de instalación de estos aparatos, que se diferencia según venga del fiscal del Gobierno o de funcionario encargado de la ejecución legal correspondiente, y según los parámetros vistos (juzgados o ley estatal).

Debe mantenerse, además, un registro con la identificación de los agentes que han obtenido estas autorizaciones y sus propósitos, fechas y seguimiento de la instalación.[425]

Además el título legal establece los casos en que, de así estar autorizado en la instalación, los actores y suministradores implicados deberán ofrecer la colaboración necesaria para la misma.

Y siguiendo la lógica descrita en los tres títulos de la Ley, estipula un procedimiento de autorización e instalación de emergencia para los casos tasados que razonablemente se observen puedan acaecer, cuales son los propios de estos supuestos (peligro inminente para personas, actividades de conspiración y crimen organizado, riesgo para la seguridad nacional o un ataque continuado a ordenadores protegidos gubernamentales).

[425] Parágrafos 3122 y 3123. Los requisitos de contenido de la orden vienen desgranados en la letra b) del 3123. El periodo máximo de autorización será de 60 días, que puede ser extendido por un mismo plazo con las garantías necesarias. Y no podrá revelarse la existencia de estas órdenes, con el objeto de proteger la investigación en curso.

Establece, igualmente, la necesidad de informe general anual por parte del Fiscal General al Congreso sobre estas autorizaciones. Junto con las definiciones que operan en este título revisten especial interés la de los propios aparatos que se utilizan para las escuchas.[426]

2.1.1 d) Consideraciones sobre la ECPA

En la segunda parte de la Ley ("Stored Communications Act") debemos fijar nuestra atención en la gran excepción de autorización establecida para las "National Security Letters ("NSL")"[427] por parte del precepto 2703. En ella, como hemos visto, la mera orden administrativa sirve para poner a disposición del Ejecutivo unos "parámetros básicos de información", que son datos personales de las personas (clientes-suscriptores principalmente). Ello en base a la *USA Patriot Act*, y que es el gran "meollo" de la posible (y masiva) puesta a disposición de los datos de los ciudadanos (no solo de los americanos, teniendo en cuenta la ubicación legal de las grandes empresas tecnológicas con influencia en todo el mundo), al Ejecutivo estadounidense por razones de seguridad.[428] Es, así, muy importante, porque establece una categorización de los accesos que el Gobierno puede ejercitar sin autorización judicial (Slove &. Schwartz, 2015, 441-463).

De los tipos de comunicación electrónica vemos, por tanto, que se necesita "warrant" (orden judicial) para:

– Los correos electrónicos en tránsito (en base al 2516 de la "Wiretap Act").

– Los correos electrónicos almacenados en ordenador doméstico (en base a la Cuarta Enmienda de la Constitución de los Estados Unidos).

[426] Parágrafos 3124 a 3127. Principalmente los términos "pen register" y "trap and trace device"

[427] Nos sirve de apoyo, al igual que en otras partes del trabajo, los resúmenes del Electronic Privacy Information Center (EPIC). (Recuperado el 1 de agosto de 2018): https://epic.org/privacy/ecpa/

[428] Interesante artículo al respecto se nos presenta en Henderson (2002). En él se concluye que el equilibrio jurídico entre privacidad y seguridad se rompe claramente a favor de la segunda tras los atentados del 11 de septiembre de 2001. Con gran decantamiento de actuación en el poder ejecutivo.

– Los correos electrónicos almacenados en "remoto" y que no estuvieran abiertos en plazo de hasta 180 días o menos (en base al 2703 de la "Stored Comunications Act").

Quedan el resto de correos electrónicos a la merced de la solicitud ejecutiva sin necesidad de orden judicial. El resto de correos serían la gran mayoría, es decir, aquellos almacenados en "remoto" abiertos o no abiertos por más de 180 días.[429]

Además, las NSL son utilizadas de manera directa para conocer los datos personales del usuario (en base al 2703 en su letra d)), pero ya con orden judicial, podrían ponerse a disposición datos que no sean de esos clientes-suscriptores, si bien relacionados con el mismo, Tales como web visitadas o dirección de correo de sus destinatarios. Y todo ello solo en base a "elementos razonables" de que sean relevantes para una investigación criminal.[430]

Es importante resaltar, además, que se otorga una importancia algo más decisiva al ámbito de privacidad regulado en esta Ley, que, en cambio, no hemos visto tan resaltada en otros sectores estudiados (ejemplo de la *Financial Privacy*). Y que se manifiesta, por ejemplo, en unas mayores penalizaciones pecuniarias por responsabilidad civil, y sobre todo, en la mayor previsión de penas de prisión (de hasta 5 años por sus infracciones muy graves). Es verdad que hay un espíritu de protección frente a los "desmanes" de los poderes públicos muy arraigado en la cultura americana, si bien se da la paradoja, de que, por otro lado y en aras de la seguridad, esa protección, en principio conceptuada con gran fortaleza, se desvanece cuando entran en juego esas razones de seguridad.[431]

Vemos así cómo en EE.UU., las leyes de privacidad son (grandes o pequeñas) islas que regulan en su conjunto lo afectante a privacidad en un entorno o sector de actividad concreto. E implican todos los recursos de regulación, y sin derivar a la legislación específica general sino incorporándose a ella. Es decir, no deriva al código penal ni a la

[429] Se puede comprobar, al entrar en las usuales cuentas de Gmail, Yahoo, Outlook o la del distribuidor americano habitual que se utilice para comunicarse electrónicamente por parte de la gran mayoría de usuarios en el entorno de referencia de este trabajo que buena parte de esos correos no dependen de la intervención de un Juez para ser investigados por el poder ejecutivo norteamericano.

[430] En este sentido es de especial interés el magnífico artículo de Bagley (2011).

[431] Algo que no se observa tanto en la normativa específica de protección de datos europea, de carácter más homogeneizado, de tratamiento menos diferenciado del sector público o privado que trate los datos, y además sin unas contradicciones tan fuertes (por ahora) cuando entra en juego el tema de la seguridad.

legislación de vulneración de secretos oficiales por ejemplo, sino que viene conteniendo, por regla general, previsiones al respecto en cada ley de privacidad; aunque sean cláusulas legales muy parecidas, casi "mainstream".

Por otro lado, y respecto a la primera parte ("Wiretap Act"), nos llama la atención el matiz sobre la "autograbación", que en principio es admisible, aunque el otro interlocutor no estuviera informado, y no es ilegal. Ya que la ECPA requiere solo el consentimiento de "una de las partes".[432]

Relacionado con el ejemplo anterior, la Ley en sus dos primeros títulos se fija también de manera concreta en lo regulado en el ámbito laboral. Establece, así, especial importancia a lo estipulado en el contrato y sus clausulas de expresa autorización, para que esta ley despliegue o no sus efectos de protección. Con lo que esta "especialidad laboral" prevalece en caso de que así estuviera advertida.[433]

Por último y para el caso de los "Pen Registers" (tercera parte) o uso de similares artilugios, nos llama la atención que tampoco nos encontramos reconocida en la Ley un derecho particular de actuación contra las actividades ilícitas de los Gobiernos en su uso.

Igualmente podremos ofrecer una visión crítica de la Ley en cuanto a la necesidad de actualización que está pidiendo, tras los últimos avances de la tecnología, sobre todo de la telefonía móvil. Ya que en las definiciones de la Ley siempre parece haber "puntos fijos" para esa transmisión electrónica y su protección. Es una Ley concebida, por así decirlo, "para el cable", si bien esa forma de transmisión cada vez se viene utilizando menos. En ello la Ley podría empezar a presentar "disfunciones" necesarias de continua interpretación.[434]

[432] Imaginemos lo que conlleva en los lugares de trabajo donde una parte (el empleador principalmente) podría establecer una vigilancia permanente a sus trabajadores.

[433] Si bien el ejemplo nos pudiera servir para cuando ese mismo empleador estableciera en las claúsulas de sus contratos esa obligación "a poder ser vigilado".

[434] El caso del almacenamiento en la "nube", y siguiendo el estudio del EPIC (2015), ya de por sí no se presentaría en clara protección, según el dictado de la Ley. Si bien en este caso ya se ha pronunciado el poder judicial, incluyendo esa protección (U.S. Court of Appeals 6th Cir. En United States v. Steven Warshak (08-3997/4085; 09-3176); Harriet Warshak (08-3997/4087/4429); TCIMEDIA, Inc. (08-3997/4212)). Autores como Kattann (2011) opinan directamente que la "Stored Communications Act" no protege la privacidad de la información almacenada en la "nube", abogando por la necesidad urgente de

Además de ello, el periodo de 180 días de "protección" parece no estar pensado para el común almacenamiento actual de las comunicaciones electrónicas. Que parecieran comunicación "abandonada" en el momento de la regulación, mientras hoy sería una información "guardada" en esos canales y servidores, que utiliza así el ciudadano para ese fin. Ya que no solo utilizamos los servidores de correo para enviar y recibir comunicaciones, sino también para mantener almacenada la misma.[435]

2.1.2 Communications Assistance for Law Enforcement Act de 1994

Esta Ley se encarga de asegurar la posibilidad de interceptación de comunicaciones electrónicas para la adecuada ejecución legal y actuación ejecutiva del gobierno federal y de los gobiernos estatales. También conocida como "The Digital Telephony Law" la CALEA (en su acrónimo) está recogida y compilada en el Título 47 del U.S.C., Capítulo 9, ocupando desde el parágrafo 1001 hasta el 1010.

La Ley surge con la idea de facilitar las interceptaciones a las autoridades encargadas de la aplicación legal en sus funciones (FBI, DEA, Departamento de Justicia, etcétera), y se aprueba durante la presidencia de Bill Clinton.

---

reforma de la Ley.

[435] Coincidiendo con la postura del EPIC, tal y como relata en su página web (Recuperado el 1 de agosto de 2018): "*The 180 day rule within ECPA is also the subject of much criticism. When ECPA was passed in 1986, web-based e-mail, such as Gmail, did not exist. Instead, e-mail primarily existed in local intranets where clients would download their messages from the server and the server would, generally, not keep a backup. Congress presumed that any e-mails left on the server for more than 180 days should be treated like abandoned property. This distinction, however, is no longer as relevant today when customers have access to nearly unlimited cloud storage*."

En este sentido citaremos las propuestas de reforma de la ECPA que han adoptado mayor forma:

- "Electronic Communications Privacy Act Amendments Act of 2015," (S.356 -114th Congress (2015-2016)) presentada en el Senado en fecha 2 de abril de 2015, por los senadores Patrick Leahy y Mike Lee, con la principal novedad de la eliminación del limite temporal de protección de los 180 días y de los correos abiertos o no abiertos.
- "Geolocational Privacy and Surveillance Act or the GPS Act" (S.237 -114th Congress (2015-2016)) presentada en el Senado en fecha 22 de enero de 2015, por el senador Ron Wyden y el representante Jason Chaffetz, que entraría a regular más específicamente la limitación de la geolocalización de los aparatos móviles.
- "Email Privacy Act" (H.R.699 -114th Congress (2015-2016)) presentada en la Cámara de Representantes en fecha 2 de abril de 2015 por el Representante Kevin Yonder.

(A la fecha de cierre de este trabajo ninguna ha culminado con éxito su tramitación parlamentaria)

Por tanto, básicamente, la Ley se puede resumir en la creación de una nueva obligación para las empresas de telecomunicaciones. que permita hacer más fácil las interceptaciones de telecomunicaciones por el sistema nacional de escuchas.[436]

Nos encontramos ante una Ley que regula las interceptaciones ante la nueva avalancha que, en los años 90, supuso la generalización del uso de tecnología móvil, y las posibilidades de investigación, principalmente penal, que esas interceptaciones podrían suponer.

Se nos muestra paradigmático que fuera una actuación conjunta de fuerte oposición por parte de las grandes empresas de telecomunicaciones afectadas y de organizaciones de derechos civiles, la que provocó el precepto que establece "pagar la factura" al Gobierno de la "actualización" técnica requerida para esta "colaboración obligada" que se nos presenta en la Ley.[437]

La aplicación de la Ley y su historia de implementación y modificaciones, se ha visto marcada por un continuo "toma y daca" entre los requerimientos del FBI (principalmente aunque también de la DEA) en su actuación, y la oposición de organizaciones civiles de derechos, que se han ido dirimiendo, en muchos casos, por la autoridad de la Comisión (FCC) y en otros casos por actuación judicial.

El Capítulo 9 del título 47 empieza con un subcapítulo primero con el título "Interception of digital and other communications", donde viene contenido el mismo y el principal objeto de la Ley.

Se establecen al inicio las definiciones de rigor, que ya van perfilando su objeto jurídico. Quizá la mayor relevancia definitoria se presenta cuando entra a establecer lo que se entiende por información que identifique al comunicador. Así como al establecer la definición de los servicios de de mensajes electrónicos.[438]

---

[436] Su historial legislativo se encuentra contenido en el informe de la Cámara de Representantes House Report No. 103-827 de octubre de 1994 con el título "Telecommunications carrier assistance to the Government". Debemos además recordar el origen del debate al que se adscribe la Ley en una sentencia de 1977 del Tribunal Supremo. United States v. New York Telephone 434 U.S. 159 (1977). En ella ya se requería a los operadores de telecomunicaciones a prestar la asistencia necesaria para llevar a cabo con éxito una interceptación electrónica"

[437] Si bien ese precepto ofrece más prestaciones a las empresas que a los propios derechos civiles afectados

[438] O qué se entiende por servicios de información, que prácticamente incluyen todos los servicios conocidos de telecomunicaciones para particulares. Parágrafo 1001.

Podremos decir que la carga regulatoria de la Ley recae principalmente sobre el suministrador de telecomunicaciones, al que se obliga a tener la capacidad operativa de poner a disposición de los Gobiernos (en su función de ejecución legal, o teniendo como origen un mandato judicial), la interceptación de toda comunicación por cable o electrónica, de manera identificable y en tiempo y forma variados en función de los requerimientos ejecutivos correspondientes. Es decir, una perfecta puesta a disposición en potencia, incluso simultánea, de estas comunicaciones.[439]

La Ley se promulga con el ánimo de no hacer más gravosa para las empresas suministradoras esta disposición, con diseños específicos de equipos o instalaciones o prohibiciones concretas de los mismos. Y así también, establece la no aplicación de la misma para los servicios de información o de prensa y sus comunicaciones, límite evidente que exige la libertad de información. Si bien también esos servicios excepcionados incluyen el correo electrónico o los accesos a Internet. Es por tanto, una ley pensada para la telefonía o medios de comunicación no fija o "fuera del cable".[440]

Además, para casos de emergencia o de especial necesidad, existe la posibilidad de imponer un determinado formato a las empresas suministradoras. Es decir, permite a la autoridad ejecutiva de que se trate hacerse cargo del control de las mismas.

Continúa la Ley regulando los requisitos técnicos y sus capacidades por parte de las empresas suministradoras, y su obligación de comunicación a las Autoridades correspondientes encargadas de la ejecución legal respectiva. Es decir, la necesidad de comunicación para estas empresas de sus capacidades actuales y hasta donde pueden llegar técnicamente. Una fotografía de su capacidad. Todo ello dentro del ánimo y objetivo de la interceptación.

Además se procede a la comprobación de esas capacidades notificadas por parte de la Autoridad ejecutiva, (principalmente por los fiscales generales), y de la posible expansión de esa capacidad. Llevándose un seguimiento por esa autoridad de las sucesivas actualizaciones de capacidades y su comprobación de conformidad.[441]

---

[439] Parágrafo 1002

[440] Además se impide la carga de la posible necesidad de desencriptación a esas empresas suministradoras. En la letra b) del 1002 encargada de las limitaciones a la misma.

[441] Si bien la autoridad respectiva debe reembolsar los costes de estas actualizaciones a las empresas por ello. Digamos que la necesariedad de la ejecución legal no debe trasladarse a las empresas de telecomunicaciones en su coste plenamente.Parágrafo 1003.

Además, las empresas de telecomunicaciones deben asegurarse de que la interceptación de la comunicación proviene de un título jurídico válido. Contemplándose la consulta y coordinación con proveedores y suministradores necesarios por la empresa de telecomunicaciones para la adecuada cumplimentación de esta Ley.[442]

En cuanto al procedimiento, se adentra la Ley en una mayor regulación tecnificada. Así la letra (a) ("Safe harbor") del parágrafo 1006 nos dice que las Autoridades consultarán la operatividad y eficiencia para la implementación de esos requisitos para la interceptación, en la forma que exige la Ley, por parte de la industria afectada, debiendo cumplir con los estándares de capacidad técnica necesarios. La ausencia de esos estándares no supondrá carga o exclusión para las empresas según el punto 3. Y su letra (b) ("Commission authority") nos dice que si no se llegan a adoptar esos estándares, entraría en juego la determinación de la Autoridad (Comisión). Entendiéndose por ella según las definiciones de la Ley a la "Federal Communications Commission."[443]

Además se da la posibilidad de petición de extensión para el cumplimiento de los estándares por parte de los servidores afectados para la acreditación de su capacidad técnica.[444] E incluso se nos asegura que un Tribunal puede ordenar la ejecución de lo establecido en esta ley, utilizando el poder judicial como garante de esa facilitación ejecutiva que contempla. Establece que el Juez debe determinar plazo razonable para que se pueda afrontar su cumplimiento e impone asimismo limitaciones a la extensión de la orden judicial, que coincide con no exceder los límites razonables de la previa capacidad que se ha ido perfilando por la Autoridad.[445]

[442] Parágrafos 1004 y 1005.

[443] Dándole así un poder ejecutivo renovado en una Ley que, ya de por sí, está hecha por y para la mayor libertad de actuación del brazo ejecutivo estatal estadounidense. Como ejemplo de este amplio poder otorgado a la FCC podemos señalar su reglamentación estableciendo a los VoIP ("Voice over Internet Protocol"), es decir, las llamada telefónicas a través de Internet con banda ancha fue incluida como objeto de aplicación de la Ley por la Comisión. Y ello a través de su decisión de 4 de agosto de 2004 (FCC 04.187).

[444] Letra c del 1006.

[445] Parágrafo 1007. Además el siguiente apartado (1008) establece el 1 de enero de 1995 como fecha clave porque es a partir de la cual las empresas se entienden deberían estar habilitadas para el cumplimiento legal, sin necesidad de ayuda pública de reembolso para afrontar estas obligaciones normativas. A partir de esa fecha ya se deja su apreciación discrecional a la Comisión sobre los acometimientos razonables de estas novedades impuestas por la ley. Además el parágrafo 1009 acoge una previsión económica de lo que costó o costaría la implementación de la Ley. Es decir el control de comunicaciones a efectos de ejecución legal en EE.UU.:500 millones de dólares en 4 años: de 1995 a 1998.

Por último, la Ley ofrece el habitual "feedback" democrático en estas leyes. Principalmente los informes de control democrático serán versados sobre la evolución y desembolso de los pagos contemplados. Tanto por parte del Fiscal General como por el Interventor general del Departamento (ministerio) de Justicia.

2.1.3 Otras determinaciones jurídicas sobre vigilancia electrónica en temas concretos.

Han habido, además de las leyes referidas, algunos pronunciamientos concretos, principalmente jurisprudenciales, sobre asuntos y temas específicos que son de interés para, al menos, ser recogidos y citados.

Sobre la confiscación y requiso de ordenadores personales debemos citar la sentencia recaída en el caso United States v. Andrus 438 F. 3d 711 (10th Circuit 2007), en el caso en que la policía encuentra en un ordenador del hijo del señor Andrus pornografía infantil descargada. El debate se centra sobre la validez del acceso a ese ordenador por la policía y en el uso de contraseñas, que permitieran determinar "el fallo de autoridad" del doctor Andrus sobre su hijo, y todo ello en orden con la Cuarta Enmienda.

Un caso muy interesante se da en el pronunciamiento *Riley v. California* (2014 WL 2864483), en le que se nos presenta voz jurisprudencial del Tribunal Supremo sobre si la policía puede, sin orden judicial, recoger información digital de un móvil confiscado por haber sido su dueño arrestado. El Tribunal rechaza los criterios de los funcionarios y policías de que esto se pudiera permitir en todo caso. Y pone el asunto en contraposición con los necesarios requerimientos de la Cuarta Enmienda, haciendo por tanto inválida aquella actuación del poder público. Y ello, aún conociendo la trascendencia de su decisión para las presumiblemente más difíciles coordinaciones en las investigaciones policiales en un futuro. Y reconociendo que la privacidad tiene un precio.[446]

[446] *"…We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost…"*

Advierte, así, que la extensión de los teléfonos móviles en la población (americana) hace demasiado arriesgado (contrario al espíritu de la lucha de los fundadores de la nación) permitir su vigilancia policial sin orden judicial.[447]

En cuanto a material de encriptación y su relación con la Primera Enmienda podemos poner como ejemplo el pronunciamiento de la sentencia *Junger v. Daley*, (209 F. 3d 481 (6th Circuit 2000)).

Sobre la intervención de los poderes públicos en la vigilancia electrónica y de los correos electrónicos tenemos el caso Steve Jackson games Inc. v. United States Secret Service (36 F. 3d 457 (5th Cir. 1994)), que interpreta la ECPA principalmente en su parte de "Stored Communications Act" y en la de "Wiretap Act". Otro asunto en que se interpreta y juzga relacionado con la privacidad de correos electrónicos lo tenemos en United States v. Warshak (631 F. 3d 266 (6th Circuit 2010)), en el que se realizan igualmente pronunciamientos sobre la "Stored Communications Act" de la ECPA.

Sobre los servicios proveedores de Internet y la privacidad podremos citar la sentencia United States v. Hambrick (55 F. Supp. 2d 504 (W.D. Va. 1999)), que requiere la posible responsabilidad civil de estos proveedores cuando cedan la información de sus registros al Gobierno sin mediación de orden judicial, si bien el asunto no deja claro que exista en ellos para el usuario "expectativa razonable de privacidad".

Para las búsquedas de Internet y las direcciones IP en su relación jurisprudencial con la privacidad podremos citar la sentencia United States v. Forrester (512 F. 3d 500 (9th Cir. 2008)), en la que el Tribunal Supremo interpreta la entrada o no en juego de la Cuarta Enmienda, que en este caso descarta. Y los equipara a los "Pen Registers", dándoles así un similar tratamiento en la ECPA fuera de la previsión constitucional.

[447] *"…Modern cell phones are not just another technologicalconvenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life,". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple— get a warrant…."*

2.2 Regulación legal con incidencia externa.

2.2.1 Foreign Intelligence Surveillance Act (FISA)[448]

En su inicio y como justificación de creación de la Ley podemos encontrar, como ya estudiamos, la separación jurisprudencial que para la interceptación de comunicaciones se produjo en la sentencia del Tribunal Supremo United States v. U.S. District Court, 407 U.S. 297 (1972) ("Keith Case"); en la que se distinguieron las diversidades para la intromisión en los derechos de privacidad procedentes de investigaciones criminales corrientes, de aquellas que pudieran afectar a la seguridad nacional, manteniendo sin embargo la necesidad de equilibrio entre derechos de los ciudadanos y la inteligencia nacional.[449]

Por tanto, con esta Ley en 1978 se creaba un régimen legal separado para el tratamiento de la vigilancia por motivos de inteligencia nacional. En 1994 y en 1998 va ampliando su capacidad de actuación, extendiéndose no solo a escuchas, sino también a la vigilancia física y a los "pen registers".

Así, la FISA es una norma antigua pero profundamente modificada y casi condicionada en su espíritu, sobre todo por los ataques terroristas perpetrados en suelo americano el 11 de septiembre de 2001, con la *USA Patriot Act*. Además, *The Protect America Act* del año 2007 introdujo cambios importantes con previsión inicial de aplicación transitoria. Por último, en 2008 la *FISA Amendments Act* (FAA) introdujo cambios, tras las revelaciones del año 2005 sobre el programa de vigilancia extensiva que se planeaba por la *National Security Agency* (NSA), para las escuchas de llamadas internacionales

[448] De utilidad habitual para este trabajo ha resultado la consulta de los resúmenes y consideraciones de EPIC sobre la FISA. (Recuperado el 2 de agosto de 2018): https://epic.org/privacy/surveillance/fisa/

[449] "*Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.*"

sin orden judicial. Esta modificación introdujo garantías nuevas a la privacidad, si bien al mismo tiempo, ampliaba la capacidad de vigilancia gubernamental.[450]

La FISA resulta, además, importantemente matizada por la *USA Freedom Act* del año 2015, producto de las revelaciones de Snowden (y que estudiaremos más adelante), provocando una mejora sustancial y ciertos avances en lo que a protección de la privacidad se refiere.

La Cuarta Enmienda constitucional, como vimos, establece la necesidad de causas razonables para sospechar ("probable cause to believe") de la comisión o posible comisión de crímenes que justifiquen una orden de vigilancia. Esta norma general se desvanece en la FISA. La causa probable se basa simplemente en razón de extranjería. No hace falta que medie sospecha de actividad criminal posible.

Para personas estadounidenses la vinculación criminal requiere sospecha de espionaje o de disposición a potencia extranjera.

En todo caso se hace un rodeo por la Ley, ya que permite utilizar esa información obtenida "vía FISA" para blandirla y utilizarla en procesos criminales de otro tipo. Y ello, a pesar de los procedimientos de minimización ("Minimization procedures"), que intentan separar las investigaciones y la utilización de la recopilación de información por motivos de inteligencia de otros ámbitos más comunes.

Además, la FISA establece un sistema jurisdiccional especial para el control judicial de lo establecido en ella, el llamado "Foreign Intelligence Surveillance Court (FISC)"

Debemos añadir que el número de órdenes judiciales de vigilancia electrónica expedidas al amparo de esta Ley ha ido aumentando significativamente, desde las 199 órdenes que se dieron en 1979 hasta las 886 del año 1999. En 2004 fueron 1758. Ello sin contar claro está, aquellas que no necesitan de autorización judicial según el dictado de la Ley, de acuerdo con Solove & Schwartz (2015, 422).

[450] Que veremos en los dictados del parágrafo 1802 letras (a) (b 2) (c) y (e)

Debemos asimismo aclarar, previamente a su estudio, el marco institucional de aplicación[451] de la Ley, que estará compuesto por los siguientes organismos y agencias gubernamentales:

-La "Federal Bureau of Investigation" (FBI) creada en 1908, si bien bautizada con su nombre actual en 1935, encargada no solo de la persecución criminal a nivel federal, sino también de asuntos de inteligencia y contraterrorismo.

-La "Central Intelligence Agency" (CIA), que nace de la Office of Strategic Sevices creada en 1942 para las tareas de espionaje que requería la entrada en la Segunda Guerra Mundial de Estados Unidos, si bien no hubo continuación legal ya que ésta se disolvió tras finalizar la guerra, y la CIA se habilitó con la "National Security Act" firmada por el presidente Truman en 1947.

- La "National Security Agency" (NSA), perteneciente al Departamento de Defensa, y encargada de labores de encriptación, nace en 1952 de la mano del mismo presidente Truman.

- Otros Organismos que dependen de otros departamentos ministeriales. Como ejemplos hablaremos de la Defense Intelligence Agency (DIA), o del State Department`s Bureau and Research (INR), o de la Oficina del Departamento del Tesoro encargada de Terrorismo e Inteligencia Financiera.

2.2.1 a) Análisis de la Ley

Nos encontramos ante una extensa norma contenida y codificada en el Título 50 del U.S.C., en su capítulo 36 bajo el enunciado "Foreign Intelligence Surveillance". Este capítulo se subdivide en 7 subcapítulos que se dividen fundamentalmente por el tipo de vigilancia y los requisitos de las mismas.

El subcapítulo I "Electronic Surveillance", contiene el principal objeto normativo, ya que se se encarga de la vigilancia electrónica en el ámbito que cubre la Ley, ocupando los parágrafos que van desde el 1801 al 1812.

[451] Siguiendo la sistematización al efecto proporcionada por Solove & Schwartz (2015, 412)

En primer lugar se establecen las definiciones que se aplican en este tipo de vigilancia, siendo especialmente relevante el concepto de "potencia extranjera".[452]

Utiliza la norma el tipo de definiciones jurídicas que se dejan plenamente abiertas o que directamente provocan confusión. Y por supuesto no ayudan a proceder al acotamiento de un claro objeto y sujeto jurídico.

Incide de manera más persistente la Ley en la larga definición de la letra b) del precepto 1081, que trata de definir a estos efectos legales al "agente de potencia extranjera". En el número 1 de la letra se habla de cualquier persona no estadounidense que:

– Esté empleado por alguna potencia extranjera (según la confusa definición precedente).

– O bien actúe de su parte en actividades de inteligencia clandestina o bien las ayude o promueva.

– O bien esté vinculada al terrorismo internacional y su preparación o a la proliferación internacional de armas de destrucción masiva.

Vemos como se va dibujando claramente el sentido de la Ley sobre todo a partir de las reformas posteriores a los atentados del 11 de septiembre de 2001.

Sigue el punto 2 de la letra b) con la definición de agente de potencia extranjera pero ya sin atender al criterio de nacionalidad negativa estadounidense, y habla de cualquier persona que:

– Se encuentre vinculada o comprometida o dirigida de manera consciente con o por la inteligencia clandestina de una potencia extranjera si ello implica la violación de la Ley penal estadounidense.

– Se encuentre vinculada o comprometida de manera consciente con el sabotaje o el terrorismo internacional o en su preparación vinculado a potencia extranjera.

[452] Precepto 1801. Por "potencia extranjera" no solo establece a Estados constituidos como tales, reconocidos o no por la Organización de Naciones Unidas, sino a todo elemento que tenga relación con el ejercicio de soberanía estatal, o a cualquiera entidades gubernamentales extranjeras distintas a la estadounidense. Además de esa vinculación, que obedecería más a los patrones clásicos, se nos presenta como "potencia extranjera", a los efectos de la ley, a los grupos vinculados al terrorismo internacional y aquellos destinados a su preparación o entrenamiento, así como los vinculados al manejo y uso de armas de destrucción masiva. Además de a organizaciones políticas extranjeras que no se componga de manera sustancial por personas estadounidenses.

– Que de manera consciente haya entrado en los EE.UU. bajo identidad falsa o fraudulenta al servicio de potencia extranjera.

Para los dos primeros supuestos también se incluyen a quienes los ayuden o induzcan o así conspiren de manera consciente.

Parece que el criterio de nacionalidad se incluye aquí solo matizado por el concurso o no de la ley penal en el supuesto de que se trate. Confundiéndose la condición extranjera con la fuerza de la ilicitud penal originada allende de las fronteras estadounidenses.[453]

Así, por tanto, la letra c) perfila el terrorismo internacional como el de aquellas actividades que:

– Impliquen actos violentos o peligrosos para la vida humana en violación de la ley penal de EE.UU. o de sus Estados en territorio estadounidense, o

– Parezcan tener intención de intimidar a la población, influenciar la política de un gobierno por coerción o intimidación, o de afectar a la política de un gobierno por medio de asesinatos o secuestros.

– Ocurran fuera de EE.UU. o trasciendan las implicaciones nacionales por los medios ejercidos, personas que intenten la coerción o intimidación o el lugar en que los criminales operan o solicitan asilo.

Como se puede observar la determinación es sumamente amplia en la incidencia de la Ley.

La letra e) nos presenta la definición de información de inteligencia extranjera, que básicamente se refiere a aquellas labores para prevenir ataques, sabotajes y terrorismo internacional, actividades de inteligencia clandestina, que afecta a la defensa nacional a o las relaciones exteriores. Básicamente y resumiendo, labores de espionaje.[454]

[453] Después se van explicando algunos términos de esas dos grandes definiciones principales, de entre las que destacaremos algunas, como los de las subsiguientes letras del precepto.

[454] La letra f) nos ofrece que entiende la Ley por vigilancia electrónica que podríamos resumir en la adquisición por cualquier medio de comunicaciones o la instalación de aparatos para su captación. Con la clausula constitucional de "razonables expectativas de privacidad" y mediante "orden judicial":
"Under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes". Dictado establecido en el respeto a la cuarta enmienda constitucional.

La Ley establece, acto seguido de las definiciones, la importante habilitación para la autorización presidencial a la vigilancia electrónica sin autorización judicial.[455]

Se da en aquellos casos en que entre en juego la definición de "potencias extranjeras" en las comunicaciones y solo entre ellas. Es decir, que en principio no puede afectar a ciudadanos o residentes legales de EE.UU.[456]

Este tipo de autorización solo se puede dar bajo la estricta atención a esos procedimientos y en coordinación con las certificaciones del Fiscal General, que deberá prestar conformidad y asesoramiento, e informar de ello al Comité del Senado estadounidense al efecto.[457]

Con la modificación de 2015 de la *USA Freedom Act* se añaden algunos puntos al precepto, incluyéndose la figura del "amicus curiae" a estos tribunales, figura tradicional romana y elemento habitual en el Common Law, que consiste en la incorporación de profesionales y terceros, en causas de especial interés y controversia públicas. La Ley, en su designación, pone su atención especial en profesionales de la privacidad y de los derechos civiles. Esta figura aportará asistencia y consejo legal y técnico sobre la decisión judicial a tomar.[458]

La Ley prosigue con la regulación de procedimiento para establecer las órdenes gubernamentales o administrativas para petición al Poder Judicial de la aprobación de escuchas, que deberán ser aprobadas previamente por el Fiscal General.

---

[455] Precepto 1802. Estas autorizaciones no pueden ser por tiempo superior a un año y necesitan de una certificación bajo juramento del Fiscal General de EE.UU. Que acredite una serie de extremos de garantía necesarios que justifiquen no seguir el cauce habitual judicial.

[456] Tal y como establece la definición del precepto 1801 en su letra h) y que establece las definiciones de los procedimientos competencia del Fiscal General. Estos procedimientos autorizados o "minimizados" ("Minimization procedures") por el Fiscal General son los que deben seguirse para estas "interceptaciones presidenciales" de las comunicaciones.

[457] Parágrafo 1803. Se establece un tribunal especial al efecto para vigilar estas vigilancias electrónicas que regula el subcapítulo. Presentando curiosidad ver cómo deben estar estos tribunales alejados al menos 20 millas en su residencia del "ruido político" del distrito de Columbia (y por tanto de Washington capital). Este Tribunal solo se reunirá en Pleno para aquellas decisiones que requieran establecer la uniformidad de criterio en la decisión o para cuestiones de especial importancia. Estableciéndose la posibilidad de revisión que se reserva al Tribunal Supremo. En los siguientes puntos del precepto se establecen criterios de organización y de procedimiento del Tribunal entre los que destacaremos: la determinación de que estos procesos se sustancien con celeridad, que sean expeditos y que el tiempo de prestación de servicios de los jueces no puede ser renovable, siendo el máximo del cargo de 7 años.

[458] *"...the presiding judges may consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board, the judges determine appropriate*..."

Los requisitos que deben reunir estas peticiones se desarrollan extensamente, en el que además de las correctas identificaciones de los solicitantes y de los "objetivos" de vigilancia, destacan los necesarios para su justificación, así como el plazo para las mismas y otras exigencias de forma.[459]

Podemos observar aquí gran dosis de excepcionalidad, con posibilidad de quiebra del principio de separación de poderes, ya que permite y por requerimiento de los directores de las principales agencias de inteligencia e investigación, que el Fiscal General revise esas órdenes judiciales.[460]

El "Issuance of order" es la definición de regulación en la norma que se encarga de la expedición de la orden de escuchas por parte del Juez. Si se cumplen los requisitos legales para la expedición de la orden se deja poco margen de maniobra al juez, ya que se antoja más una garantía jurídica de esos requerimientos, que propiamente de un órgano decisor en el inicio de la tramitación.[461]

En la línea de excepcionalidad propia de la regulación estadounidense de la privacidad, se establecen los caracteres de la orden para casos de emergencia u órdenes de emergencia.

Además, la Ley estipula que el uso de la información procedente de estas autorizaciones de escuchas estará (evidentemente) adecuado a las personas autorizadas para su uso y al objeto de su autorización.[462]

Importante nos parece que se prevé la posibilidad de supresión del uso de esa información, cuando haya sido obtenida sin los requisitos y garantías que exige la Ley. También relevante nos resulta la posible revisión judicial de la autorización de

[459] Precepto 1804. Sin perjuicio de que el Fiscal General solicite cualesquiera otras informaciones y certificaciones que estime necesarias, atribuyéndole además un especial poder de revisión.
[460] Para los casos del punto 2 de la letra b) del 1801
[461] Letras a y c del parágrafo 1805. Sin perjuicio de que el Fiscal General solicite cualesquiera otras informaciones y certificaciones que estime necesarias, atribuyéndole además un especial poder de revisión. Otras características de la orden como su duración y revisión, se darán por el "periodo necesario para conseguir sus objetivos" o en general para 90 días. Si bien si se trata de determinadas escuchas puede llegar a ser de 1 año. O también de 120 días, si se trate de un "agente de potencia extranjera" que no tenga la nacionalidad estadounidense. Todo ello con la posibilidad de extensión en los mismos términos con la limitación temporal máxima de 1 año.
[462] Precepto 1806. No se puede divulgar o publicar esa información y para un uso ajeno a los propios de los órganos y funcionarios federales legalmente habilitados para ello (en caso de otras instancias administrativas o estatales) se deberá notificar debidamente a la "aggrieved person" de ello.

vigilancia. Deja así, en los dos casos, ciertas garantías de actuación para los particulares afectados o por los juzgados vigilantes ante posibles actuaciones ilegales.

Se establece, asimismo, la garantía de supresión de pruebas obtenidas ilegalmente, así como la garantía de la destrucción de información recopilada de manera no intencionada o irrelevante al caso y que pueda vulnerar la privacidad. Deja a discreción del juez aquellas vigilancias realizadas empleando la categoría de urgencia y que después no son ratificadas, pudiendo posponerse, suspenderse o eliminarse igualmente.

Termina el subcapítulo con la previsión de informes democráticos. Un informe general anual por parte del Fiscal General al equivalente al Consejo del Poder Judicial, y al Congreso (todos los meses de abril de cada año). Otro informe dirigido a los diversos comités constitucionales, y sobre una base semestral y de carácter más pormenorizado. Y un informe más excepcional y casi de tipo estratégico, cuatrienal, para temas de Inteligencia. Se prevén además, las posibles responsabilidades de tipo penal y civil por estas vigilancias.[463]

El Subcapítulo II "Physical Searches" se enmarca en la vigilancia física de los ciudadanos u "objetivos" como deshumanizadamente viene refiriéndose la Ley. Abarca los parágrafos que van desde el 1821 al 1829.

Comienza con una reproducción de las definiciones analizadas anteriormente para la vigilancia electrónica del anterior subcapítulo, con algunas variaciones en el perfil de "Aggrieved person" o en el de "Minimization procedures". De nueva importancia se presenta la definición que da pie al subcapítulo sobre "seguimiento o vigilancia física", sin incluir la vigilancia electrónica o información de inteligencia sobre el extranjero.[464]

Continúa el dictado legal con el núcleo regulatorio que se sumerge en la privacidad por razones de seguridad (en este ámbito físico). En él se siguen unos parámetros muy similares a los vistos en la vigilancia electrónica. La autorización presidencial obedece a

[463]La guerra, como es sabido, lo altera y excepciona todo, y lo primero, el Estado de Derecho. Así consecuentemente se establece al final del subcapítulo la regulación diferenciada para tiempos de guerra. Parágrafos 1807 a 1811.
[464] Precepto 1821

los mismos requisitos y a las mismas garantías procedimentales, debiendo el Fiscal General establecer persona custodia en estas vigilancias físicas.[465]

Sigue también de manera muy similar lo establecido en la vigilancia electrónica para la solicitud de la orden de vigilancia y su aprobación y ejecución. Con algunas diferencias propias de las características de la vigilancia física, como puede ser la duración tipo de la misma. En este caso 90 días o 120 días (sin esa duración prolongada de una año), si bien se comparte la premisa temporal de "el tiempo necesario que requiera la investigación". También se comparten la existencia y los requisitos generales de las órdenes de emergencia.[466]

Caso práctico judicial concreto donde se ubica esa invocación de emergencia así como sobre la necesidad o no de "warrant", es el de Global Relief Foundation, Inc v. O'Neil.[467]Creándose un fallo procedimental con la discordancia entre la invocación de emergencia y la posterior aprobación de no necesidad de orden judicial, reconociéndolo así el Tribunal. Si bien no deja por ello de validar la actuación sobre la "causa probable" para creer que los ejecutivos de la "Global Relief Foundation" eran agentes de potencia extranjera según los términos de la Ley.[468]

Siguiendo con la Ley, el artículo referido al uso de la información es prácticamente copia del establecido para las vigilancias electrónicas. Y también el que viene referido al

[465] Parágrafo 1822

[466] Precepto 1823 ("Application for order") y el precepto 1824 ("Issuance of order")

[467] Global Relief Foundation, Inc v. O'Neil 207 F. Supp. 779 (N.D. I11. 2002)
En este caso juzgado en Illinois, y que se contextualiza en las postremerias de los atentados del 11 de septiembre de 2001, agentes del FBI registran la sede de esta Fundación encargada de dar ayuda humanitaria "islámica", y lo hacen el 14 de diciembre de 2001, en relación con las investigaciones de los atentados. Lo hacen sin orden judicial ("warrant") basándose el Fiscal del Estado en la excepción de la FISA para situaciones de emergencia. Si bien el Tribunal especial (FISC) aprobaría una actuación sin necesidad de ese tipo de orden posteriormente.

[468] "*…We conclude that the FISA application established probable cause to believe that Global Relief and the executive director were agents of a foreign power, as that term is defined for FISA purposes, at the time the search was conducted and the application was granted (…)*
This Court has concluded that disclosure of the information we have reviewed could substantially undermine ongoing investigations required to apprehend the conspirators behind the September 11 murders and undermine the ability of law enforcement agencies to reduce the possibility of terrorist crimes in the future. Furthermore, this Court is persuaded that the search and seizure made by the FBI on December 14 were authorized by FISA. Accordingly, we decline plaintiff's request that we declare the search invalid and order the immediate return of all items seized."

informe de corte democrático sobre las autorizaciones aprobadas y llevadas a cabo que tendrá periodicidad semestral.[469]

El Subcapítulo III ("Pen registers and trap and trace devices for foreign intelligence purposes")[470] abarca los parágrafos del Código que van desde el 1841 hasta el 1846.[471]

Merece un comentario que para los términos "pen register" y "trap and trace device" se nos deriva al siguiente contenido establecido en la parte del U.S.C. en materia penal, y que consecuentemente tiene un efecto general que afecta a varias leyes (como a la "Pen Register Act" citada), en su definición y por lógica, seguridad jurídica. Se añade igualmente con la reforma de la *USA Freedom Act* el término "specific selection term", ya que se exige, tras el conocimiento de los hechos expuestos por Snowden, la necesidad de concreción de "la persona, cuenta, dirección o aparato (device) personal o cualquier otro identificador personal" y limitado para el fin de investigación concreto, para permitir el uso de estos mecanismos del subapartado.[472]

Se prosigue fijando el uso de estos aparatos en este ámbito de la Ley. Aquí, la solicitud viene comprendida para la figura del Fiscal General, y su aprobación está en manos de los Tribunales, observándose la no intervención del poder ejecutivo y presidencial en este campo, o no al menos de manera directa o de una forma tan clara como en anteriores procesos de vigilancia (principalmente en la "Electronic Surveillance").[473]

Se siguen igualmente los parámetros y requisitos de las autorizaciones en situaciones de emergencia estudiadas. Y se repite dictado para tiempos de guerra.

---

[469] Esta segunda parte legal se encarga también de los ilícitos penales cometidos en infracción de las garantías de este subcapítulo. Así como de la posible responsabilidad civil. Repitiendo el estipulado de la habitual regulación de falta de necesidad de regulación y procedimiento en tiempo de guerra. Preceptos 1825 a 1829

[470] Al igual que lo visto en la anterior Ley en clave interna, la *Electronic Communications Privacy Act of 1986* (ECPA) en su tercera parte de "Pen Register" aquí se repiten esas regulaciones de uso de estos artefactos, esta vez en su aplicación a la "inteligencia exterior".

[471] Las definiciones de este subapartado siguen la estela de los definidos en las anteriores parte de la ley y siguiendo el mismo esquema empiezan con ellas en su ("Definitions") (Parágrafo 1841)

[472] Y ello sin que pueda incluir el identificador del proveedor de telecomunicaciones ni una región geográfica amplia (en su ánimo de concreción de investigación) para su uso. Añadido el punto 4 del parágrafo 1841.

[473] También se establece la posibilidad y los requisitos de la solicitud a instancia de parte. Y la limitación temporal de 90 días, compartiendo cómputo con otras anteriores ya vistas, o de un año para tratamiento extranjero, al igual que en la comunicación electrónica. Parágrafo 1842.

Para el "uso de información" se sigue, de igual manera, lo ya legislado bajo esta misma titulación en los anteriores capítulos, con la regla general de no divulgación, y el establecimiento de todas las cautelas y requisitos garantistas en ese uso recabada por estos medios.[474]

En 2015 se añade por la USA Freedom Act el parágrafo 1845 que regula el uso de la información obtenida a través de estos artilugios, añadiendo toda una serie de garantías como, entre otras, la "moción de supresión" de su contenido por persona agraviada, igual que lo visto en el anterior subcapítulo, las notificaciones necesarias así como el efecto de invalidez para los obtenidos ilegalmente. La vigilancia del Congreso también se añade en esta reforma legal con el añadido del parágrafo 1846.

Como ejemplo jurisprudencial de lo recogido en este subcapítulo legal podremos referirnos al caso United States v. Isa[475] (por la utlización de micrófonos ya que la justificación mantiene la referencia al parágrafo 1801 del primer subcapítulo, y de corte general para toda la Ley).

En esta ocasión se nos ofrece un ejemplo de la utilización de la información vigilada para fines distintos a su autorización, si bien el Tribunal, alegando el 1801 (h)(3) y el 1806 (b) (f) de la Ley que autorizan la retención y utilización de este tipo de pruebas que evidencian un delito, mantuvo la condena y denegó la pretensión de los apelantes.[476]

---

[474] De igual manera se nos ofrecen las previsiones de control democrático semestral en forma de informe al Congreso por el Fiscal General. Parágrafos 1845 a 1846.

[475] United States v. Isa 923 F. 2d 1300 (8th Circuit 1991)
La familia Isa (Zein Hassan Isa y su mujer María Matias) estaba siendo vigilados con micrófonos ocultos en su casa, ya que se sospechaba por el FBI que el padre de familia (y ciudadano naturalizado americano) era un agente de la Organización para la Liberación de Palestina (OLP). Si bien una tarde surgió una prueba de voz en la que la pareja reconocía el asesinato de su hija de 16 años. Los Isa fueron condenados a pena de muerte por el Estado de Missouri, donde residían. Si bien apelaron a que las grabaciones fueron hechas con un propósito de seguridad nacional y debían ser destruidas y no utilizadas en su contra, al tratarse de un caso de crimen "doméstico".

[476] *"…Notwithstanding the minimization procedures required by 50 U.S.C. §§ 1804(a)(5), 1805(b)(2)(A) and defined in 50 U.S.C. § 1801(h), the Act specifically authorizes the retention of information that is "evidence of a crime", 50 U.S.C. § 1801(h)(3), and provides procedures for the retention and dissemination of such information. 50 U.S.C. § 1806(b)-(f). (…)*
Thus, we conclude that the tapes are "evidence of crime" and that the district court correctly denied appellant's motion to suppress. 50 U.S.C. § 1801(h)(3)…"

El Subcapítulo IV, "Access to certain business records for foreign intelligence purposes", extiende la maquinaria de vigilancia e introduce al verdadero "caballo de Troya" estadounidense, a estos efectos, en todo el mundo: sus empresas. Entra a regular ese acceso a los negocios que vendan cosas tangibles (es decir, la gran mayoría, ya que incluye libros y producción intelectual),[477] ofreciéndose una vigilancia global a través de sus empresas multinacionales de distribución presentes en todo el mundo, ya que se permite al FBI el acceso de investigación a los registros de las mismas, y con los requisitos vistos anteriormente (intervención del Fiscal General, etcétera). El Subcapítulo comprende los parágrafos 1861 y 1862.

El precepto 1861 regula ese acceso a través de mandato judicial necesario para una investigación criminal en el ámbito de la Ley. Detalla los requisitos y motivación que la solicitud al juez o tribunal debe contener. También puede iniciarse a instancia de parte (letra c), y se protege la buena fe de terceros (letra e). Cabe la posibilidad de revisión judicial (letra f), y al igual que en lo ya analizado, el procedimiento especial de "Minimization procedures" (letra g), con el especial protagonismo en él del Fiscal General.

El precepto 1862 recoge el habitual control democrático, con ciertas variaciones derivadas de la materia. Mantiene su periodicidad de 1 año al Comité de Inteligencia de la Cámara de Representantes y al Comité Judicial del Senado, y en abril a los Comités permanentes de las Cámaras. Todos han de ser presentados por el Fiscal General. Si bien ambos preceptos se han matizando mucho a partir de la reforma de 2015, que mejora las garantías que venían en él establecidas. Esta reforma añade, además, el precepto 1864 que aporta una "contraprestación" a la Seguridad, como es la notificación por el operador de telecomunicaciones de su cambio de política de almacenamiento de llamadas y archivos sobre las mismas en caso de periodos de retención inferiores a 18 meses. Y que el Director de la "National Intelligence" debe notificar al Comité de Inteligencia del Congreso.

El Subcapítulo V "Oversight" contiene los preceptos 1871 a 1874, y se encarga de la supervisión de corte democrático sobre los estipulados y ejecución de la Ley. El 1871

[477] *"... of any tangible things (including books, records, papers, documents, and other items)"*

regula el informe semestral del Fiscal General, que incluye un enfoque integral e información completa de los diversos tipos de autorizaciones aprobadas conforme a esta Ley y su resultado, así como justificaciones y objetivos a un nivel más global. Y ello, con carácter semestral.

La *USA Freedom Act* de 2015, además de cambiar el nombre al subcapítulo, añadió los tres presceptos 1872, 1873 y 1874, imponiendo la desclasificación de las decisiones y opiniones importantes de los FISC (los tribunales específicos previstos en la Ley) que ofrezcan interpretación de Ley, haciéndolos públicos, con la limitación de no poner en juego la seguridad nacional. Además añade una serie de informes anuales de carácter democrático-institucional, principalmente dirigidos a los Comités de Inteligencia y Seguridad del Congreso. Además de la necesidad de Informes públicos de carácter semestral sobre el número de órdenes directivas o "national security letters" y requerimientos recibidos.

El Subcapítulo VI, "Additional procedures regarding certain persons outside the United States", sigue la estela de la determinación de especialidades a la regla general de la ya de por si especial regulación de vigilancia norteamericana.[478]

Se ofrece como principal regulación de este apartado toda una especialidad normativa total al procedimiento general para la vigilancia de personas fuera del territorio de EE.UU. Con motivo de esta investigación "de inteligencia", y por el plazo máximo de 1 año. Establece limitaciones que son más de forma que de fondo, y que pudieran resumirse en la evitación de las equivocaciones no intencionadas. Además de los requisitos de este procedimiento y la habitual excepcionalidad de los "Minimization procedures" y sus criterios generales.

Importante es señalar el mantenimiento de garantía necesaria en derecho de posibilidad de revisión judicial en cada uno de los campos, como mínimo imprescindible.

[478] El subcapítulo ofrece esta regulación diferenciada en sus preceptos desde el 1881 al 1881g. Empieza esta parte con los términos previstos en el precepto 1801 iniciático de las definitorias. Si bien se presentan algunas definiciones adicionales que se redirigen a algunas establecidas en el U.S.C. y que entrarían en juego en este subcapítulo.Precepto 1881.

Se nos habla igualmente de las normas generales que se da el Fiscal General para el cumplimiento de las limitaciones establecidas en la Ley.[479]

Se sigue con las excepciones a lo excepcional para "objetivos" de vigilancia no asimilables en los preceptos anteriores. Y se prevé la posibilidad de solicitudes y autorizaciones conjuntas que aúnen elementos comunes de estos supuestos de autorizaciones.[480]

Por ultimo en el Subcapítulo VII, "Protection of persons assisting the government", se blinda a aquellas personas que colaboran y asistan en su ejecución. Está contenido en los preceptos 1885 a 1885c.

Se recogen las habituales definiciones, todas ellas ya recogidas anteriormente, a excepción de lo que se entiende por "Asistencia". Y entra a legislar el blindaje de la colaboración o asistencia en este campo con las medidas gubernamentales, sin que se les pueda demandar a estas personas ante la jurisdicción civil por este motivo. Y se marcan claramente las preeminencias legislativas impidiendo a los Estados inmiscuirse (aún en el ejercicio de sus competencias) cuando afecten a este campo en el ámbito civil. Manteniendo así la protección referida en este subcapítulo en todas las demarcaciones territoriales estadounidenses. Por último mantiene la necesidad de informe democrático al Congreso en lo acaecido al paraguas de este subcapítulo.

[479] Y de los requisitos que debe reunir la certificación o documento jurídico del Fiscal General que apoye esta excepcional intervención en la privacidad. Y se desgrana la posibilidad de revisión judicial y las distintas regulaciones de esos procedimientos.Precepto 1881ª
La regulación de excepcionalidad continúa, si bien regulándose acto seguido el nivel judicial de revisión ya que la excepcionalidad se da para personas dentro del territorio estadounidense. Se establecen las jurisdicciones competentes para ello, las limitaciones y el contenido y forma de las solicitudes, siguiendo como regla general en estos parámetros de actuación judicial similitud a los ya establecidos para el proceso general (de este subcapítulo de excepcionalidad). Precepto 1881b.

[480]Se remite La Ley a la regulación general de vigilancia de la legislación en el uso de información contenida en el precepto 1806 de esta Ley. Y por último los informes democráticos habituales para dar una "fotografia" al Congreso de lo que hace en el sentido de este subcapítulo el brazo ejecutivo. Parágrafos 1881c, 1881d, 1881e y 1881f.

2.2.1 b) Ejemplo de Revisión Judicial del FISC. El caso *In Re Sealed Case*.[481]

Este caso es el primer pronunciamiento de revisión que el Tribunal especial de revisión de los propios miembros del Tribunal FISC, creado por la FISA, tiene que abordar.

En 2002 el Fiscal General Ashcroft envió al FISC ("Foreign Intelligence Surveillance Court") para su aprobación, su propuesta de "procedimientos de minimización" definidos en el parágrafo 1801 (h) de la Ley. El Tribunal (FISC), preocupado por las repercusiones que en septiembre de 2000 tuvieron ciertos errores en esas solicitudes, y que se dejaron ver en el Informe del Congreso sobre los atentados del 11 de septiembre del siguiente año, decide rechazar esos procedimientos.

Estos fallos fueron provocados por la falta de colaboración entre las autoridades de vigilancia penal y las de inteligencia así como la falta de puesta en común entre las aplicaciones FISA aprobadas (algunas con errores en sus objetivos-personas), a través de esos procedimientos de minimización y el FBI.

Así, el Gobierno recurre esta decisión ante el propio FISC y tenemos este primer pronunciamiento de este Tribunal de apelación o segunda instancia (dentro de la especialidad jurisdiccional de la FISA), que se pronuncia expresamente sobre esa situación de barreras ("walls" como se popularizó por la prensa norteamericana) entre los órganos de investigación. Elemento que saltó a la luz en las investigaciones del Congreso sobre las previas investigaciones, que no consiguieron evitar el ataque a las Torres Gemelas de Nueva York (National Commission, 2004).

El Tribunal trata de solventar este tema y de interpretar correctamente la FISA para que no se den esos errores interpretativos que puedan provocar fallos en la seguridad. Y pasa a pronunciarse sobre si la FISA, tras las últimas modificaciones que había sufrido con la *USA Patriot Act* (que veremos seguidamente es una ley omnibus en materia de seguridad), era coherente con la Cuarta Enmienda. No puede aportar, al final, una verdadera solución jurisprudencial al tema, dejando una incierta aseveración de que si

[481] In Re Sealed Case 310 F.3d 717 (FIS Ct. Rev. 2002)

bien la FISA (a ese momento de redacción) tenía una justificación plena, algunos de los procedimientos de "minimización" aprobados bajo su manto y que se juzgaban aquí, "si no reunían los requisitos mínimos de la Cuarta Enmienda, se le acercaban."[482]

2.2.2 USA Patriot Act de 2001

Nos encontramos ante una verdadera Ley *mainstream* que sobrevuela y afecta a una buena parte de la legislación estadounidense sobre privacidad, introduciendo modificaciones de calado en ella, basadas en la seguridad nacional como premisa y fin último. Además de esos preceptos modificadores de leyes distintas, y que, ya en su conjunto hemos estudiado en ellas, esta Ley presenta, además, unas determinaciones propias en materia de privacidad que en cuyo estudio nos centraremos principalmente aqui. Es verdad también que en junio de 2015 se aprueba la *USA Freedom Act* que viene a presentarse como contrapartida a esta *USA Patriot Act* (sobre todo en la modificación del dictado de la FISA), a la cuál, asimismo, modifica en algunos puntos (principalmente en su sección 215).[483]

Su título confuso y algo engañoso "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", hace entender la citación habitual resumida de la Ley. La norma, de extensa longitud, abarca un gran abanico de cambios legislativos en pos de la ultradefensa de la seguridad estadounidense, implicando varias secciones con multitud de títulos y de amplio espectro sectorial.

---

[482] En la conclusión de la sentencia por el Tribunal (FISC) nos dice: *"FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from "ordinary crime control." After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date. We acknowledge, however, that the constitutional question presented by this case — whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer (…)*
Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from Keith, that FISA as amended is constitutional because the surveillances it authorizes are reasonable…"
Contraviene y deja sin efecto así la decisión del FISC en primera instancia.

[483] Si bien prorroga elementos clave de la USA Patriot Act hasta 2019. Será objeto de atención más adelante.

En cuanto a la aprobación de la Ley llama la atención que semejante redacción legislativa se presentara al Congreso en menos de una semana tras los ataques del 11 de septiembre de 2001. Firmándose por el Presidente George W. Bush el 26 de octubre de ese año. Será recordada así como la Ley con menor discusión parlamentaria en la historia del procedimiento legislativo de los Estados Unidos.[484]

Debemos comentar además que muchas de las medidas en materia de vigilancia y de socavación de los derechos de privacidad estaban ya elaboradas y habían sido propuestas antes de los ataques terroristas. Digamos que aprovecharon el "paso del Pisuerga por Valladolid" y de los infaustos aviones por Nueva York para aprobar unas medidas restrictivas de las libertades personales, en aprovechamiento del momento político y de conmoción que se vivió.[485]

Como elemento político discordante en la tramitación legal debemos recordar la posición del Senador Russ Feingold (Demócrata por el Estado de Wisconsin), único legislador que se opuso a la Ley y advirtió siempre de sus posibles efectos perjudiciales.[486]

---

[484]Su versión de base fue la "Anti-Terrorism Act of 2001 (ATA)", de mayor alcance restrictivo para las libertades, y que contenía verdaderas disposiciones propias de sistemas no democráticos en cuanto a las prerrogativas del Gobierno actuante (el proyecto contenía un sistema de vigilancia masiva con escasísimos controles legales). En cualquier caso, esa situación de flaqueza comprometida de las libertades individuales se sigue observando en la versión final. O, si se quiere, como una declaración de estado de excepción en forma legal.

[485] Podesta (2002) Profesor de la universidad de Georgetown y jefe de Personal de la Casa Blanca con Bill Clinton entre 1998 y 2001 habla de la posibilidad de una auténtica caza de brujas por el mero hecho de ejercer la libertad de opinión, utilizando el antiterrorismo como coartada permanente, y hace una crítica feroz a la falta de protección de la privacidad que queda seriamente comprometida tras la norma.

[486] En su aseveración (Statement Of U.S. Senator Russ Feingold On The Anti-Terrorism Bill. From The Senate Floor. October 25, 2001); mostraba la profunda carga de sus preocupaciones sobre el futuro que implicaba para la tecnología y su determinación condicionada al "hecho musulmán":

"*...Now here's where my cautions in the aftermath of the terrorist attacks and my concern over the reach of the anti-terrorism bill come together. To the extent that the expansive new immigration powers that the bill grants to the Attorney General are subject to abuse, who do we think is most likely to bear the brunt of that abuse? It won't be immigrants from Ireland, it won't be immigrants from El Salvador or Nicaragua, it won't even be immigrants from Haiti or Africa. It will be immigrants from Arab, Muslim, and South Asian countries. In the wake of these terrible events, our government has been given vast new powers and they may fall most heavily on a minority of our population who already feel particularly acutely the pain of this disaster.*

When concerns of this kind have been raised with the Administration and supporters of this bill they have told us, "don't worry, the FBI would ever do that." I call on the Attorney General and the Justice Department to ensure that my fears are not borne out.

The anti-terrorism bill that we consider in the Senate today highlights the march of technology, and how that march cuts both for and against personal liberty...."

Las principales leyes afectadas y modificadas por la USA Patriot Act, muchas de las cuales las hemos tratado en este trabajo, fueron:

* The Electronic Communications Privacy Act (ECPA) (principalmente en sus partes de "Wiretap Statute" y de la "Pen Register and Trap and Trace Statute")

*The Computer Fraud and Abuse Act.

* TheForeign Intelligence Surveillance Act (FISA).

* The Family Education Rights and Privacy Act.

* The Money Laundering Act.

* The Immigration and Nationality Act.

* The Money Laundering Control Act.

* The Bank Secrecy Act.

* The Right to Financial Privacy Act.

* The Fair Credit Reporting Act.

Las mayores modificaciones en materia de privacidad se encuentran contenidas en la "Communications Assistance for Law Enforcement Act," en la "Electronic Communications Privacy Act (ECPA)", sobre todo en su parte de habilitación de escuchas, así como en la "Foreign Intelligence Surveillance Act (FISA)".

El título III de la *USA Patriot Act* regula los contenidos de la comunicación, sobre la que actúa en la plasmación de cualquier información que sea concerniente a la sustancia y significado de esa comunicación. Siempre teniendo en cuenta las consideraciones del Tribunal Supremo de la aplicación íntegra de las protecciones de la Cuarta Enmienda.

Por tanto, las limitaciones del Título de la Ley a la obtención gubernamental de esa información son de carácter restrictivo.

– Deben venir avaladas por orden judicial que avale los indicios de causa probable de que la persona cuya información se ve afectada, está cometiendo algunos de los delitos enumerados en la Ley, siendo comunicaciones concretas que se vean vinculadas

a la seguridad que regula la Ley, y que la misma se están utilizando en ese sentido infractor.

– Los funcionarios que ejecuten ese acceso deben ser claramente identificados, designados y autorizados para ello.

– La interceptación será por periodo concreto y determinado. Y será sometida a la regla de exclusión de su utilización como prueba en caso de ser conseguida en violación de ley.[487]

Entraremos ya en el análisis de aquellos apartados de la Ley que vienen a afectar a la privacidad de los ciudadanos, si bien ya contenidas en las partes de regulación sobre privacidad de aquellas leyes modificadas precisamente por esta. Ya que además la *USA Patriot Act* tiene un contenido mucho más extensivo, que llega a la regulación de la inmigración o a la lucha antiterrorista.

El primer artículo que nos encontramos con esta dedicación es la sección 105 que dota de autoridad al Servicio Secreto en la investigación electrónica de posibles crímenes en un amplio rango de actuación, creándose una red nacional al efecto.[488]

La sección 202 y la 217 de la Ley vienen referidas a los empleados públicos que podrán adquirir la condición de "computer trespassers", y modifican la *Computer Fraud and Abuse Act.*[489]

La sección 204 rebaja las exigencias de la *Stored Communications Access Act* para acceder al contenido de los mensajes de voz. Y la sección 210 amplía la información que los empleados públicos pueden obtener de los suministradores de comunicaciones electrónicas. La sección 211 también debilita las exigencias de la *Cable*

[487] El análisis jurídico de la *USA Patriot Act* es profuso. A modo de ejemplo citaremos los siguientes análisis generales: Ball (2004), Banks (2004), Whitehead & Aden (2002) y Gross (2002). Y más concretamente en lo que afecta de la Ley a la privacidad: Copeland (2004), Galloway (2002) Jaeger (2003) y Sullivan (2003).

[488] SEC. 105. "Expansion of National Electronic Crime Task Force Initiative"

[489] SEC. 202. "Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses." y SEC. 217. "Interception of computer trespasser communications".
Computer Fraud and Abuse Act, codificada en el 18 U.S.C. Bajo el epígrafe 1030, y que hemos estudiado en este trabajo.
La sección 217 define el concepto de "computer trespasser", coincidiendo con el establecido en otras leyes vistas (precisamente por ser la Patriot Act su introductora).

Communications Act sobre la capacidad de acceso a la información personal de los suscriptores.

La sección 213 introduce en la justificación de acceso a la privacidad por persecución penal, la mera "causa razonable para creer que la inmediata notificación de la ejecución del mandato judicial pudiera tener un efecto adverso" apreciada por el Tribunal. Elimina así la previa notificación al afectado.

Uno de los artículos principales en la incidencia en la privacidad se presenta en la sección 216, y es el que modifica las autoridades competentes en el uso de "pen registers y trap devices" que ya estudiamos en *la Electronic Communications Privacy Ac*t. Con esta nueva visión que impone la "Patriot Act" se amplia el elemento comunicación, expandiendo la vigilancia a todo el ámbito electrónico en cualquiera de sus formas y permite la interpretación extensiva del FBI sobre la norma, lo que ha implicado la puesta en práctica de su controvertido sistema de vigilancia "Carnivore".[490]

La sección 215 enmendaba el título V de la FISA (Foreign *Intelligence Surveillance Act of 1978*) y asegura, en un principio, al FBI un mayor acceso a documentos en las investigaciones de terrorismo internacional (y que permitía el acceso y recopilación masiva de metadatos). Si bien aquí entra la *USA Freedom Act* de 2015 para cortar esa "vigilancia masiva" posible y establecer su prohibición general y necesidad de concreción.[491]

La sección 218 establece enmiendas con menores estándares en la FISA en lo que se pueda entender como "inteligencia extranjera" a los efectos de ser investigada. Igualmente la FISA se ve afectada por la sección 206 y la introducción de la capacidad de investigación conocida como "escuchas itinerantes" ("roving wiretap"), sin especificación concreta de lineas determinadas. Órdenes genéricas de escuchas que han tenido un impacto evidente en los derechos de multitud de inocentes usuarios en pos de la seguridad.

[490] Para un mayor ahondamiento en el análisis de este sistema de vigilancia es relevante el trabajo (Tountas, 2003)

[491] Adquiriendo en un principio la facultad el Director del FBI de requerir judicialmente cualquier "cosa tangible", si bien tras la Ley 2015 generalmente prohibida y limitada a lo razonable dentro de la investigación y lo concreto del "specific selection term" que hemos visto anteriormente.

La sección 220 de la Ley permite una orden judicial única de autorización de esa investigación electrónica y que permita actuar en todo el territorio nacional. En el mismo sentido, la jurisdicción única para la persecución del terrorismo de la sección 219. Expande por tanto aquí la jurisdicción por causa de terrorismo a todo el territorio nacional estadounidense, con una mera orden única, que implica un "salvoconducto" de investigación a lo largo y ancho del país, también para todos sus operadores de telecomunicaciones. Antes de la modificación la orden, que por su propia naturaleza es así, requería una determinación específica de jurisdicción donde la investigación se vendría a llevar a cabo. Tras la *USA Patriot Act* el requisito jurisdiccional desaparece en pos de una supuesta mayor eficacia investigadora.

Debemos añadir que la Ley incorpora una previsión de finalización (en la poética costumbre de titulación "sunset"- atardecer- de las leyes estadounidenses), de buena parte de sus prerrogativas de vigilancia y de enmienda legal para el 31 de diciembre de 2005.

Por último, y como reflexión postrera, nos hacemos eco del pensamiento de Rubel (2007) que aborda la Ley y sus implicaciones desde una perspectiva filosófico jurídica; y en la que nos concluye en que la imposibilidad de conocer si nuestra información está siendo utilizada o rastreada, a pesar del enmarque legal en el que esa vigilancia trata de legitimarse, hace a los ciudadanos estadounidenses menos capaces de saber si tienen o no certeza cierta de disponer o no realmente de privacidad.

2.2.3 La vigilancia de la NSA y las revelaciones de Snowden

Fue en el año 2005 cuando por primera vez los ciudadanos estadounidenses despertaron del sueño de su "mundo feliz", y pasaron de la novela de Huxley a la realidad de los tiempos. Fue entonces cuando el New York Times informaba en su primera plana que la "National Security Agency (NSA)" interceptaba comunicaciones, también para cuando una parte de los comunicantes se encontraba en Estados Unidos, y ello a través del programa de vigilancia antiterrorista aprobado por el Gobierno de George W. Bush.

Aquello fue originando una serie de demandas y controversias judiciales que provocaron la modificación temporal de la FISA por la "Protect America Act" que en 2007[492] enmendaba a aquella por plazo de 180 días, introduciendo mayores potestades ejecutivas de vigilancia, y permitía escuchas sin autorización judicial ("warrants") en comunicaciones desde países extranjeros.[493]

En junio de 2013 el resto del mundo, incluidos los socios "fiables" europeos, empezó a sentir que la novela era otra. Y que nos encontrábamos ante una vigilancia global, de millones de ciudadanos, y de mandatarios señalados, y que entrabamos de lleno en la superación de los elementos contenidos en 1984 de George Orwell, alcanzados con holgura en el siglo XXI. Así, un analista de información de la NSA nos revelaba lo que realmente significaba la privacidad global hoy. El diario británico The Guardian y el estadounidense The Washington Post nos presentaban a Edward Snowden, que, en un oportuno sentimiento de ética individual, alumbró al mundo sobre estos hechos, y arruinó de paso su vida personal.[494]

Poitras (2014) realiza un documental acerca de todo el periplo que el analista ha sufrido debido a sus revelaciones, y Stone (2016) lo complementa con una película basada en la vida de este último héroe y traidor americano. Asimismo dos académicos noruegos lo proponen, también en 2014, como candidato a Premio Nobel de la Paz[495] por su contribución a "un mundo más estable y pacífico". Y recibe el premio "Right Livelihood Award", conocido como el "Nobel Alternativo"[496] en Suecia "por su valentía

[492] Ley de enmienda que se aprueba como Public Law No: 110-55 (2007), y que afecta a las definitorias de la FISA. Ley temporal que no fue renovada o confirmada en su permanencia por el Congreso expirando en julio de 2008.

[493] Entre las numerosas noticias a finales de 2005 nos hacemos eco de una del NY Times donde se revelan las órdenes presidenciales de escuchas sin autorización judicial (Recuperada el 2 de agosto de 2018):
http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

[494] En junio de 2013 salta la noticia en el periódico británico (y en el estadounidense). (Recuperada el 2 de agosto de 2018):
https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
En The Guardian se publica el 1 de noviembre de 2013 dosier explicativo de las revelaciones (Recuperado el 2 de agosto de 2018):
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[495] The Guardian (2014) Recuperado el 2 de agosto de 2018:
https://www.theguardian.com/world/2014/jan/29/edward-snowden-nominated-nobel-peace-prize

[496] Sobre el premio Nobel Alternativo, El Mundo (2014) (recuperado el 2 de agosto de 2018):
http://www.elmundo.es/internacional/2014/09/24/5422ed5c22601d7d478b458c.html

y destreza en la revelación sin precedentes de materia relacionada con la vigilancia estatal que viola los procesos básicos de la democracia y los derechos constitucionales". Asimismo, el Parlamento Europeo[497] se ha pronunciado en más de una ocasión sobre Snowden, entre ellas para pedir que se garantice su asilo por los Estados miembros o que se retiren los cargos en su contra, reconociéndole el carácter de "defensor internacional de los Derechos Humanos" (llamamiento aprobado por 285 votos contra 281), además de una serie de consideraciones y recomendaciones de gran importancia democrática alrededor de estas revelaciones en la resolución propiamente (que lo fue por 342 votos contra 274 y 29 abstenciones). La relevancia así, de la persona y del personaje, que acaban por confundirse, es indicativa de la importancia que ha tenido y tiene Edward Snowden en estas primeras década del siglo XXI.

Una de las escasas entrevistas que ha dado el ex analista a los medios en castellano la concedió al periódico digital español eldiario.es, en el que expresa su opinión sobre algunos de los elementos normativos estadounidenses analizados en este trabajo, así como sobre la vigilancia y la relación jurídica de la misma con Europa por parte de la potencia americana.[498]

Entre las declaraciones de mayor relevancia para nuestro trabajo y para que conozcamos los "hechos" detrás de todo este aparente derecho, podemos ver cómo nos asegura que "desafortunadamente, ninguna de las reformas que ha llevado a cabo el Gobierno de Estados Unidos desde 2013 ha tenido en cuenta que, con la ley vigente, el Gobierno puede monitorizar las actividades privadas de todo el mundo de manera indiscriminada, también a los ciudadanos estadounidenses (…) Bajo este paradigma, llamado "recolección a granel" por el Gobierno y vigilancia masiva por el resto del mundo, no se necesita una orden judicial individual para interceptar y archivar secretamente tus actividades". Continuando con la importancia de los metadatos para rastrear nuestra huella digital y sobre todo, lo más importante es que ello no parece haber servido para

[497] Parlamento Europeo (2014) Recuperado el 2 de agosto de 2018: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES
Parlamento Europeo (2015)

[498] Disponible en dos entregas. Eldiario.es (2016) Recuperado el 2 de agosto de 2018 : http://www.eldiario.es/internacional/entrevista_Edward_Snowden_0_494150889.html
Y la segunda:
http://www.eldiario.es/internacional/teleco-usando-conectada-cordel-privacidad_0_494500669.html

conseguir una mayor seguridad; aludiendo al informe[499] encargado por la Casa Blanca a auditoras independientes donde se asegura la no prevención de actos terroristas a través de estas escuchas masivas (de las previstas en la sección 205 de la USA Patriot Act). Asegurando así el ex analista que "la vigilancia no tiene que ver con la seguridad, tiene que ver con el poder". Resumiendo el espíritu de su lucha muy bien en la siguiente frase: "Dejar de ser una sociedad libre por miedo al terrorismo es la única manera que tienen los terroristas de ganar."

Más concretamente en la segunda entrega de sus declaraciones Snowden alude al Acuerdo "Safe Harbour" y a su sustituto, el "Privacy Shield", y que estudiaremos más adelante, para reflexionar sobre las relaciones sobre Privacidad entre Estados Unidos y Europa. Y suena revelador: "Si después de conocer en 2013 cómo había sido el espionaje masivo de la NSA, la Unión Europea hubiera leído la ley tal cual aparece en los libros de los Estados Unidos en lugar de como se la contaban sus representantes, se habrían dado cuenta de que, con el nivel de protección de la privacidad de los datos, ningún ciudadano extranjero estaba protegido", Y ello en relación con el Acuerdo de Puerto Seguro.

Lo expresa claramente, y relacionado también con el capítulo de la privacidad del consumidor, tratada en esta parte de este trabajo: "en Europa hay muchas leyes distintas de protección de datos que gestionan cómo los datos pueden ser conseguidos, manejados y protegidos de una industria a otra y de un sector a otro. En los Estados Unidos no tenemos una ley de protección de datos: lo que hay son unas pocas leyes que regulan la privacidad en sectores muy particulares. El sector de servicios financieros y la industria de servicios médicos tienen alguna pequeña protección para el consumidor pero, a no ser que se utilicen esos datos en un contexto muy específico, hay barra libre para manejar los datos.

En vez de una legislación, lo que tenemos son esos contratos en los que cada proveedor de servicios establece los términos de servicio. Y en esos acuerdos de términos de uso,

[499] Washington Post (2014) El informe y la noticia sobre el mismo puede ser objeto de consulta. Recuperado el 10/11/2016: http://apps.washingtonpost.com/g/page/world/pclobs-report-on-the-nsas-collection-of-americans-phone-records/757/
Si bien en nuestra última consulta y tras la fecha de aplicación del Reglamento Europeo de Protección de Datos aparece el siguiente literal: "*Due to new European data protection law, this page is temporarily unavailable to you*."

estás comprando software donde los términos pueden ser modificados unilateral e inmediatamente por el proveedor de servicio en cualquier momento. Usando ese servicio, estás de acuerdo con que te estafen y abusen de ti de manera permanente."

Indica además que, en su opinión, el *Privacy Shield,* confirmará el mismo efecto de protección: "en términos legales, nada ha cambiado. La Administración de Obama se ha curado en salud diciendo que están implementando políticas en las que serán más cuidadosos al tratar los datos de los ciudadanos europeos, pero esta "protección" se refiere únicamente a cuando están leyendo la información. Ellos registran todo de todo el mundo, ciudadanos americanos y ciudadanos europeos, sin la justificación de una sospecha criminal previa. Tanto si creen que eres inocente como si creen que eres Osama bin Laden.

La NSA guarda un registro de todo lo que hace un ciudadano europeo, independientemente de si hace algo malo o no. Y pueden acceder a ese registro sin una orden y examinar todos los archivos. La única diferencia es cómo los tratan después de haberlos investigado. El *Privacy Shield* no es más que un intento de ganar tiempo."

Sobre todo ello, apuntaremos algunos elementos jurídicos que se han producido desde entonces, sobre todo en el ámbito de jurisdicción de la agencia de información, que es Estados Unidos, y las reacciones que hasta el momento se han perfilado en aquel terreno de derecho. Principalmente las acciones se han visto del tipo jurisprudencial, si bien ya hay apuntados cambios normativos, y algunos no van dirigidos necesariamente hacia una mayor protección de la privacidad.

Precisamente, y más tras recientes ataques de terrorismo demencial, la balanza de la libertad individual y de los derechos de privacidad quizá se vea finalmente alzada por el gran peso que la seguridad va a seguir adquiriendo en las décadas venideras. La *USA Freedom Act*, que veremos a más adelante, es la principal materialización legal de estas propuestas de reforma.

2.2.3 a) Consideraciones

Las revelaciones de Snowden apuntan a la vigilancia de personas en varias categorías, tal y como apuntan Solove y Schwartz (2015), destacando las siguientes: aquella vigilancia de personas no estadounidenses y fuera de Estados Unidos en base a la Sección 702 de la Ley (codificada en el parágrafo 1881(a) que hemos estudiado), es decir, a través de algún conducto con vinculación jurídica estadounidense (como pueden ser las redes sociales más populares y globales). Aquella vigilancia consistente en el almacenamiento de metadatos telefónicos, en base a la sección 215 de la *USA Patriot Act* (que también hemos analizado) (y previo requerimiento a las compañías de telecomunicaciones estadounidenses). Aquella vigilancia a líderes mundiales, con ayuda británica, y que van desde mandatarios aliados como Ángela Merkel, hasta aquellos de países competidores como China, pasando por multitud de personajes importantes, sobre todo del ámbito económico, a lo largo de todo el mundo (como el presidente de Petrobras). Aquí no existe elemento de vinculación jurídica claro. Y por último aquella actuación de debilitamiento de los sistemas de encriptación de empresas y del mundo comercial, con la clara intención de hacer accesibles los datos de los clientes a la Agencia (siendo el mejor ejemplo la última contienda con Apple al respecto, para conseguir que abran “puertas de atrás” en su dispositivos para el FBI) (Slove & Schwartz, 2015, 460-462).

En este sentido, el relator especial para el Consejo de Derechos Humanos de Naciones Unidas, David Keyne nos dice que “Las amenazas contra el cifrado y anonimato reflejan que los derechos online están en peligro" ya que en su opinión, “"El cifrado y el anonimato proporcionan la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de opinión y expresión en la era digital".[500]

Estas revelaciones de Snowden tienen, para ser justos, ciertas contrapartidas análogas de vigilancia en Europa. Así debemos mencionar y aún en menor medida, resaltar las escuchas generalizadas llevadas a cabo por la que se ha venido a conocer como la “NSA alemana” a través del sistema “XKeyscore”. Así el Servicio Federal de Inteligencia alemán la BND (en sus siglas en alemán) recabó y almacenó ilegalmente una enorme

[500] Ver Kaue (2015) (Recuperado el 2 de agosto de 2018)
http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

cantidad de datos (si bien parece que no de ciudadanos europeos), según se ha podido conocer tras informe clasificado de la Comisión de Protección de Datos de Alemania, poniéndolos a disposición de la NSA americana.[501]

E igualmente tenemos nuestros propios pequeños luchadores europeos por la privacidad como es el caso de Sabine Leutheusser-Schnarrenberger, antigua ministra de Justicia alemana de 64 años, que mantiene una cruzada contra la vigilancia y la retención masiva de datos, y ello a través de dos frentes: internamente con el actual Ministro del Interior de su país, y en el ámbito europeo con la comisaria Cecilia Malmström, por sendas leyes y Directivas en esos ámbitos respectivos. La de mayor impacto en este sentido, y que analizaremos en la parte europea del trabajo, será la declaración de invalidez por el TJUE de la Directiva de retención de datos europea. Añadiremos además que esta activista es falsa la dicotomía libertad versus seguridad, que han tratado de establecernos.[502]

2.2.3 b) Jurisprudencia reactiva

Se ha dictado desde esta presentación de los hechos, de la realidad de la vigilancia global un lógico conflicto jurídico que se ha ido sustanciado en algunas interesantes sentencias.

Así en *Clapper v. Amnesty International USA 133 S. Ct. (2013)* se presenta una disputada decisión en el que el Tribunal Supremo mantiene la constitucionalidad del precepto 1881(a) del 50 USC (sección 702) de la FISA, sobre una demanda en base al artículo III de la Constitución estadounidense por parte de un conjunto de abogados, juristas y activistas de los derechos humanos de EE.UU (siendo Clapper el director de Información de Inteligencia del Gobierno estadounidense). En una ajustada votación de

[501] Netzpolitik (2016) (Recuperado el 2 de agosto de 2018): https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/

[502] Politico (2016) (Recuperado el 2 de agosto de 2018): http://www.politico.eu/article/the-way-of-the-german-privacy-warrior-sabine-leutheusser-schnarrenberger-germany-former-justice-minister-data-retention-law/

5 contra 4 votos particulares se tomó esta decisión de respaldo constitucional y validez legal al precepto de la FISA.

Se presenta el caso sobre la demanda de posibles perjuicios y daños que el precepto en cuestión puede estar planteando a los abogados y a las organizaciones de derechos humanos que pueden verse afectados en sus comunicaciones con sus clientes y usuarios, que se encuentren fuera del territorio de Estados Unidos y que pueda comprometer su trabajo y actividad, así como el ejercicio de esas personas en su calidad de testigos o de meros sujetos con derecho al respeto de su información personal y secreto de comunicación.

El Tribunal en su determinación intenta realizar una labor clarificadora, estableciendo punto por punto la defensa legal del precepto 1881 (a) de la FISA, y desmontando las pretensiones de los demandantes.

Primero observa "especulativo" que el Gobierno pueda considerar como un objetivo inminente a este tipo de comunicaciones de los demandantes.[503]

En segundo lugar considera también especulativo que el Gobierno utilice, en el caso que se presenta, los métodos del 1881 (a) "cuando tiene otros numerosos métodos de vigilancia". Y tercero, sigue siendo especulación de los demandantes, "que esa vigilancia se vaya a autorizar". En cuarto lugar el Tribunal no considera claro si el Gobierno tendría éxito en esa vigilancia, y concretamente en los contactos extranjeros de los demandantes. Y quinto, es especulación considerar que, a pesar de los sujetos, sea precisamente esa comunicación con ellos la que fuera a ser objeto de vigilancia.

Así acaba el Tribunal manteniendo la plenitud constitucional del precepto y negando la pretensión de perjuicio porque ese posible daño debiera fundarse en un temor que tendría que ser "claramente inminente".[504]

Si bien queda el otro posicionamiento del Tribunal de manifestación mucho más interesante para el sostenimiento de la privacidad (y de la posición de los demandantes), a pesar de resultar minoritaria, en forma de voto particular.

---

[503] *"… First it is speculative wether the Government will imminently target communications to wich respondants are parties"*

[504] Sobre esta decisión alguna doctrina ya ha manifestado su parecer, en cuanto cierra las posibilidades de protección de los datos personales en defensa del dictado del precepto: Wright (2013).

De esta manera, y encabezado por el Juez Breyer, y secundado por los Jueces Ginsburg, Sotomayor y Kagan se presenta la voz disidente. En opinión contraria estos jueces hablan de que las pretensiones de los demandantes dependen de la probabilidad de actuar que el Gobierno tiene bajo el paraguas del 1881 (a) del 50 USC, precepto sobre el que versa principalmente la sentencia, y que ello les provocará perjuicios si se interceptan sus comunicaciones privadas. Y que ese daño no sería "especulativo".[505]

Y continúa desgranando sus argumentos, estableciendo que no nos encontraríamos ante casos amparados expresamente por el precepto (del que no duda el voto de su constitucionalidad), ya que deberíamos entender, dice, la naturaleza de esa vigilancia.

En ella, empieza el Tribunal a separar la redacción del precepto antes y después de la modificación operada en él en 2008. En un principio se deben particularizar los objetivos, para solicitar la autorización judicial, especificándose además el tipo y forma de vigilancia. Y la necesidad de demostrar el carácter de "foreign power or foreign agent" del objetivo a controlar.

Tras aquella modificación se elimina esa necesidad de especificación al Gobierno, se elimina la necesidad de demostración de "foreign power or foreign agent" en el objetivo y se disminuye la capacidad de los tribunal en su control y supervisión.[506]

Se considera además, más adelante, que ello sí refleja un posible daño cierto a los demandantes que se relacionan en sus comunicaciones con esas personas extranjeras que pueden ser motivo probable de vigilancia. Ya que tienen un "fuerte" motivo para comunicarse con ellas mientras el Gobierno, tiene un "fuerte" motivo para querer

[505] Señalando además que aquel propio Tribunal ya se había basado en futuribles para la base de sus sentencias (poniendo como ejemplo más adelante el caso Mosanto y su decisión respecto a la alfalfa genéticamente manipulada como efecto de daño futuro para los agricultores tradicionales).
"*…In my view, this harm is not "speculative." Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing. I dissent from the Court's contrary conclusion…*"

[506] Por ello se concluye que al usar la autoridad otorgada por el 1881 (a) se pueden dar estas autorizaciones con el principal propósito de recabar información de inteligencia y se abre la vía legal al uso del objetivo de vigilancia general y de intromisión en la privacidad.
"*…Thus, using the authority of §1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information," and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved…*"

escucharlas. Además de que, (y poniendo como ejemplo la experiencia de Guantánamo), el "comportamiento pasado" del Gobierno da indicaciones de esa probabilidad.[507]

Otra importante sentencia es *Klayman v. Obama* 957 F.Supp. 2d 1 (D.D.C. 2013) que surge de dos demandas sobre "ciertas prácticas de recogida de inteligencia" realizadas por el Gobierno de Estados Unidos sobre la masiva captación y almacenamiento de metadatos a ciudadanos estadounidenses, a través de la NSA y a raíz de las informaciones contenidas en el diario británico *The Guardian* en fecha 5 de junio de 2013[508]. Y que relataba la puesta a disposición masiva de millones de datos de usuarios de Verizon a esta Agencia, y a través del programa de contraterrorismo "PRISM", y ello sobre la base del precepto 1861 de la FISA (que hemos analizado en este bloque de contenidos).

Este sistema de recogida masiva telefónica de metadatos consiste básicamente, y en base a unos parámetros previos introducidos por la NSA, en capturar una masiva serie de llamadas, y en mantener los datos contenidos en ellas para rastrear posibles pistas que puedan servir de prueba en prevención antiterrorista. Según alega el Gobierno en este caso, son datos que no permiten identificar a los usuarios previamente a que "salte" la pista. Lo que implicaría seguir los pasos legales de autorización judicial (del tribunal especializado FISC), y así defiende estar siguiendo los trámites adecuados, a pesar de esa masiva recopilación. Al ser datos "desagregados", defiende el Gobierno, no se produce violación legal en estas capturas masivas.

El Tribunal pasa a exponer sus razonamientos sobre el artículo III de la Constitución y sobre la Cuarta Enmienda en relación con el caso, y que aquí observa comprometida. Reconoce el Tribunal que no estábamos ante el mismo caso que en "Clapper" y se separa de aquella decisión.[509]

---

[507] Finalizando así el voto disidente: "*While I express no view on the merits of the plaintiffs' constitutional claims, I do believe that at least some of the plaintiffs have standing to make those claims. I dissent, with respect, from the majority's contrary conclusion*."

[508] The Guardian (2013) Recuperado el 2 de agosto de 2018: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[509] *"…The NSA's Bulk Telephony Metadata Program involves two potential searches: (1) the bulk collection of metadata and (2) the analysis of that data through the NSA's querying process. For the following reasons, I have concluded that the plaintiffs have standing to challenge both. First, as to the collection, the Supreme Court decided Clapper just months before the June 2013 news reports revealed*

Y reconoce la quiebra de la Cuarta Enmienda constitucional con estas actuaciones por parte del Gobierno y su violación de la razonable expectativa de privacidad, dando la razón a los demandantes sobre los posibles perjuicios ocasionados.[510]

Y continúa el Tribunal estableciendo consideraciones de calado sobre los tiempos de vigilancia "casi orwelliana" que nos está tocando vivir, diferenciándolo de previas sentencias del siglo pasado sobre la Cuarta Enmienda (como el caso "Smith" que analizamos anteriormente), a través y gracias a una tecnología (sobre todo manifestada en los actuales y actualizados teléfonos móviles) que nos deja expuestos de manera omnipresente para la vigilancia de estas Agencias.[511]

Si bien y para terminar, debemos apuntar que el propio Tribunal en sentencia posterior (al mes siguiente) con su pronunciamiento en el caso "In Re FBI 2013 WL 5307991 (FISC 2013)", parece seguir manteniendo válido el precedente "Smith v Maryland" rebatido en la sentencia que acabamos de analizar, llegando a una decisión contradictoria con esta.

---

the existence and scope of certain NSA surveillance activities. Thus, whereas the plaintiffs in Clapper could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention…"

[510] *"…The threshold issue that I must address, then, is whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do—and a Fourth Amendment search has thus occurred—then the next step of the analysis will be to determine whether such a search is "reasonable." (…)*

I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy…"

[511] *"…the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979 (…)*

Finally, and most importantly, not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater(…)

Admittedly, what metadata is has not changed over time. As in Smith, the types of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like.57 But the ubiquity of phones has dramatically altered the quantity of information that is now available and, more importantly, what that information can tell the Government about people's lives…"

2.2.3 c) Legislación reactiva. La USA Freedom Act.[512]

La *USA Freedom Act* es la Ley que surge como reacción legal a las revelaciones de Snowden. Podría considerarse una continuación de la *USA Patriot Act* y de su regulación de estado de excepción, si bien adecuada a los nuevos tiempos propios de su aprobación. También se puede ver desde la óptica de la Ley que viene a sustituir a la *USA Patriot Act*, a la que pone fin en algunos términos. La *USA Freedom Act* es una continuación, y al mismo tiempo, un punto final a la *USA Patriot Act*. En el primer caso desde un punto de vista material con matices favorables a la privacidad, y en el segundo caso desde la perspectiva formal para algunos puntos, sobre todo en lo que a Ley modificadora de la FISA se refiere.

La Ley, aprobada por el Congreso el 13 de mayo de 2015 y firmada por el Presidente Obama el 2 de junio de 2015, viene, en la parte que nos interesa, a poner fin a la recopilación masiva de datos por parte del Gobierno estadounidense, tal y como se venía produciendo.[513]

En resumen, podremos decir que la Ley no prohíbe del todo la recopilación masiva de datos por parte del Gobierno, pero sí limita los requerimientos del mismo a las compañias de telecomunicaciones para suministrar información sobre un investigado criminal, si el Gobierno puede demostrar "razonable" la vinculación de esa persona con actividad u organización terrorista. Además, establece nuevos requisitos de informe al Gobierno en su relación con los tribunales de la FISA (FISC), junto a la desclasificación de las opiniones de estos Tribunales, que se dan a conocer. Si bien extiende algunas previsiones de la *USA Patriot Act*, como la sección 215, hasta diciembre de 2019 (Suárez, 2017).

Además, también resulta de importancia la voluntad de concreción investigatoria que promueve la ley a la hora de exigir al Gobierno la especificación del objeto a investigar,

[512] En su nombre largo "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015 "Public Law 114–23
La página del Congreso de EE.UU. recoge el texto legal y hace un resumen del mismo. Recuperada el 2 de agosto de 2018:
https://www.congress.gov/bill/114th-congress/house-bill/2048

[513] La declaración del Presidente al respecto. Recuperada el 2 de agosto de 2018:
https://www.whitehouse.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act

sin la laxitud interesada que se venía dando, y que provocaba la recopilación masiva de datos. Y recoge en su Sección 103 esta matizada prohibición de recopilación masiva de datos en las investigaciones criminales previstas en la FISA.[514]

Forsyth (2015) hace una lectura positiva de la Ley como avance en la prohibición de la vigilancia estatal masiva y los equilibrios entre seguridad y privacidad, aludiendo a la deseable "solución política" del asunto.

Algunos autores como Swire (2015) además ponen el foco en el avance que supone la Ley para aplacar las "preocupaciones europeas" sobre las prácticas de vigilancia reveladas por Snowden. Y lo que supone esta Ley como cambio de rumbo jurídico en esta vigilancia.

[514] Sec. 103. Prohibition on Bulk Collection of Tangible Things"
La Ley lo establece así en su sección 107 dedicada a las definiciones: *"'specific selection term'—*
(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and
(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things".

PARTE III. EL DERECHO A LA PROTECCIÓN DE DATOS EN EUROPA.

INTRODUCCIÓN

El derecho a la protección de datos en Europa se ubica dentro de los derechos de tercera generación, dentro de la clasificación general de los derechos humanos,[515] y es producto, como hemos analizado en la parte introductoria del trabajo, de la asimilación de las tradiciones jurídicas nacionales, de la influencia del Consejo de Europa y su Protocolo 108, de la Carta de Derechos Fundamentales de la UE y de la labor jurisprudencial europea, tanto del Tribunal de Luxemburgo como de la de Estrasburgo.

En este sentido resulta de utilidad la visión del recorrido que nos presenta Rebollo Delgado (2008) en su clasificación de las etapas de generación de la normas en materia de protección de datos en Europa, desde el punto de vista de las tradiciones jurídicas nacionales.

La primera que coincide con los años 50, con una informática incipiente, se enfoca más a la protección de las posibles injerencias del sector público. En ella se encuadran la Ley de Hesse de 1970, la Ley sueca de 1973, la de Renania Palatinado de 1974.

La segunda tiene más presente al sector privado y profundiza en el principio de calidad en la conservación de los datos. La "Privacy Act" de 1974 estadounidense es ejemplo de la primera fase de esta generación. Una segunda fase, en la que ya se empiezan a reconocer los "datos sensibles" la ejemplifica la Ley Federal alemana de 27 de enero de 1977.

La tercera etapa viene motivada por la sentencia del Tribunal federal alemán de 15 de septiembre de 1983 que declara inconstitucionales algunos preceptos de la Ley del Censo. Fecha de 1983 que coincidía además con la aparición de Internet. El culmen de esta generación de protección lo encontramos con la Directiva europea de 1995 (Rebollo Delgado, 2008, 89-94).[516]

[515] Presentada originalmente por Karel Vasak (1977) en su artículo "Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights".

[516] Incide en la idea anteriormente expresada en la introducción del trabajo: "configuró un nuevo

Esta clasificación es coincidente, en lo sustancial, con la que nos brinda Arenas Ramiro (2008, 128-130), que incluye en la primera generación además las Leyes de Francia, Dinamarca, Luxemburgo, Noruega, Austria y Alemania, caracterizadas por exigir una autorización previa para la creación de ficheros de datos y por crear Autoridades de control; y establece en la segunda generación las leyes de Irlanda, Holanda, Bélgica, Finlandia, Reino Unido, Portugal y España, caracterizadas por su carácter post protocolo 108 del Consejo de Europa y su tendencia a la simplificación de trámites y búsqueda de la autorregulación.

Asimismo, González Fuster (2014) nos relata que el nacimiento de la protección de datos surge como moderno concepto autónomo en Europa, tras una labor de comparativismo jurídico con el concepto estadounidense de privacidad a partir de los años 70 (sobre todo tras la Privacy Act), y con el Convenio Europeo de Derechos Humanos como faro que alumbra su contenido esencial. Y sobre todo, actualizada a su versión informática acaecida en la época. Indica las Leyes de Hesse y de la propia Alemania, junto con la de Suecia y Francia, como puntos de interés en el origen legal del concepto de protección de datos en Europa, siendo Austria, España y Portugal avanzados en su reconocimiento a nivel constitucional.

Explica la autora (2014, 163-212) el surgimiento del derecho fundamental, en modo conclusivo, en Europa, destacando su evolución no solo por la influencia internacional (OCDE, CEDH etcétera) en la protección de los derechos humanos, sino también en la no distinción idiomática dentro de los flujos legales intraeuropeos; que no hace una delimitación clara entre protección de la vida privada, privacidad y protección de datos personales. Termina, al final, en una separación (que no distinción) en la Carta Europea entre el artículo 7 de respeto a la vida privada, y el 8 de protección de datos personales. Surge así el derecho a la protección de datos personales de la ambivalencia, a raíz del más amplio abrigo del derecho a la privacidad presente en las normas europeas e internacionales de referencia, si bien revelándose como un derecho fundamental en sí mismo en esa evolución.

concepto al que denomina derecho a la autodeterminación informativa como derecho que tiene el individuo de decidir básicamente por sí solo la difusión y utilización de sus datos personales…" (Rebollo, 2008, 93).

Podríamos hablar que, a partir de 2012 y materializándose en 2016, se abre un nueva generación de protección en Europa con el paquete de reforma legislativa que aquí estudiaremos más adelante.

Por tanto, y recapitulando los antecedentes institucionales y normativos, diremos que un primer paso para la institucionalización de la protección de datos como derecho fundamental en Europa lo encontramos en la Declaración conjunta del Parlamento, Consejo y Comisión sobre Derechos Fundamentales de 5 de abril de 1977[517], donde ya se pone de relieve la necesidad de dotarse, por parte de las Comunidades Europeas, de un catálogo de derechos fundamentales normativizado.

Más adelante, el Acta Única Europea de 1986 empezará ya a interpelar de manera indirecta a los derechos fundamentales como pilares europeos.[518]

Y llegaremos al Tratado de Maastricht de 1992 en el que el artículado ya vendrá a reflejar ese respeto fundamental sobre la guía del CEDH. [519]

Para arribar al Tratado de Amsterdam, que será el primero en reconocer el respeto a la vida privada en consonancia con el artículo 8 del CEDH, y que establece una protección reforzada respecto al tratamiento y circulación de datos personales. Estableciéndose en el ámbito de la cooperación penal, e insertándose en su aplicación de protección a las instituciones y organismos europeos.[520]

[517] Publicada en el DOCE núm. C 103, de 27 de abril de 1977.

[518] Nos refiere, en su exposición de motivos, que los Estados miembros se muestran "Decididos a promover conjuntamente la democracia, basándose en los derechos fundamentales reconocidos en las Constituciones y leyes de los Estados miembros, en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en la Carta Social Europea, en particular la libertad, la igualdad y la justicia social".

[519] En el apartado 2 de su artículo F nos dice que "La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma el 4 de noviembre de 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario." Mencionamos relacionado el Dictamen 2/94 del TJUE de 28 de marzo de 1996 sobre su actuación en materia de Derechos Fundamentales.

[520] Modificación del artículo K2 y Punto 54 modificando el 213 b).

CAPÍTULO PRIMERO.

EL CIMIENTO CONSTITUCIONAL DE LA PROTECCIÓN DE DATOS EN EUROPA.

1. La protección de datos en el Derecho Europeo.

El artículo 16 del Tratado de Funcionamiento de la Unión Europea puede considerarse como el primer precepto establecido en el derecho originario de la Unión, en el que se prevé el derecho a la protección de datos de manera nítida y directa. El artículo tiene como precedente el artículo 286 del Tratado de la Comunidad Europea, en el que no se hacía una mención tan abierta y general a la protección de datos personales, dedicado entonces más bien al objetivo interno de protección en las instituciones comunitarias.[521]

El artículo 16 nos dice:

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

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

[521] El dictado era el siguiente: "1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo.
2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes."

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."

Es por ello que debemos destacar, que este camino de constitucionalización[522] del derecho a la protección de datos personales y su principio de protección, no se ha manifestado en su plenitud hasta el Tratado de Lisboa. El derecho a la protección de datos no es único ni solitario en este sentido, ese revestimiento y dotación constitucional lo han recibido otros derechos que antes se contemplaban de manera más indirecta o aproximativa, mercado único mediante, y que el Tratado de Lisboa viene a consagrar como derechos de los europeos propiamente. Enraiza así con la idea de ser un residuo potentísimo del naufragio de la Constitución para Europa, y cuasi similar en lo sustancial a aquélla. Así se estima en su gran parte, en el gran grueso la asimilación de aquel dictado constitucional fallido (Bar Cendón, 2009).[523]

Además resaltaremos en esa línea la incorporación efectiva (si bien no formal y directa), y el carácter jurídicamente vinculante de la Carta de Derechos Fundamentales, asi como la previsión de incorporación del CEDH, junto con la previsión del armazón institucional, constitucional y de sistemática organizativa, siguiendo la Constitución para Europa. Al igual que su ámbito competencial y su división, añadiendo la previsión de los derechos de la ciudadanía europea. Son todos elementos evidentes de esa sucesión.

No obstante, los orígenes de la regulación de este bien jurídico protegido los podemos encontrar por varias vías:

[522] Sobre el procedimiento de constitucionalización de la Unión Europea en general disponemos de abundante doctrina. A modo de ejemplo citaremos a Solozábal (2003) con especial mención a la Carta de Derechos Fundamentales; Balaguer Callejón (2007) que pone el foco en la identidad europea conectada a su elemento constitucional o Diez Picazo (2008) sobre su carácter híbrido entre el derecho internacional y el constitucional. Más concretamente López Aguilar (2017) nos ilustra sobre la constitucionalización de la protección de datos en Europa, a partir del Tratado de Lisboa.

[523] Ver igualmente Borrell, J., Carnero, C. y López Garrido D. (2003). Construyendo la Constitución Europea. Crónica Política de la Convención. Madrid: Real Instituto Elcano de Estudios Internacionales y Estratégicos.

- La labor del Consejo de Europa desde el punto de vista de sus Principios, a través de la actuación jurisprudencial del Tribunal Europeo de Derechos Humanos y desde la óptica normativa con el Convenio 108.

- El surgimiento, en el marco de la Unión Europea de una norma como la Carta de Derechos Fundamentales de la Unión Europea, que viene a recoger este derecho, incluso antes que el propio texto "constitucional", tomando por tal al Tratado de Funcionamiento de la Unión Europea y su artículo 16 reseñado.

- Como antecedente y consecuencia de esta regulación encontramos todo del Derecho interno de los distintos Estados miembros, adaptado así, a esas líneas directrices europeas.

2. El Consejo de Europa.

2.1 El Consejo de Europa y el CEDH

El Consejo de Europa[524] es la primera organización internacional regional europea que abraza y se propone el ideal de integración europea, a través del ejercicio inexcusable de la paz y la democracia. Y dentro de sus medios y objetivos está el de la salvaguardia de los derechos humanos, entre ellos, el derecho a la privacidad y protección de la vida personal y familiar.

Así, su instrumento principal es el Convenio Europeo de Derechos Humanos (en adelante CEDH). El 4 de noviembre de 1950 se firma en Roma el Convenio para la salvaguardia de los derechos humanos y las libertades fundamentales, más popularmente conocido como Convenio Europeo de Derechos Humanos, y su entrada en vigor se produjo el 3 de septiembre de 1953[525]. Todos los Estados miembros del Consejo de Europa han suscrito el Convenio Europeo de Derechos Humanos.

[524] El Consejo de Europa, es una organización internacional constituida como consecuencia del Congreso de La Haya de 7 de mayo de 1948, que tiene por finalidad según el artículo 1 de su Estatuto regulador hecho en Londres el 5 de mayo de 1949:
"a) La finalidad del Consejo de Europa consiste en realizar una unión más estrecha entre sus miembros para salvaguardar y promover los ideales y los principios que constituyen su patrimonio común y favorecer su progreso económico y social.
b) Esta finalidad se perseguirá, a través de los órganos del Consejo, mediante el examen de los asuntos de interés común, la conclusión de acuerdos y la adopción de una acción conjunta en los campos económicos, social, cultural, científico, jurídico y administrativo, así como la salvaguardia y la mayor efectividad de los derechos humanos y las libertades fundamentales.
c) La participación de los Miembros en los trabajos del Consejo de Europa no debe alterar su contribución a la obra de las Naciones Unidas y de las restantes organizaciones o uniones internacionales de las que formen parte.
d) Los asuntos relativos a la defensa nacional no son de la competencia del Consejo de Europa."

[525] Publicado en«BOE» núm. 108, de 6 de mayo de 1999, la Resolución de 5 de abril de 1999, de la Secretaría General Técnica del Ministerio de Asuntos Exteriores, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.

Dentro del Convenio fijaremos nuestra atención concreta al artículo 8 que se encarga de manera general de la intimidad en el ámbito personal y familiar. Así, el artículo 8 del Convenio nos dice:

"Derecho al respeto a la vida privada y familiar.

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."[526]

Indica Guerrero Picó (2006, 28) que, es precisamente este organismo el que ostenta el título de precursor de la preocupación sobre la protección de datos personales, a principios de los años 70, con la aparición de los ordenadores, "máxime cuando aún permanecía muy vivo en la memoria colectiva el referente del régimen nazi, que podría haberse valido de las incipientes técnicas informáticas para identificar a las personas que pertenecían a los colectivos por él perseguidos".

Al respecto, conviene tener presentes la Resolución 22 de 26 de septiembre de 1973 y la Resolución 29 de 20 de septiembre de 1974, que tienen como objetivo, según la autora, "favorecer la elaboración de legislaciones nacionales inspiradas en unas directrices comunes que garanticen los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos, ya sea en su fase de registro, tratamiento en sí o difusión de la información. Este mínimum común se concibe como un paso más del camino hasta llegar a un "orden público europeo" compartido" (Guerrero Picó, 2006, 31).

[526] Podemos apuntar siguiendo a John Wadham el sentido de proporcionalidad teniendo en cuenta las circunstancias para la medición de lo "necesario" en una "sociedad democrática", cuando nos dice que el Estado "no puede usar un mazo para abrir una nuez" dado en su conferencia en marzo de 2000 en la Universidad de Cambridge. Tal y como recogen Solove & Schwartz (2015, 1109-1110). Como análisis general sobre el artículo 8 del CEDH citaremos a Santolaya Machetti (2005).

Al final, y en última instancia, todas esas consideraciones del Consejo de Europa podemos decir que se han ido añadiendo e incorporando a la legislación de la UE, así como a la de los Estados que lo componen. Y que la han ido desarrollando.

Esos principios de inspiración, y ya contenidos en las Recomendaciones citadas, serían, según la autora: el de publicidad, el de autorización previa, el de fijación del plazo de conservación o utilización de datos, el de derecho de acceso y el de acceso a los datos (Guerrero Picó, 2006, 33).

2.2 Jurisprudencia del TEDH en base al artículo 8 del CEDH

El Tribunal de Estrasburgo ha sido el eminente productor de derecho sobre la protección de datos en el ámbito del Consejo de Europa, a través de una continuada y prolija jurisprudencia relacionada. Se puede estudiar, debido a su abundancia, por las materias relacionadas dentro de esa protección.

El listado del año 2017 publicado por el Consejo de Europa sobre asuntos del TEDH concernientes a la protección de datos nos da una idea del gran volumen de atención prestado por el Tribunal a este derecho.[527]

También nos resulta útil e interesante el seguimiento jurisprudencial propuesto por el Manual conjunto del Consejo de Europa y la Agencia de Derechos Fundamentales de la UE (FRA en sus siglas en inglés) que distingue en particular, dentro de este tratamiento judicial, las siguientes clasificaciones: sentencias relacionadas con la intercepción de las comunicaciones, las relacionadas con las diversas formas de vigilancia, y aquellas sobre la protección contra el almacenamiento de datos personales por parte de las autoridades públicas. O aquellas incluso donde se establece la obligación positiva de garantizar activamente el respeto efectivo a la vida privada y familiar (ADFUE/CoE, 2014, 15).[528]

[527] Ver Consejo de Europa (2017). Recuperado el 23 de agosto de 2018: https://rm.coe.int/case-law-on-data-protection/1680766992

[528] En sus ejemplos más característicos de cada una de ellas el Manual cita respectivamente:
El caso Malone contra el Reino Unido, nº 8691/79, de 2 de agosto de 1984 y el de Copland contra el Reino Unido, nº 62617/00, de 3 de abril de 2007, sobre intercepción de las comunicaciones.

Apuntaremos aquí inicialmente, siguiendo esa clasificación, algunas de esas sentencias. Hemos de aclarar que hacemos mención a algunos pronunciamientos particularmente relevantes en la materia por parte del TEDH, que no se agotan en este epígrafe, sino que ampliaremos más adelante con comentarios de otras sentencias igualmente importantes, pero que inciden sobre aspectos concretos de la protección de datos, o implican también postulados de la CDFUE que analizaremos seguidamente y allí vincularemos; además de en otras partes del trabajo encargado de este análisis de la protección europea. Las que ahora siguen se encargan de manera pionera, de la interpretación de lo estipulado con carácter general en el artículo 8 del CEDH.

Así, relacionadas con la privacidad de las comunicaciones y sus interceptaciones podemos citar, entre otras, la sentencia Malone o el asunto Klass.

En primer lugar el caso **Malone contra el Reino Unido**, (nº 8691/79, de 2 de agosto de 1984). El señor Malone, comerciante de antigüedades, es acusado de delitos en relación con tenencia de bienes robados. La demanda está sustanciada sobre la base de que la "interceptación, monitoreo y grabación de conversaciones sobre sus líneas telefónicas sin su consentimiento era ilegal, incluso si se hace de conformidad con una orden del Secretario de Estado"[529]. Tas analizar la justificación o no de esta injerencia del Estado británico en las comunicaciones del señor Malone, y la legislación nacional de cobertura, aclarando que ""ley / loi" debe interpretarse que abarcan no sólo a la ley escrita sino también al derecho no escrito[530], termina fallando que, "la interferencia con el derecho del demandante en virtud del artículo 8 a que se respete su vida privada y la correspondencia (véase el apartado 64 supra) no eran "de conformidad con la ley" "necesarias en una sociedad democrática" para un propósito reconocido", proclamando la violación del artículo 8 del Convenio.[531]

Klass y otros contra Alemania, nº 5029/71, de 6 de septiembre de 1978 así como Uzun contra Alemania, nº 35623/05, de 2 de septiembre de 2010, sobre diversas formas de vigilancia.
Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987; junto con el caso S. and Marper contra el Reino Unido, nº 30562/04 y 30566/04, de 4 de diciembre de 2008, sobre almacenamiento de datos personales por parte de las autoridades públicas.
Y el caso I. contra Finlandia, nº 20511/03, de 17 de julio de 2008; y el caso K.U. Contra Finlandia, nº 2872/02, de 2 de diciembre de 2008, sobre la obligación positiva de garantía. (2014, 15)

[529] Parágrafo 15 de la sentencia.

[530] Parágrafo 66 de la sentencia.

[531] Parágrafo 80 de la sentencia.

En segundo término en el asunto **Klass y otros contra Alemania**, (nº 5029/71, de 6 de septiembre de 1978), se admite por el Tribunal una injerencia en las comunicaciones de los usuarios de los servicios postales y de telecomunicaciones (en base a la legislación alemana que la contemplaba), si bien con garantías suficientes para la evitación de abusos, no observándose aquí violación del artículo 8.

En relación con el derecho de acceso a los datos tenemos pronunciamientos clave como el caso Leander o el asunto K.U.

En **Leander contra Suecia**, (nº 9248/81, de 26 de marzo de 1987) nos encontramos con una sentencia pionera para ese derecho de acceso, tutelado por la aplicación del derecho a la intimidad y vida privada del artículo 8 del CEDH. En este caso, iniciada por demanda del señor Leander, carpintero de profesión, y trabajador interino como técnico en el Museo Naval de Karlskrona, que, por supuestos defectos en esa contratación laboral (no rellenar una encuesta previa de control por pertenecer el museo al Ministerio sueco de Defensa), se ve impedido para la misma. Ante esta situación reclama al Gobierno sueco, alegándose por el Mando Supremo de las fuerzas armadas, que los posibles accesos a zonas restringidas e informaciones secretas (al encontrarse el museo al lado de una base naval), es suficiente para desestimar su petición; y basándose además en un anexo secreto con la información depositado en el Consejo Nacional de Policía (al que no tuvo acceso el señor Laender, ni figuraba en la documentación obrante en el Tribunal). En su petición el demandante alega precisamente esa imposibilidad de acceso al documento, donde se especificaban entre otras cosas, la antigua pertenencia del carpintero al Partido Comunista sueco.

El Tribunal, tras destacar que, sin lugar a dudas ese registro secreto de la policía contenía datos relativos a la vida privada del demandante, realiza un análisis pormenorizado sobre si está justificada esa injerencia en una sociedad democrática. Sigue lo estipulado para esa comprobación: un objetivo legítimo de seguridad nacional, previsto por la ley y si es necesaria, en una sociedad democrática, para esa seguridad nacional. Esta última ha de fundarse, como sabemos, en una necesidad social imperiosa y proporcionada al fin perseguido; siendo para este caso también “preciso sopesar el

interés del Estado demandado en proteger su seguridad nacional frente a la gravedad de la violación del derecho del demandante al respecto de su vida privada". El Tribunal reconoce la amplitud de apreciación que en estos casos poseen los Estados, si bien da por buenas las doce garantías de protección adecuada, que presenta en su defensa el Gobierno sueco, y "su derecho al considerar que los intereses de la seguridad nacional prevalecían en este caso sobre los intereses individuales del demandante[532][533] (…) La injerencia que el señor Leander tuvo que soportar no se puede considerar, por lo tanto, desproporcionada al fin legítimo perseguido", desestimando la existencia de violación del artículo 8.[534]

En **K.U. contra Finlandia**, (nº 2872/02, de 2 de marzo de 2009), el demandante, que es un menor de edad, reclama verse sujeto a una publicación de un anuncio de carácter sexual en Internet. El prestador de esos servicios en la red no revela la identidad de quién publica esa información, amparándose en los principios de confidencialidad de la legislación finlandesa. Así, el menor aduce que la legislación finlandesa no establecía protección suficiente contra esas actuaciones de las que había sido víctima.

El TEDH nos dice que los Estados tienen obligación, no solo de abstenerse de injerencias arbitrarias en la vida privada, sino además de verse concernidos por obligaciones positivas que implicarían "la adopción de medidas destinadas a garantizar el respeto a la vida privada, incluso en el ámbito de las relaciones entre los propios individuos"[535][536]

[532] Ver García San José (2001).

[533] El parágrafo 56 nos dice que "el Derecho sueco da al ciudadano indicaciones adecuadas sobre el ámbito y las modalidades de ejercicio del poder" y el parágrafo 57 "La injerencia, en el presente caso, en la vida privada del señor Leander estaba por lo tanto «prevista por la ley» en el sentido del artículo 8".

[534] Parágrafos 59,67 y 68 de la sentencia.

[535] Parágrafo 43 de la sentencia.

[536] En I. contra Finlandia, nº 20511/03, de 17 de julio de 2008 tenemos otro ejemplo sobre el tema y precisamente contra el mismo Estado. En el pronunciamiento se establece que existe violación del artículo 8 CEDH por acceso ilegítimo al historial clínico de la demandante por parte de compañeros del hospital en el que trabajaba. La demandante no puede demostrar ese acceso ilegítimo perdiendo, a nivel nacional sus acciones civiles, si bien el Tribunal señala la falta de protección activa que brinda el Estado finlandés en su sistema de protección de la vida privada de la demandante.

Otras sentencias significativas, una relativa al derecho de acceso y otra en el ámbito de los datos de la salud podremos ejemplificarlas en el caso Gaskin y en el caso K.H., como líneas maestras en la difícil ponderación de los valores en juego.

Así en **Gaskin contra el Reino Unido**, (nº 10454/83, de 7 de julio de 1989), se nos ofrece otra de las sentencias pioneras en Europa sobre el derecho de acceso a ficheros, en este caso, públicos, ya que se presentó reclamación por el señor Gaskin ante el Ayuntamiento de Liverpool, institución competente en su acogimiento y guarda durante su orfandad, y durante la cual sufrió abusos y maltratos; tratando de acceder años después a los registros relativos a aquel periodo de su vida. Acceso que le fue denegado en sucesivas instancias desde 1978 hasta 1986.

El litigio en cuestión enfrenta la pretensión del demandante basada en el artículo 8 del CEDH y la violación de ese derecho, y en el artículo 10 del mismo, sobre acceso a la información, con las restricciones y limitaciones propias "de una sociedad democrática", que alegan los sucesivos organismos británicos.

El TEDH, aún entendiendo el carácter reservado que el expediente debía tener durante la minoría de edad del menor, ya que "favorecía el desarrollo eficaz del régimen de asistencia a la infancia y, hasta cierto punto, pretendía una finalidad legítima al proteger no sólo los derechos de los informantes (…), sino también los de los niños que necesitaban los cuidados"[537]; no obstante también piensa que "las personas que estén en la situación del demandante tienen un interés primordial, protegido por el Convenio, en recibir las informaciones necesarias para conocer y comprender su infancia y sus años de formación",[538] ponderándose un equilibrio muy ajustado en este caso que se juzga. Así, al final, no da la razón al demandante en cuanto al artículo 10 del CEDH, diciendo que el "derecho del señor Gaskin a recibir informaciones, protegido por el artículo 10, no sufrió ninguna injerencia"[539], con lo que su prohibición de acceso estuvo ajustada a derecho. Si bien si que observa violación en el artículo 8 del CEDH, anticipando la necesidad de existencia y actuación de las autoridades de control. Nos lo dice así: "cuando no se consigue entrar en relación con el informante o niega abusivamente su conformidad, el sistema debe proteger los intereses de cualquiera que pretenda consultar los datos sobre su vida privada y familiar; y sólo estará de acuerdo con el principio de

[537] Parágrafo 43 de la sentencia.
[538] Parágrafo 49 de la sentencia.
[539] Parágrafo 53 de la sentencia.

proporcionalidad si dispone de un órgano independiente que, en el supuesto de que un informante no conteste o no dé su consentimiento, pueda tomar la resolución definitiva sobre la cuestión. Ahora bien, no sucedió así en el caso de autos.

Por consiguiente, los procedimientos seguidos no aseguraron al señor Gaskin el respeto de su vida privada y familiar exigido por el artículo 8 del Convenio. En consecuencia, el precepto fue violado."[540]

Esta sentencia es un ejemplo de la difícil ponderación entre los valores en juego en una sociedad democrática, entre las exigencias de la confidencialidad y reserva de información para el funcionamiento y seguridad del Estado y los derechos de acceso y de información de los individuos. Como así lo reflejaron sus numerosos votos particulares y los disidentes de los señores Jueces Jörundsson, Gözübüyük, Weitzel, Danelius y Sir Bassil Hall, que no compartían la opinión de esa violación, o la votación de la Comisión Europea de Derechos Humanos al respecto, por seis votos contra seis, con el decisivo del Presidente, sobre la existencia de esa violación.

Guerrero Picó (2006) se hace eco de esas matizaciones del TEDH sobre los tres requisitos que se deben entender acerca de lo "necesario en una sociedad democrática" del art. 8.2 del CEDH. Y lo hace precisamente fijándose en algunas de las sentencias referidas (asunto Leander contra Suecia, Gaskin contra Reino Unido junto con la de Z contra Finlandia). Ese "test democrático de restricción de derechos " al que alude, deberá observar que, en primer lugar, "la injerencia debe estar prevista por ley, entendida no en sentido formal sino material, y en condiciones de precisión, claridad y previsibilidad". En segundo término: "...el parámetro de la necesidad obliga a realizar una ponderación entre los intereses públicos por los que habría que tratar la información personal y la privacidad de los individuos. La medida en cuestión tiene que responder a una "exigencia social imperativa" y no ser solamente útil o "conveniente"". Y en tercer lugar: "...el fin perseguido debe ser proteger la seguridad de Estado, la seguridad pública, los intereses monetarios del Estado, la represión de infracciones penales, la protección de la persona concernida (...) o la defensa de los derechos y libertades de otras personas..." (Guerrero Picó, 2006, 37-38).

[540] Parágrafo 49 in fine de la sentencia.

Un supuesto, en cambio, de total unanimidad jurídica, se presenta en el **caso K.H. y otros contra Eslovaquia**, (nº 32881/04, de 28 de abril de 2009), en un caso de negligencia médica de un conjunto de afectadas de hospitales públicos eslovacos, que sospechaban haber quedado estériles tras sus intervenciones de cesárea. Para ello, y con asistencia letrada, intentaron acceder y obtener copia de los archivos hospitalarios que les concernían, sin éxito, alegándose desde el Ministerio de Salud eslovaco que la legislación de aquel país impedía el acceso a registros y archivos médicos, provocándose una acción conjunta de demanda ante los hospitales responsables de esos archivos. Llegándose hasta la cúspide de las instancias con el rechazo de la reclamación por el Tribunal Constitucional eslovaco. El Tribunal, aún reconociendo la especial protección que se brindan a los datos sobre la salud, advierte del riesgo de abuso de ese principio vital, e implicando esa posición del Gobierno eslovaco una violación del derecho a la vida privada del artículo 8; si bien lo matiza hablando de una falta de efectiva protección positiva y respeto del mismo. Posición que se mantiene de manera unánime por todos los miembros del Tribunal.[541]

Esta y otra jurisprudencia del TEDH de Estrasburgo ha ido perfilando, por tanto, los requisitos para entender qué se entiende por tratamiento lícito[542] y entender así justificada una injerencia del Estado en el derecho reconocido por el artículo 8 del Convenio.

Un primer requisito es que esa injerencia esté contemplada, en todo caso, por Ley nacional, que debe cumplir determinadas características. Debe ser "accesible para las personas a las cuales concierna y previsible en cuanto a sus efectos".[543]

Una norma será previsible "si está formulada con la suficiente precisión como para permitir que cualquier persona (si es necesario, con adecuado asesoramiento) regule su

[541] Parágrafo 58 de la sentencia.

[542] Seguimos aquí la muy útil sistematización del Manual de legislación europea en materia de la protección de datos de la Agencia de los Derechos Fundamentales de la Unión Europea y del Consejo de Europa. (2014, 69, 70 y ss).

[543] Según sentencias Amann contra Suiza, nº 27798/95, de 16 de febrero de 2000, apdo. 50; o la analizada, Kopp contra Suiza, nº 23224/94, de 25 de marzo de 1998, apdo. También podemos citar Iordachi y otros contra Moldavia, nº 25198/02, de 10 de febrero de 2009, apdo. 50.

comportamiento".[544] Además el grado de precisión exigible de "la ley" depende de la materia en particular.[545]

Un segundo requisito será el de perseguir un fin legítimo.[546]

Y el tercer requisito, que la injerencia sea necesaria en una sociedad democrática, es decir, que "responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue".[547]

Más actualmente, y para la construcción de este tercer requisito, tenemos el pronunciamiento del TEDH, Khelili contra Suiza, (nº 16188/07, de 18 de octubre de 2011). En la que la demandante, ciudadana francesa, que, tras registro de la policía en Ginebra, se comprueba que portaba tarjetas en las que, junto a su número de teléfono, se presentaba como "«Mujer bonita y agradable, bien entrada en la treintena, desearía encontrar a un hombre para tomar una copa o salir de vez en cuando." La policía ginebrina, basándose en la ley cantonal de aplicación, le da de alta en un registro criminal como caso de prostitución, llegando a tomar la medida cautelar de prohibición de residencia en Suiza por dos años. La demandante niega ejercer esa profesión y años después descubre que sigue apareciendo calificada como "prostituta" en esos registros públicos. El TEDH, aún entendiendo la justificación de determinados registros,

[544] Agencia de los Derechos Fundamentales de la Unión Europea / Consejo de Europa. (2014, 69, 70 y ss) nos cita igualmente las siguientes pronunciamientos al respecto: Amann contra Suiza, nº 27798/95, de 16 de febrero de 2000, apdo. 56; Malone contra el Reino Unido, nº 8691/79, de 26 de abril de 1985, apdo. 66; Silver y otros contra el Reino Unido, números 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, de 25 de marzo de 1983, apdo. 88).

[545]Agencia de los Derechos Fundamentales de la Unión Europea / Consejo de Europa. (2014, 70) Ejemplo en la sentencia del TEDH The Sunday Times contra el Reino Unido, nº 6538/74, de 26 de abril de 1979, apdo. 49.

Otros ejemplos jurisprudenciales del TEDH relacionados son el de Rotaru contra Rumanía, nº 28341/95, de 4 de abril de 2000,(apdo. 57) o el caso Taylor-Sabori contra el Reino Unido, nº 47114/99, de 22 de octubre de 2002 también concluyendo el Tribunal en la violación del artículo 8 CEDH, y en los que, como nos ilustra el manual se produce en ambos por indefinición de los límites y los tipos en las respectivas legislaciones nacionales, en función del caso concreto.

[546] En este sentido la sentencia del TEDH, Peck contra el Reino Unido, nº 44647/98, de 28 de enero 2003, en especial, el apdo. 85. En la que no se encuentran suficiente justificación en la prevención criminal para la difusión sin consentimiento por parte de la policía a los medios de comunicación de las imágenes (sin ocultación de rostro o pixelación) captadas por su vigilancia, en la que se salva a una persona de un intento de suicidio.

[547] Apartado 58 de la sentencia del TEDH, Leander contra Suecia, nº 9248/81, de 11 de julio de 1985.

Sobre esa necesidad de ponderación y la proporcionalidad de las medidas debemos citar la sentencia del TEDH de 9 de enero de 2018 (asunto López Ribalta y otros), en el que impone la obligación de indemnización a los particulares afectados por videovigilancia en el entorno laboral (concretamente una cadena de supermercados) por parte del estado español por omisión "in vigilando" en la correcta aplicación de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de carácter Personal.

considera demasiado vaga y general la apreciación policial, resultando ese mantenimiento en el tiempo de la apelación registral ni justificado ni necesario en una sociedad democrática. Y vulnerador del artículo 8 del CEDH. Además se ordenó el pago indemnizatorio de 15.000 euros a la Sra, Khelili, víctima de esa vulneración.

2.3 El Convenio 108

El 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, es un elemento de gran importancia, a pesar del tiempo transcurrido desde su aparición, ya que se trata del primer instrumento jurídicamente vinculante internacionalmente en la materia de protección de datos, y posiblemente el elemento de fundación jurídica de esa protección en Europa y en su ámbito regional de influencia.[548]

Su origen se remonta a la preocupación surgida a partir de los años 60 y 70 a raíz de las innovaciones tecnológicas y su rápido desarrollo, que presentaba un mundo informatizado sin aparente limitación.

Al contrario que en Estado Unidos donde el derecho a la privacidad tiene una raigambre más cercana a los finales del siglo XIX y los principios del XX (como desarrollo del derecho a la intimidad y su relación con el invento de la fotografía y las publicaciones de las mismas), y si bien es evidente que se desarrollaría igualmente a partir de la informatización; en Europa parece surgir directamente de la era de la informática y sus inicios. Conceptuándose así, de manera menos problemática (de forma independiente) el derecho a la protección de datos con surgimiento de más autonomía respecto al derecho a la intimidad.

Si la Resolución 22 de 1973 y la Resolución 29 de 1974, sobre la protección de datos en el sector privado y público respectivamente, representan el inicio institucionalizado

[548] En este sentido Campuzano Tomé (2000, 79) nos habla del "primer texto internacional que permitió la armonización de las leyes de los diversos Estados y, en definitiva, el primer paso importante a la elaboración de un armazón legislativo común en el campo de la protección de datos".

de esta preocupación por parte del Consejo de Europa, en ellas se tenía por objetivo la toma de conciencia de los Estados integrantes del organismo respecto a estos asuntos, y la promoción, en consecuencia, de legislaciones nacionales de protección.

Así, y tras cuatro años de elaboración negociada, surge el Convenio 108, que pone su atención en la proporcionalidad y en la adecuación a los fines de los datos recogidos, y en los derechos de acceso y rectificación (elementos de inspiración irradiadora en las sucesivas normas europeas referidas).[549]

Hemos de apuntar que actualmente son 50 los estados parte del Convenio 108.[550]

Debemos observar además que, a pesar de que muchos países miembros han mostrado su parecer favorable a invitar a la Unión Europea a la firma del Convenio, por ahora no está dentro de los tratados abiertos por el Consejo de Europa para su firma por aquella; aún cuando se ha modificado el protocolo en 1999 precisamente para poder permitir y abordar esa futura incorporación de la UE como parte.[551]

[549] Siguiendo a Guerrero Picó (2006, 34) vemos el resumen del itinerario de aprobación "...el 28 de enero de 1981, tras varios años de negociación, se abre a la firma el Convenio número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (…) que entró en vigor el 1 de octubre de 1985, tras la ratificación de cinco Estados (Suecia, Noruega, Francia, Alemania y España). Fue elaborado por un comité de expertos gubernamentales del Comité Europeo de Cooperación Jurídica y tomaron parte en los trabajos preparatorios observadores de la OCDE y cuatro de sus Estados miembros no europeos (Australia, Canadá, Japón Y Estados Unidos), de Finlandia, de la Conferencia de la Haya de Derecho Internacional Privado y de las Comunidades Europeas. Es el primer instrumento jurídico internacional contraído con vocación universal en el ámbito de la protección de datos." Que también nos señala su estructura: el Convenio"tiene tres partes principales: las disposiciones de derecho material, enunciadas bajo la forma de principios y derechos, las que regulan los flujos transfronterizos de informaciones personales y las que establecen los mecanismos de ayuda mutua entre las Partes" (Guerrero Picó, 2006, 36)

[550] No son muchos los Estados no miembros invitados (teniendo 5 años de vigencia la invitación), entre los que se encuentran Marruecos o Cabo verde, si bien los que lo han ratificado son Uruguay, Mauritania y Senegal. Ver Consejo de Europa, recuperado el 15 de agosto de 2018: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa

[551] Y no solo son favorables a la incorporación de la UE sus Estados miembros (en la que todos se muestran de acuerdo) sino también otros estados como Rusia y Suiza.
Ver en este sentido Consejo de Europa: Modificaciones del Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (CETS nº 108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros, en Estrasburgo, el 15 de junio de 1999; artículo 23, apartado 2, del Convenio nº 108 en su forma modificada.

Sin perder de vista su razón de ser en la intensificación de la circulación de datos a través de las fronteras, el Convenio justifica su fin en la conciliación de esa circunstancia con el respeto a los valores y derechos de la vida privada, y concretamente en el ámbito del tratamiento automatizado de los datos de carácter personal.

Las definiciones del artículo 2 han sido de enorme influencia en el establecimiento jurídico conceptual de la protección de datos europea. A modo de ejemplo vemos el carácter de datos personales definidos como "cualquier información relativa a una persona física identificada o identificable", (que, como veremos, es piedra angular en toda la arquitectura jurídica de la protección de datos europea).

Los conceptos clave en la protección de datos de fichero y tratamiento automatizado y el de autoridad de control también son originarios del Convenio.

La importancia de estas definitorias podemos apreciarla en que, por ejemplo, el concepto de datos personales con arreglo al CEDH, es el que se contempla en el Convenio 108, sobre todo en base a lo que esté relacionado con personas identificadas o identificables, tal y como ha indicado el propio TEDH en algunos pronunciamientos.[552][553]

En lo relativo al significado de "tratamiento", el artículo 2, letra c) permite que pueda ser ampliado por el Derecho nacional en lo que respecta a incluir el tratamiento manual. En este sentido, es llamativo que el derecho de la UE lo incorpora, como veremos en el Capítulo concerniente a esta regulación.

La aplicación del Convenio cubre a los ficheros y tratamientos automatizados de datos de los sectores público y privado, si bien cualquier Estado, en el momento de firma o ratificación o ulteriormente, puede comunicar al Secretario General del Consejo de

[552] Amann contra Suiza, nº 27798/95, de 16 de febrero de 2000 apdo. 65, Odièvre contra Francia, nº 42326/98, de 13 de febrero de 2003; y Godelli contra Italia, nº 33783/09, de 25 de septiembre de 2012

[553] Igualmente y sobre el carácter de "identificable" ver Consejo de Europa: Comité de Ministros (1990), Recomendación nº R Rec(90) 19 relativa a la protección de los datos personales utilizados para el pago y otras operaciones conexas, de 13 de septiembre de 1990.
Recuperada el 25 de septiembre de 2018:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e15cd

Europa que no aplicará, bien determinadas categorías de ficheros de datos, bien determinadas informaciones "relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica",[554] (se observa ya aquí originariamente la excepción o la especialidad propia de partidos y confesiones religiosas que llega en la regulación hasta hoy). O bien ficheros que no sean objeto de tratamientos automatizados (se comprueba también ya aquí la excepción de los ficheros domésticos). Estas declaraciones de excepción son revocables en cualquier momento y en igual forma por el Estado que las emitió.

El Capítulo II (Artículos 4 a 11) del Convenio recoge los principios que serán fundacionales y fundamentales para la protección de datos en Europa, y que recopilarán de uno u otro modo, las distintas normas europeas y nacionales con posterioridad. Así, se instituyen el principio de calidad de los datos que incluye su obtención y tratamiento leal y legítimo, adecuados, no excesivos y pertinentes a los fines también legítimos, exactos y de conservación no más allá de lo necesario. Vemos cómo, de ese principio, se vendrán a expandir otros habituales en la protección de datos, y su tratamiento en Europa. De igual manera, se recoge el principio de particularidad de los datos que contengan "origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual", y también para los "referentes a condenas penales". Principio que ha constituido una constante hasta nuestros días, con determinación además de normativa especializada y diferenciada para los datos de origen penal.

El principio de seguridad de los datos se contempla igualmente, así como el principio que servirá de germen de los derechos ARCO (acceso, rectificación, cancelación y oposición), bajo el genérico título de "garantías complementarias para la persona concernida" con el derecho de información y acceso, el de rectificación o borrado y el derecho a recurso o reclamación.

Se establecen además las garantías que serán elemento sustancial, y con carácter principal, del derecho a la protección de datos en las futuras normativas europeas.

[554] Artículo 3.3 letras a) a c)

También las excepciones que hoy consideramos habituales se presentan originariamente en el Convenio, y "siempre que sea una medida necesaria en una sociedad democrática: a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de otras personas."[555]

Debemos citar en este ámbito de atención a los datos sensibles la actuación jurisprudencial en el caso Z. contra Finlandia, (nº 22009/93, de 25 de febrero de 1997). El ex marido de la demandante, infectado con VIH, había cometido una serie de delitos sexuales, por los que se le condena por homicidio, ya que los tribunales finlandeses apreciaron intencionalidad consciente en la exposición al contagio a sus víctimas. Se ordena por el Tribunal que la sentencia y las actuaciones judiciales relacionadas siguieran siendo confidenciales durante diez años. La demandante solicitaba un periodo mayor, que en apelación se le deniega, ya que la sentencia incluía su nombre completo. La Corte de Estrasburgo que afirmó no estar convencida "de que, al prescribir un plazo de diez años, las jurisdicciones internas hayan acordado suficiente peso a los intereses de la requirente", y que "el interés que hay a proteger la confidencialidad de tales informaciones pesará fuertemente pues en el balance cuando se trate de determinar si la injerencia era proporcionada al fin legítimo perseguido, sabiendo que una tal injerencia no puede conciliarse con el artículo 8 de la Convención (art. 8) sino cuando ella mira a defender un aspecto primordial del interés público"[556]; acaba sosteniendo injustificada esta injerencia por la divulgación "en la sentencia de la corte de apelación de Helsinki, hecha pública, de la identidad y del estado de salud".[557]

Se contemplan también las restricciones a los derechos para los datos que se "utilicen con fines estadísticos o de investigación científica" si bien aquí se ha ido subiendo el listón, en la posterior normativa con la ampliación del concepto "cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas" por el de que puedan afectar a sus derechos y libertades o al de terceros.[558][559]

[555] Artículo 8 y 9. Ver García San José (2001)
[556] Parágrafos 96 y 112 de la sentencia.
[557] Parágrafo 113 de la sentencia.
[558] Artículo 9.3.
[559] Dentro de la Jurisprudencia del Tribunal Europeo de Derechos Humanos relativa al acceso podemos encontrar algunos pronunciamientos importantes como son las siguientes sentencias: Godelli contra

El establecimiento de sanciones y recursos y la posibilidad de una protección más amplia se prevén también en el Convenio.[560]

Los flujos transfronterizos de datos se contemplan en el capítulo tercero, anticipando, asimismo, las regulaciones venideras sobre estos flujos motivados por la globalización del mercado, y la necesidad de amparar, aún mínimamente, los derechos de los afectados por ese incesante devenir de información mundial[561]. El artículo está orientado más bien a la no paralización de esos flujos (garantía del mercado) que a la protección propia del derecho, y habla de la posibilidad de excepción solo para determinadas categorías de datos, o en caso de posible fraude de ley con un Estado interpuesto en ese flujo[562]. Aquí, la corriente de protección ha cambiado en Europa, y ha ido evolucionando desde esta previsión, pasando por la inspiración mercantilista aunque más protectora de la Directiva del 95, hacia la matización sin complejos de esos flujos, motivada por el respeto al derecho fundamental que supone la protección de datos, en el nuevo paquete reformador de 2016, con el exponente principal del Reglamento.

El Capítulo Cuarto,[563] bajo el título de "asistencia mutua", pone el andamiaje de la colaboración y cooperación interestatal en la protección de datos en Europa y la previsión primera de las autoridades de control que son ya instituciones consagradas en esa normativa europea de protección, que partían como engranaje esencial en esa colaboración. Igualmente relacionado nos encontramos con la previsión de un Comité Consultivo (al igual que los establecidos en las distintas normativas posteriores), con

Italia, nº 33783/09, de 25 de septiembre de 2012; K.H. y otros contra Eslovaquia, nº 32881/04, de 28 de abril de 2009; Odièvre contra Francia , nº 42326/98, de 13 de febrero de 2003; (y las anteriormente Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987; Gaskin contra el Reino Unido, nº 10454/83, de 7 de julio de 1989).

[560] Artículos 10 y 11, viéndose su carácter de protección elemental y de partida, que al menos se pone de límite mínimo a cumplir en la región europea y del ámbito del Consejo de Europa.

[561] Artículo 12.

[562] Ver Protocolo Adicional y Pavón Pérez (2002).

[563] Artículos 13 a 17.

carácter asesor y de impulso y seguimiento, en la materia que se viene a establecer en el Capítulo Quinto[564].

En cuanto a la valoración del texto, seguimos de nuevo a Guerrero Picó (2006), que piensa en modo conclusivo que tiene a su favor que: "prevé que los Estados protejan a las personas frente a injerencias de los poderes públicos y contra abusos del sector privado; es un instrumento flexible, la generalidad de sus términos favorece la vigencia de las pautas que proporciona (...); es el único texto mundial de protección de datos personales jurídicamente vinculante; no admite la formulación de reservas lo que tiende a garantizar una equivalencia en la protección asegurada..."

Si bien observa también algunas objeciones como las de que "... no es directamente aplicable; no integra normas para resolver conflictos de ley aplicable (...); el margen de elección que da a los Estados puede dificultar la constatación de si existe un nivel d protección equivalente que permita realizar una transferencia internacional y puede utilizarse para escamotear garantías a los ciudadanos..." Preguntándose, por último, si "basta con la protección brindada por el Convenio..." Haciéndose eco de la posible elevación de ese derecho con mejoras y protocolos adicionales al mismo (Guerrero Picó, 2006, 40-41).

Sobre una valoración de futuro y el análisis de la posible modernización del Protocolo, Greenleaf (2016) lo califica como un standard internacional válido, incluso para que sea adoptado por las Naciones Unidas como referente (Greenleaf, 2012), dando una visión de la relevancia de origen y futuro de esta norma en su repercusión internacional.

[564] Artículos 18 a 20. El resto de capítulos (sexto y séptimo) se encargan de cuestiones procedimentales y estipulaciones finales, destacándose la voluntad de inclusión del Convenio en su artículo 23, abriendo la posibilidad de unión por invitación a Estados no miembros del Consejo de Europa.

3. La protección de datos en la Carta de Derechos Fundamentales de la Unión Europea.

3.1 El artículo 8 de la Carta

Es en la Carta[565] donde el derecho a la protección de datos se estipula ya de manera concreta y determinada como tal, en el ámbito de la Unión Europea. Lo hace en el artículo 8 (número mágico en esta constitucionalización de la protección de datos en Europa), que nos presenta el siguiente literal:

"Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

Así, Kranenborg (2014) nos dice que hay un debate en la literatura legal sobre la diferencia entre el derecho a la privacidad y el derecho a la protección de datos: "un

[565] En 1999 el Consejo Europeo se eecarga de recoger en una Carta los derechos fundamentales vigentes en la UE t la Carta queda formalmente proclamada por las tres Instituciones de la Unión en Niza en diciembre de 2000, pero no será jurídicamente vinculante hasta el Tratado de Lisboa y su entrada en vigor el 1 de diciembre de 2009, estando ya equiparada a los postulados de los Tratados.
La Carta de Derechos Fundamentales además de su preámbulo contiene 54 artículos en 7 capítulos:
El capítulo I sobre la dignidad, el capítulo II sobre la libertad (en el que está ubicado el derecho a la protección de los datos de carácter personal), el capítulo III sobre la igualdad, el capítulo IV referido a la solidaridad, el capítulo V sobre ciudadanía, el capítulo VI relativo a la Justicia, y por último, unas disposiciones generales en el capítulo VII.
Un lúcido resumen para entender el espacio común de derechos fundamentales que supone la Carta lo encontramos en Carmona Contreras (2016).

vínculo conceptual entre ambos derechos se hace con la introducción de la noción de autodeterminación informacional que implica el control sobre la propia información personal de cada uno". Esa noción de "autodeterminación informacional", que tiene raíces germanas, según el autor "no es igual a la protección de datos generalmente considerada en el Consejo de Europa y en la UE". La autodeterminación informacional implica y está vinculada al consentimiento para el procesamiento de datos como noción clave para su legalidad. Sin embargo en la Convención 108 no jugaba un papel determinante, si bien en la legislación de la UE el consentimiento sí se va a ir creciendo en su importancia para terminar siendo uno de los campos de su legitimidad en la Directiva de 1995.

El sistema de la UE, por tanto, es más bien un sistema de checks and balances, y parece no resultar la propuesta alemana de la autodeterminación informacional (o informativa) vencedora en la conceptuación del derecho en Europa, que hubiera imbricado los dos conceptos en uno nuevo (Kranenborg 2014, 229).

Vemos así como la sustanciación de la privacidad en Europa que parte de esa concepción alemana de la autodeterminación informativa para plasmar el derecho a la privacidad de manera coherente en Europa, va evolucionando, empujada tanto por la via jurisprudencial, que va dejando unn sedimento jurídico importantísimo, como por el camino de plasmación normativa para llegar a ese elemento propio y diferenciado que es la protección de datos europea.

Por tanto, como vemos, el derecho a la privacidad y a la protección de datos están estrechamente unidos, pero no deben considerarse el mismo derecho. La inclusión como derecho separado en la Carta así lo viene a confirmar[566].

Esa sustantividad propia se aprecia al tener en cuenta que el artículo precedente se encarga del respeto de la vida privada y familiar, produciéndose así su diferenciación de manera expresa. El literal del artículo 7 nos dice en un precepto amplio: "Toda persona

[566] Una referencia de visión general sobre la diferenciación la encontramos en Blume (2010). Autores como Kokott & Sobotta (2013) anotan, ya más jurídicamente, la diferenciación de los conceptos desde el estudio de las distintas aproximaciones jurisprudenciales por parte del Tribunal de Justicia de la Unión de Luxemburgo y del Tribunal Europeo de Derechos Humanos de Estrasburgo.

tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."

En este sentido, Coudhry (2014, 153), nos ilustra sobre la sustitución de la palabra comunicación a la habitual de correspondencia, debido al desarrollo tecnológico en comparación con el artículo 8 del CEDH. Hace un recorrido de análisis sobre el artículo parándose en la sentencia del TJUE en el caso Nexaus France SAS and Nexaus SA contra la Comisión Europea de 14 Noviembre de 2014 (Asunto 135/09), en el que nos dice el tribunal que "la necesidad de protección contra la intervención arbitraria o desproporcionada por las autoridades públicas (…) constituye un Principio General del Derecho de la UE". Coincide ello con la Cuarta Enmienda americana y su conexión con el artículo 7 de la CDFUE y el 8 del CEDH, y conectado al artículo 17 de la Convención Internacional de Derechos civiles y políticos.

Para la definición de la palabra "comunicaciones" debemos observar, con la autora, que parece ser absorbida por el concepto más amplio y general de "vida privada" y así también, incluso en su esfera de protección. Esa protección incluye, no solo correspondencia "íntima" o de naturaleza íntimamente privada entre personas naturales, sino también correspondencia profesional y comercial (Coudhry, 2014, 154).

Y ello, y siguiendo el recorrido de análisis de la autora, ya según sentencias del TEDH, en los casos Kopp, Wieser y Bicos Beteilungen GmbH e Iliya Stefanov, relativas todas a las búsquedas e intervención de comunicaciones realizadas en el entorno profesional de despachos legales y de abogados, y que aportan luz sobre lo contenido en este precepto. Además de que las comunicaciones se venían considerando protegidas con independencia de su emisión, recepción o almacenamiento en lugar de trabajo, según sentencia del TEDH en el caso Halford (Coudhry, 2014, 154).[567]

[567] En la sentencia ya vista de Kopp contra Suiza de 25 de marzo de 1998; sentencia nº 74336/01 Wieser y Bicos Beteilungen GmbH contra Austria de 16 de octubre de 2007; sentencia nº 8429/05 Iliya Stefanov contra Bulgaria de 22 de mayo de 2008. Y en la Sentencia Halford contra U.K. (73/1996/692/884) de 25 de junio de 1997.
Siguiendo el análisis, esta interpretación del Tribunal de Estrasburgo parece haber dado un giro según una última sentencia de 2016 en el caso Bàrbelescu en el que la monitorización de una empresa del correo de un trabajador (del servidor Yahoo Messenger y creado por la empresa a efectos laborales) se entiende que no vulnera el artículo 8 del CEDH, como se comprueba en la sentencia 61496/08 Bàrbelescu contra Rumanía de 12 de enero de 2016. En cuanto al concepto de nombre e identidad personal el TEDH lo vincula también al ámbito familiar, por la posible identificación de parientes que puede acarrear (Sentencia Burghartz v. Suiza de 22 de febrero de 1994).

Debemos recordar que todo ello debe estar acorde con los artículos 51 y 52 de la Carta, y que establece el ejercicio mediato de estos derechos, y sus limitaciones por la ley europea y nacional en la aplicación del artículo 7 de la CDFUE.[568]

Una aproximación crítica a este primer esfuerzo de sistematización constitucional que intenta llevar a cabo la CDFUE en el derecho a protección de datos lo tenemos en Ruiz Miguel (2003, 10) que opina que "no establece un estatuto jurídico único para el derecho a la protección de los datos personales, sino más bien una multiplicidad de regímenes, todos ellos válidos, cuya aplicación eventualmente se solapa; por otro lado, es ambigua al determinar la cuestión de si los derechos de las Constituciones estatales tienen fuerza normativa, como tales, "en el nivel europeo"".

En sentido contrario en cambio Azpitarte Sánchez (2005, 357) sí contempla ese bagaje de fuerza conformadora del derecho nacional en el escenario europeo de protección de derechos fundamentales: "Quizá, los derechos constitucionales estatales y los principios generales comunitarios coincidan en el punto de partida. No obstante, se enriquecen en su punto de llegada, plural y diverso debido a las múltiples causas que provoca el amparo de los derechos fundamentales."

Elementos de cuestión que, además, la aprobación y aplicación del Reglamento General de Protección de Datos viene a solucionar en cuanto a esa posible multiplicidad de regímenes aludida, ya que el Reglamento sirve, con independencia de su desarrollo o complemento por las legislaciones nacionales, como veremos, de marco estatutario común innegable en la protección de datos europea con fuerza directamente vinculante. Aprobación normativa que, además, da la razón, en el ámbito del derecho fundamental de protección de datos, a esa conformación de llegada que recoge los elementos del derecho europeo en todos sus campos (también el de la aportación estatal).

[568] Como ejemplo de este tipo de limitaciones referenciamos las conclusiones del Abogado General Mengozzi en el caso Dereci de fecha 29 de septiembre de 2011, y que deja fuera del estatuto de ciudadanía europea su extensión a familiares no comunitarios. En este sentido, y sobre la sentencia ver Juárez Pérez (2012).

3.2 Las condiciones de las limitaciones lícitas con arreglo a la Carta de la UE

Debemos destacar que la Carta y el CEDH son distintos a la hora de estructurar el derecho, variando en su contenido y también en su forma de limitarlo. La Carta establece unas estipulaciones concretas que permiten un punto de partida sin, en principio, la deducción jurisprudencial que hemos visto en el CEDH y el TEDH.

Así nos dice el artículo 52.1 de la Carta:

"Alcance e interpretación de los derechos y principios

1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás."

De lo que debemos deducir que la limitación solo será válida en caso de que: la establezca una ley; que respete el contenido esencial de los derechos y libertades de que se trate; que la limitación sea necesaria, siguiendo el principio de proporcionalidad; y responda efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.[569]

A pesar de las diferencias, vemos que se repiten en estas condiciones del tratamiento lícito de este artículo lo dispuesto esencialmente en el CEDH y en su artículo 8.2, sobre todo al tener en cuenta el propio apartado tercero del artículo 52 de la Carta: "en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y

[569] En estos casos la labor jurisprudencial no ha dejado tampoco de ser sumamente importante, y a pesar de la previsión del precepto. En este caso, por parte del Tribunal de Luxemburgo en la Sentencia del TJUE, asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen, de 9 de noviembre de 2010, apdos. 89 y 86.

de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa."

Que vincula directamente, por tanto, con esos requisitos mínimos en interpretación del artículo 8 del CEDH, vistos en el anterior apartado, para esas limitaciones y su consideración como lícitas.

Además, sobre el artículo 8 de la Carta (al igual que para el 8 del CEDH) y la necesidad de ponderación del derecho y sus posibles limitaciones en ambos preceptos, debemos apuntar los siguientes pronunciamientos judiciales de los tribunales europeos: la sentencia del TEDH, Von Hannover contra Alemania asuntos 40660/08 y 60641/08, de 7 de febrero de 2012; y las sentencias del TJUE, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado, de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10), y la sentencia del TJUE, Productores de Música de España (Promusicae) contra Telefónica de España SAU, de 29 de enero de 2008 (asunto C-275/06).

De igual manera debemos tener en cuenta, además de la "inalcanzable" adhesión de la UE al CEDH del 6.2, el artículo 6.3 del Tratado de la Unión Europea que nos dice: "los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales". Con lo que como nivel mínimo, y por ahora y mientras no se alcance la adhesión, esas estipulaciones sobre el CEDH son principios generales a seguir y respetar de manera obligada por el ordenamiento de la Unión. Si bien esa falta de adhesión formal directa por parte de la UE viene siendo salvada, como hemos apuntado, por el artículo 52.3 de la Carta, en un ejemplo perfecto de la complementariedad del carácter multinivel del derecho europeo.

3.3 La sentencia contra el Land de Hesse

La sentencia del Tribunal de Justicia (Gran Sala) de 9 de noviembre de 2010, Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen (asuntos acumulados C-92/09 y C-93/09), nos sirve como ejemplo de interpretación de la Carta en materia de protección de datos; y más concretamente es importante por juzgar las limitaciones del derecho a la protección y su necesidad de justificación, como ya hemos apuntado en el anterior epígrafe.

Interpreta los artículos 8 y 9 de la CDFUE, así como los artículos 18 y 20 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Aquí dos demandantes (una empresa agrícola y un agricultor), entran en controversia jurídica con el Land de Hesse por la publicación en la página de este Estado Federado de datos de carácter personal relacionados con el cobro de ayudas Feader y FEAGA. Entra también aquí en juego el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, así como la 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, al igual que los dos Reglamentos reguladores de los Fondos y por la que se modifica la Directiva 2002/58/CE.[570]

Los demandantes alegan la inexistencia de intereses públicos preponderantes que justifiquen la publicación de los importes que han percibido. La región alemana considera tener una obligación de publicación en base a los dos Reglamentos citados.

[570] Reglamento (CE) nº 1290/2005 del Consejo, de 21 de junio de 2005, sobre la financiación de la política agrícola común y el Reglamento (CE) nº 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento nº 1290/2005 en lo que se refiere a la publicación de información sobre los beneficiarios de fondos procedentes del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (FEADER). Siendo el artículo 44 bis del Reglamento de 2005 donde se establecen estas publicaciones de los beneficiarios.

El órgano judicial preguntante estima, asimismo, una posible violación de los derechos fundamentales referidos en su cuestión.

El Tribunal separa nítidamente en su respuesta las dos cuestiones, para recordar al órgano jurisdiccional alemán que la CDFUE, también en su artículo 8 que consagra el derecho a la protección de datos personales de la persona, "no constituye una prerrogativa absoluta", y recuerda, además, el literal del segundo apartado del artículo, así como el del 52 de la Carta, que ya matizan normativamente en este sentido al derecho enunciado.[571]

Continúa la sentencia sobre el tema de la publicación requerida en el 44 bis y de si esa injerencia (que admite como tal) establecida por Ley, constituye una violación del derecho fundamental a la protección de datos o está amparada por las excepciones de la Directiva.

Y se decanta el Tribunal por esta última situación con la atención a la necesidad de transparencia pública que se debe seguir "al reforzar el control público sobre la utilización de los importes abonados por el FEAGA y el Feader. La publicación exigida por las disposiciones cuya validez es objeto de controversia, contribuye a que la Administración utilice apropiadamente los fondos públicos", siendo este considerado "un objetivo de interés general reconocido por la Unión." Si bien hace la sentencia posteriormente llamamientos a la ponderación permanente por parte de los poderes públicos implicados, para conciliar los derechos de privacidad y transparencia. Pero considera, a su vez, adecuada la normativa europea en este caso para las personas jurídicas.[572]

Sí que fija su atención el Tribunal en la preponderancia jurídica de los datos de las personas físicas, haciendo para ellas efectiva la invalidez de los artículos de los Reglamentos en cuestión. Ahora bien, limita la invalidez temporalmente y por razones de seguridad jurídica, a partir de la fecha de la sentencia.[573]

---

[571] Parágrafos 48 a 51 de la sentencia.

[572] Parágrafos 69 y 71 de la sentencia y Parágrafo 88 donde nos dice que "procede concluir que, en la medida en que se refieren a la publicación de los datos relativos a personas jurídicas, las disposiciones del Derecho de la Unión cuya validez pone en duda el órgano jurisdiccional remitente respetan un justo equilibrio en lo que respecta a la toma en consideración de los intereses que aquí se enfrentan".

[573] El parágrafo 92 nos ilustra: "que los artículos 42, punto 8 ter, y 44 bis del Reglamento nº 1290/2005 y el Reglamento nº 259/2008 son inválidos en la medida en que obligan, por lo que respecta a las personas físicas beneficiarias de ayudas del FEAGA y del Feader, a publicar datos de carácter personal de

Para terminar, el Tribunal interpreta propiamente la Directiva, y afirma que ni el artículo 18 ni el artículo 20 de la misma imponen al encargado del tratamiento la obligación de llevanza de registro antes del tratamiento de los datos personales ni el sometimiento de los controles previos contemplados para la publicación de informaciones de los Reglamentos de los Fondos Agrícolas.[574]

Y se dan por lo tanto en la sentencia dos pronunciamientos diferenciados: el de interpretación de aplicación de la Directiva propiamente para el caso concreto, y el de declaración de invalidez de los artículos de los Reglamentos sobre la financiación de la política agrícola común y el de su aplicación sobre el Fondo Europeo Agrícola de Garantía (FEAGA) y el Fondo Europeo Agrícola de Desarrollo Rural (Feader) (artículos 42, punto 8 ter, y 44 bis) en sus publicaciones respecto a las personas físicas perceptoras de esas ayudas.

La sentencia nos sirve, así, para comprobar la importancia del principio de proporcionalidad, como elemento configurador del derecho europeo y componente importante en la interpretación de la CDFUE, concretamente en su aplicación al derecho de protección de datos europeo. Y sirve de referencia jurisprudencial, además, de la ponderación como piedra de toque para que entren en juego las condiciones de justificación de esa protección en Europa.

---

todos los beneficiarios, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas han percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas"

[574] Coincidiendo aquí sustancialmente con las conclusiones de la Abogado General Eleanor Sharpston presentadas el 17 de junio de 2010.

4. Consideraciones

Por último, y a modo de recapitulación, deberemos destacar la importancia de raíz generadora que lo establecido en este capítulo supone para la posterior progresiva aprobación y consolidación de la normativa europea en materia de protección de datos. Principalmente nos estamos refiriendo a la labor del Consejo de Europa y de su Convenio 108 en esa moldura, impulso y origen de justificación en este derecho y en su protección. Y el primer hito para su consideración dentro del abrigo de los derechos fundamentales europeos.

Así, seguiremos la percepción de Téllez Aguilera (2002) cuando nos ofrece su visión de la alimentación del derecho de la UE en la fuente originaria del Consejo de Europa, en cuanto al derecho de protección de datos se refiere; y de la importancia del Convenio 108 como antecedente irradiador de la futura legislación europea. Sobre todo, en cuanto a la conceptuación como derecho humano de aquel. Su obra, además, presenta interés como consulta de los antecedentes e inspiraciones de las legislaciones nacionales en la construcción del derecho a la protección de datos europeo. Elementos de inspiración que van desde la Resolución 22/1973 de 20 de noviembre del CdE sobre regulación de los ficheros electrónicos en el sector privado hasta las Recomendaciones de la OCDE de 26 de noviembre de 1992 relativa a la seguridad de los sistemas de información, pasando por las leyes alemana, francesa, danesa o luxemburguesa de los años 70, que antes hemos citado.

Nos arroja también luz sobre el recorrido paralelo que ha llevado el reconocimiento de los derechos humanos en el Derecho de la Unión, y el de protección de datos en el mismo. A veces, cruzándose en su asentamiento y en manifiesta conexión. La culminación se puede ver, para ambos, con la llegada de la CDFUE, en la que como dice el autor, “si se examina toda la Carta, puede fácilmente comprobarse que este derecho a la protección de datos de carácter personal es uno de los más ampliamente explicitados en dicho texto, y evidenciándose cómo el mismo viene desligado de los derechos al respeto a la vida privada y familiar, el domicilio y las comunicaciones (…)

La importancia del derecho consagrado en el artículo 8 debemos deducirla del valor que estos Derechos Fundamentales tienen en la propia Carta...” (Téllez Aguilera, 2002, 64)

Se nos ofrece así, una medida de la relevancia de este derecho como paradigma de esa necesaria constitucionalización a nivel europeo de los derechos fundamentales, que recorren, desde Estonia a Portugal, la vida jurídica diaria de todos los europeos.

CAPÍTULO SEGUNDO

EL RECORRIDO NORMATIVO DE LA PROTECCIÓN DE DATOS EUROPEA EN EL DERECHO DERIVADO.

El derecho derivado europeo en materia de protección de datos está marcado por dos grandes hitos: la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que además pone fecha de derogación a aquella a partir del 25 de mayo de 2018.[575]

Las dos normas son hijas de su tiempo, y forjan, de manera determinante, la protección de los ciudadanos europeos (irradiando una influencia jurídica internacional muy importante) en su derecho a la protección de datos, así como en la evolución normativa del propio derecho.

La Directiva, como veremos, supone un salto posibilista de gran calado, que utiliza al mercado (al igual que éste utiliza la protección de datos), como elemento armonizador para establecer una protección más o menos homogénea a lo largo de Europa, con resultados muy satisfactorios en ambos estamentos. El Reglamento, del que nos ocuparemos en profundidad en el siguiente capítulo, ofrece ya una dimensión más integradora e integral de la protección de los datos como derecho fundamental, directamente exigible y homologado a nivel europeo; que supone un verdadero salto adelante en la defensa de la protección de datos como modelo dentro del campo de los Derechos Humanos, siendo signo netamente europeo en el ámbito global.

[575] Artículo 94 del Reglamento.

Entretanto, dejaremos plasmadas las sucesivas e importantes aportaciones normativas que el Derecho Derivado europeo ha ido alumbrando en ese intervalo jurídico: desde el paquete de Directivas del marco de comunicaciones electrónicas, hasta el destacado Reglamento de 2001 sobre protección de datos en las instituciones europeas, un, asimismo, pequeño gran hito en esta forja de la protección de datos en Europa que nos ocupa.

Así, por tanto, abordaremos en este capítulo en primer lugar como antecedente clave la mención a la Directiva. Aludiremos después a las definiciones de la protección de datos en el Reglamento en comparativa con la Directiva, así como a su delimitación jurisprudencial, finalizando con las indicaciones del importante desarrollo del Derecho Derivado entre ésta y aquel. Y, por último, dejaremos planteado el Reglamento, cuyo contenido (o el de la protección de datos europea en general), vendrá desarrollado en el siguiente capítulo.

1. La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre

1.1 Introducción

A principios de los años 90 se inicia la tramitación del entonces procedimiento de codecisión de la Directiva, que, por vez primera, introducía en el ordenamiento comunitario un incipiente derecho de protección de los datos personales.[576]

Como antecedentes de la Directiva tenemos que hablar, como ya apuntábamos al inicio del trabajo, de la Ley del Land de Hesse de 1970 y la Ley de Suecia de 1972, que pueden considerarse las dos normas positivas originarias de la protección de datos en Europa.

Para ilustrarnos sobre los precedentes de la Directiva y de la protección de datos en Europa seguiremos las consideraciones de Heredero Higueras (1997), que se remonta a la preocupación manifestada por la Comisión en 1973 (y propia de los tiempos) en la Comunicación: "Una política comunitaria de informática". Y así como nos relata ya en 1974 "Lord Mansfield presentó ante el Parlamento Europeo el estudio bajo su dirección (en sesión de 21 de febrero de 1975) y nueva Resolución del Parlamento de 8 de abril de 1976 en la que el Parlamento animaba a la diligencia de la Comisión en sus estudios sobre el tema" (Heredero Higueras, 1997, 17-20).

También se remite al Informe Bayerl, que da lugar a la Resolución del Parlamento Europeo de 8 de mayo de 1979, y que sigue de cerca el Convenio 108 del CdE, y lo completa con un órgano de protección que no venía previsto en el instrumento del Consejo de Europa.[577]

---

[576] Con el procedimiento de codecisión 1990/0287/COD siendo su adopción por la Comisión de fecha 18 de julio de 1990, terminándose el procedimiento, tras cinco años, con la aprobación del Consejo en segunda lectura el 24 de julio de 1995 y firma del Presidente del Parlamento y del Consejo en fecha 24 de octubre del mismo año. Podemos consultar su procedimiento de aprobación (recuperado el 24 de agosto de 2018) en:
https://eur-lex.europa.eu/legal-content/ES/HIS/?uri=celex:31995L0046

[577] Resolución de 8 de mayo de 1979 del Parlamento Europeo, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática (DOC 140 de 5 de

Siguiendo al autor, podemos decir que los años 80 fueron aciagos en la consecución de una norma europea, y que no es hasta el año 1990 cuando se presenta una propuesta de Directiva. Si bien es verdad que el Acta Única Europea supuso un avance conocido para dotar de fundamento jurídico a la misma, cimiento que antes de 1986 no existía sobre el que edificar la efectiva protección de datos en Europa (1997, 23y ss.). Es decir, no había base jurídica en el Derecho Originario previamente para sustentar la protección. A pesar de ello, la propuesta de Directiva SYN 287 de 1990 sufrió problemas de interpretación en la consistencia de su base jurídica. Las principales inspiraciones normativas de la norma se encontraban en la Ley alemana, en el Convenio 108, en la Ley francesa y, en la belga, así como en la de Reino Unido, y en la de los Países Bajos, y gozó de la cooperación del Parlamento Europeo, siendo las negociaciones en el Consejo las que suscitaron mayores controversias (1997, 33-44).[578]

Se presenta así nueva propuesta por la Comisión en julio de 1992, con contrapropuesta de Alemania, Dinamarca Irlanda y Reino Unido el 15 de octubre de 1993, para llegar al texto definitivo bajo presidencia griega del Consejo el 20 de febrero de 1995.[579]

Debemos incidir, de nuevo, en la influencia del Convenio 108 en su espíritu y en su redacción, (que incide también en su coincidente voluntad expansiva dejando abierta la Directiva al igual que el Convenio su aplicación territorial a otros países), que nos dice que la Directiva de protección de datos está diseñada para dar contenido a los principios del derecho a la privacidad ya contemplados en el Convenio nº 108, así como para ampliarlos.

El hecho de que, en 1995, todos los estados miembros de la UE también fueran Partes Contratantes del Convenio nº 108 excluye la adopción de normas contradictorias de protección de datos, sin embargo la Directiva ofrece la posibilidad, contemplada en el artículo 11 del Convenio nº 108, de añadir instrumentos de protección. En particular, la introducción de una supervisión independiente como instrumento de mejora del

---

junio).

[578] Apuntaremos también aquí el interés que presenta el dictamen de la Comisión de Asuntos Jurídicos de enero de 1992, así como la conceptuación y diferenciación de fichero (y derecho) público y privado que supuso un choque de percepciones del derecho entre las tradiciones anglosajonas y continentales, o más resumidamente entre Reino Unido e Irlanda y Francia.

[579] Como referencia en la consulta citaremos también a Téllez Aguilera (2002) como competente referencia diseccionadora del proceso de aprobación de la Directiva 95/46/CE, así como de los antecedentes y preliminares de la protección de datos en Europa.

cumplimiento de las normas de protección de datos demostró ser una importante aportación al eficaz funcionamiento de la legislación europea en materia de protección de datos. (Por consiguiente, esta característica fue adoptada en el Derecho del CdE en 2001 a través del Protocolo adicional al Convenio nº 108)" (ADFUE/CoE, 2014, 19), demostrando así una positiva retroalimentación entre ambos cuerpos normativos.

1.2. Obstáculos para su plena transposición.

La Directiva, como sabemos, supuso una verdadera revolución en la consolidación del derecho a la protección de datos en Europa. Asimismo, se convirtión en un modelo regional de referencia mundial. Su pequeña extensión, con ánimo marcadamente flexible, no ha impedido que se hayan dado dificultades en su transposición efectiva en distintos Estados miembros, que llegan hasta fechas cercanas. Así relataremos algunos ejemplos de actuación del TJUE acerca de incumplimientos relacionados y representativos de estas dificultades.

De acuerdo con el contenido de la Directiva esta debería ser traspuesta "a más tardar al final de un período de tres años a partir de su adopción", plazo al que seguiría un informe de la Comisión al Consejo y al Parlamento para analizar su grado de transposición. Teniendo en cuenta su fecha de publicación y entrada en vigor, la Directiva debería haber estado transpuesta por sus sujetos destinatarios, todos los Estados miembros, el 24 de octubre de 1998.

Incumplimientos que se pueden distinguir, bien por ausencia de transposición, bien por incumplimiento del propio contenido de la Directiva.

Ejemplo de sentencia por recurso por incumplimiento respecto a la no transposición de la Directiva lo tenemos en la Sentencia del Tribunal de Justicia (Sala Primera) de 4 de octubre de 2001 de la Comisión de las Comunidades Europeas contra el Gran Ducado de Luxemburgo, por no adaptación del Derecho interno a la Directiva 95/46/CE (Asunto C-450/00).

También podemos citar, por incumplimiento de contenido, la sentencia del Tribunal de Justicia (Gran Sala) de 9 de marzo de 2010, Comisión Europea contra la República Federal de Alemania (asunto C-518/07).

En este caso no se trataba de un incumplimiento por ausencia de transposición propiamente, sino de un incumplimiento como tal del artículo 28 de la Directiva por adaptación incorrecta de su normativa nacional a la misma. Es de destacar que el tema parte de la tradicional diferenciación en Alemania de la protección de datos en función de su tratamiento público o privado, y la intervención al respecto de las Autoridades independientes de protección de los Lander.[580]

Igualmente por incumplimiento del artículo 28 de la Directiva pero más enfocado en el concepto de independencia de las Autoridades, encontramos la Sentencia del Tribunal de Justicia (Gran Sala) de 16 de octubre de 2012. Comisión Europea contra República de Austria. Asunto C-614/10. Esta vez no tanto por adaptación normativa nacional errónea sino por adopción incompleta de medidas de adaptación para hacer verdaderamente efectiva ese requisito de independencia. Y ello debido a la dependencia funcional y estructural del funcionario encargado de la Autoridad de protección de datos de la Cancillería federal austriaca.

Asimismo, nos fijaremos en la sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Comisión Europea contra Hungría (asunto C-288/12). Otro pronunciamiento de incumplimiento por parte de un Estado y con el artículo 28 (y el Considerando número 62) y las Autoridades nacionales de control como protagonistas. El carácter independiente que debe reunir la Autoridad y, en este caso, con una nueva legislación nacional húngara que pone fin al mandato de la autoridad de control con anterioridad a lo previsto así como el establecimiento de una nueva autoridad de control y el nombramiento de su titular, hacen que la Comisión[581] requiera en 2012 a Hungría por no cumplir los requerimientos de la norma comunitaria.[582]

[580] "…procede declarar que la República Federal de Alemania ha incumplido las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, al someter a la tutela del Estado a las autoridades de control competentes para vigilar en los diferentes Länder el tratamiento de datos personales en el sector no público, y al haber adaptado así incorrectamente su normativa nacional a la exigencia de que dichas autoridades ejerzan sus funciones con «total independencia»".

[581] Exponiendo la Comisión: "al poner fin antes de tiempo al mandato del Supervisor, al no consultar a éste acerca del proyecto de la nueva Ley de protección de datos y al contemplar esta Ley demasiadas

El Tribunal, advirtiendo a Hungría[583] (que aducía la inadmisibilidad del recurso) de la ya reconocida jurisprudencia previa, da la razón a la Comisión que se fija en su demanda en los criterios jurisprudenciales asentados por el propio Tribunal para determinar lo que se entiende por independencia de las Autoridades nacionales de control, que implicaría "una independencia total frente a cualquier influencia directa o indirecta que permite que la autoridad de control de que se trate actúe con total libertad, a resguardo de cualquier tipo de instrucciones y presiones, sin influencia externa y sin riesgo de que se pueda ejercer tal influencia." Y establece que la mera independencia funcional no es garantía de esa independencia. Para terminar dejando claro que "si cada Estado miembro tuviera la posibilidad de poner fin al mandato de una autoridad de control antes de que éste llegue al término inicialmente previsto sin respetar las normas y las garantías establecidas previamente en tal sentido por la legislación aplicable, la amenaza de tal terminación anticipada que en tal caso planearía sobre esa autoridad durante todo su mandato podría generar una forma de obediencia de ésta al poder político incompatible con dicha exigencia de independencia".[584]

---

posibilidades de poner fin al mandato del presidente de la Autoridad, reconociendo atribuciones al Presidente de la República y al Primer Ministro a este respecto..."

[582] Sobre la deriva de Hungría, que fue además una de las primeras en reconocer la independencia de la autoridad de control citaremos a Jóri (2013).
En este sentido ver el proceso incoado por la Comisión sobre el peligro a la independencia de varias instituciones en Hungria (Recuperado el 25 de septiembre de 2018):
http://europa.eu/rapid/press-release_IP-12-24_es.htm

[583] Lo deja claro en el párrafo 32 de la sentencia: "carece de incidencia a este respecto por no guardar relación con la cuestión de si el incumplimiento alegado había o no dejado de producir efectos en la fecha de expiración del plazo fijado en el dictamen motivado, ya que el presente recurso sólo tiene por objeto dilucidar si Hungría ha incumplido las obligaciones que le incumben en virtud de la Directiva 95/46 al poner fin antes de tiempo al mandato del Supervisor."
Y en el párrafo 34: "El hecho invocado por Hungría, según el cual le sería imposible subsanar el incumplimiento alegado sin infringir la Directiva 95/46 o vulnerar el principio de seguridad jurídica, suponiendo que pueda demostrarse, pertenece en cualquier caso al ámbito de la ejecución de la sentencia que declare la existencia del incumplimiento y, por lo tanto, carece de influencia en la admisibilidad del presente recurso".

[584] Párrafos 37, 52 y 54.

1.3. Los Considerandos

Del estudio de los Considerandos que exponen los motivos de creación de tan importante norma podemos extraer algunas conclusiones que sistematizaremos en los siguientes grupos de motivación de los mismos:

- Aquellos basados en las **necesidades propias del mercado interior**, de las actividades económicas de este mercado así como de las necesidades del principio de competencia en el mismo y su desarrollo. Más o menos vinculados se encuentran los Considerandos 3, 4, 5, 7, 8, 19, 20, 40, 61 y 71. Si bien se rigen como el "leit motiv" instrumental para la aprobación de la norma.

- La **integración más estrecha entre los europeos, los derechos humanos y el respeto al derecho europeo, así como las garantías de los mismos** se observan en buena parte de los Considerandos como sustrato sustancial de la justificación de la norma y su desarrollo. Así los Considerandos 1, 2, 9, 10, 11, 12, 15, 23, , del 25 al 30, 33, 38, 39, 41 y del 51 al 60, más relacionados con las garantías, así como los Considerandos 60, 62, 64, 65,70 y 72.

- El bloque de Considerandos en los que se aprecian las **excepciones, limitaciones o alusiones a especificidades de regulación en el derecho de protección** también es significativo en su número y alusión: Considerandos 13, 16, 17, 21, 22, 24, 34, 35, 36, 37, 42, 43, 44,47,48,49, 50, 58, 66, 67, 69 y 68.

- Por último debemos hacer una distinción en los Considerandos basados en las **justificaciones propias del estado de la técnica y del progreso de los tiempos**, que serían: el 6, 14 y 46.

El momento jurídico de aprobación de la Directiva constituye un tiempo muy diferente al actual, y sus premisas de aprobación diferían de las otorgadas actualmente, tanto por el Tratado de Lisboa como por la Carta de Derechos Fundamentales, que dieron base jurídica de protección europea directa al derecho de protección de datos de los europeos.

Su base jurídica se encontraba en el Artículo 100 A del Tratado constitutivo de la Comunidad Europea.[585]

En ese inicio nos encontramos con el antiguo sistema de pilares propios del Espacio de Libertad, Seguridad y Justicia, y con la justificación legislativa de aproximar legislaciones nacionales (de ahí su carácter de directiva). Así, la Directiva estaría ubicada en el antiguo primer pilar comunitario (Derecho comunitario, en este caso por afectar al mercado interior), dejando fuera los datos tratados en la órbita del segundo y tercer pilar (Política Exterior y de Seguridad Común y Cooperación Policial y Judicial), que estarían excluidos de su regulación.

Además, ese momento de oportunidad aclaratoria se manifiesta en la aprobación de leyes previas nacionales en Europa con ánimo de cumplimiento del Convenio o Protocolo 108 del Consejo de Europa al que nos hemos referido anteriormente.

Esa doble motivación, de aproximación y armonización, fue el motor jurídico principal para la aprobación de la que vendría a ser, para las siguientes dos décadas, la principal norma de protección de datos en Europa, fuente de emanación marco de las subsiguientes leyes nacionales de los Estados miembros de la Unión, y referente internacional como norma de protección de datos.

Es, por ello, que la Directiva aúna en su motivación la protección del derecho fundamental de la protección de datos en Europa y el aseguramiento de la libre circulación en el mercado interior e imbrica entre los dos su seguridad jurídica. Crea e inicia así, lo que podríamos denominar el "espacio de privacidad europea". Aproxima, asimismo, las legislaciones de protección del derecho en Europa, y armoniza el mercado común, dotándolo de la seguridad jurídica necesaria en el tratamiento de los datos a ese nivel.

[585] Ubicado en su Titulo V, Capitulo 3 "Aproximación de las legislaciones".

1.4. Objeto de la Directiva.

En el artículo 1 se nos presenta que el objeto de la Directiva es la protección de la intimidad, si bien concretada a través de la protección de los datos personales de las personas físicas. Se considera el derecho de un nivel superior hacia su concreción en uno más específico pero ubicado dentro de la generalidad de su protección en la esfera de la intimidad, quizá precisamente por la conexión de los datos personales con la necesidad de protección de los derechos fundamentales de la persona y de su dignidad como tal.

Así se conceptúa la protección que se encarga a los Estados como un todo para la defensa de las libertades (vinculadas a las derivadas de la Unión), y los Derechos Fundamentales: "los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales." Aquí podemos ver cómo, al inicio del camino jurídico de la protección de datos europea, su contenido autónomo y desgajado en el derecho derivado, se encontraba algo diluido todavía bajo el peso del general derecho a la intimidad.

Esa protección de derechos no se podrá utilizar en un sentido económicamente proteccionista, ya que según el artículo 1.2 "los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1" (Heredero Higueras, 1997, 70)[586]

Autores como Guerrero Picó (2005) vinculan directamente la finalidad de la aprobación de la Directiva, tal y como refleja su primer artículo, a las exigencias del mercado interior y el levantamiento de una de sus trabas, dejando el derecho a la protección de

[586] Siguiendo, como nos apunta Heredero Higueras, el Dictamen del Consejo Económico y Social que aconsejaba no limitar el objeto de la Directiva a la protección de la Intimidad, como el CEDH. Igualmente el Servicio Jurídico del Consejo se manifestó en Dictamen 8987/91 JUR 103, acerca de que el objeto de la Directiva era facilitar la libre circulación de los datos personales y eliminar los obstáculos de la disparidad de las legislaciones.

los datos de los europeos en su mejora, como un efecto subsiguiente y relacionado a esa primera motivación.[587]

1.5. Ámbito de aplicación

La Directiva se aplica, según su artículo 3, a todo "tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

El tratamiento "efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal", está fuera del ámbito de la Directiva. Al igual que aquel "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas."

Así podremos destacar, a modo de resumen, que:

La Directiva va dirigida a la regulación del tratamiento de los datos de las personas físicas (y no las jurídicas) identificadas e identificables, por cualquier medio. Y ello constituye el núcleo explicatorio del concepto de datos personales.

El tratamiento de los datos implica cualquier operación automatizada o no, sobre esos datos. Y relacionado con ello estaría el concepto de fichero referido a la ordenación estructural de esas operaciones y tratamiento.

[587] Así nos lo expresa (2005, 298): "es, pues, una herramienta para impedir las trabas a la libre circulación de información personal en el contexto del mercado interior; el modo de evitar que la defensa de los derechos fundamentales se torne en freno para los objetivos de la integración económica, eludiendo por demás el inconveniente de que dicha tutela sea argüida por las Administraciones nacionales para falsear la competencia e incumplir los cometidos que les atribuye el Derecho comunitario. No es, como el Convenio número 108 del Consejo de Europa, un instrumento orientado directamente a la protección de los derechos de las personas, si bien es evidente que indirectamente conseguirá el objetivo menos crematístico de asegurar un elevado nivel de protección de la vida privada en la esfera comunitaria..."

El Asunto Österreichischer Rundfunk se nos presenta como una importante interpretación sobre la aplicabilidad de la Directiva, y se sustancia en la sentencia del Tribunal de Justicia de 20 de mayo de 2003 en el asunto Rechnungshof (C-465/00) contra Österreichischer Rundfunk y otros y Christa Neukomm (C-138/01) y Joseph Lauermann (C-139/01) contra Österreichischer Rundfunk. Que sustancia además las siguientes peticiones de decisión prejudicial: Verfassungsgerichtshof (C-465/00) y Oberster Gerichtshof (C-138/01 y C-139/01).[588]

El caso afecta a la divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof (Tribunal de Cuentas austriaco), ya que según Ley federal constitucional sobre la limitación de la retribución de funcionarios públicos, se obligaba a estas entidades a comunicar determinadas retribuciones (que pasaran de un umbral) de sus empleados públicos a ese Tribunal de Cuentas; y ello en contestación al Verfassungsgerichtshof (Tribunal Constitucional) que plantea la pregunta al Tribunal de Justicia de la Unión Europea.

Las preguntas del Constitucional austriaco, que ya dudaba de que estas injerencias en la vida privada pudieran afectar "al bienestar general del país" (principal justificación que se desprendía de la Ley para estas comunicaciones de datos) son claras:

"1) ¿Deben interpretarse las disposiciones de Derecho comunitario, en particular aquellas relativas a la protección de datos, en el sentido de que se oponen a una normativa nacional que obliga a un organismo estatal a recoger y comunicar datos sobre ingresos con el fin de publicar los nombres y los ingresos de empleados de:

a) un ente territorial,

b) un organismo de radiodifusión de Derecho público,

c) un banco central nacional,

d) un organismo de representación de intereses profesionales establecido por ley,

e) una empresa gestionada con ánimo de lucro parcialmente bajo influencia del Estado?

[588] Asuntos acumulados C-465/00, C-138/01 y C-139/01. Mediante Auto de 17 de mayo de 2001 el Presidente del Tribunal ordena la acumulación de los asuntos C-465/00 C-138/01 y C- 139/01, implicando así otro caso con el Gobierno austriaco además de con el Italiano (si bien presentaron observaciones además los Gobiernos danés, neerlandés, finlandés, sueco y británico).

2) En caso de que el Tribunal de Justicia de las Comunidades Europeas respondiese en sentido afirmativo, al menos parcialmente, a la cuestión que se plantea:

Las disposiciones que se oponen a una normativa nacional como la descrita, ¿son directamente aplicables en el sentido de que las personas obligadas a revelar datos pueden invocarlas para evitar la aplicación de normas nacionales contrarias a ellas?"

Ya en la sentencia el Tribunal justifica la plena aplicabilidad de la Directiva, pero no fundando el título jurídico para ello en la defensa de los Derechos Fundamentales, sino interpretando y dejando claro el objetivo real de la misma, cual es la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros, y confirmando, hermenéuticamente, ese objetivo principal de su redacción, que ya apuntábamos, en el mercado interior y su defensa. Percepción jurídica de aplicabilidad en contra del criterio mostrado en sus conclusiones generales por el Abogado General Antonio Tizzano presentadas el 14 de noviembre de 2002. Conclusiones que tienen, no obstante, mucho interés, ya que apuntan, como nos advierte De Miguel Sánchez (2006, 324), la desvinculación entre derecho a la intimidad y protección de datos en la doctrina del Tribunal de Justicia, que "adquiere una evidencia fuera de toda duda en las Conclusiones del Abogado General Sr. Antonio Tizzano".

Para pasar a responder e interpretar ya concretamente el asunto y la Directiva en su aplicación, considerando en primer lugar que nos encontramos ante datos personales ya que se trata de "información sobre una persona física identificada o identificable", e indicando los preceptos que analiza para su respuesta (artículos 6, apartado 1, letra c), 7, letras c) y e), y 13 de la Directiva y artículo 8 del CEDH) sobre si ha habido injerencia o no (que determina en sentido positivo), en la vida privada o si se encuentra ésta justificada por razones de excepción de interés público.[589]

[589] Según párrafo 75: "Para demostrar la existencia de tal injerencia, carece de relevancia que los datos comunicados tengan o no carácter sensible o que los interesados hayan sufrido o no eventuales inconvenientes en razón de tal injerencia (…) Basta con observar que el empleador ha comunicado a un tercero los datos relativos a los ingresos que percibe un trabajador o un pensionista".

Y continúa para analizar si esa injerencia está justificada, dentro de la clausula del CEDH que opera en su artículo 8, que no estaría justificada "salvo que, «prevista por la ley», persiga uno o varios de los objetivos legítimos contemplados en el apartado 2 de esta disposición y, «en una sociedad democrática, sea necesaria» para alcanzar tal o tales objetivos" (párrafo 76). Remitiéndose directamente a la Jurisprudencia del TEDH (ejemplo claro del poder judicial multinivel europeo en materia de protección de derechos humanos) y recordando el acervo jurisprudencial del mismo en su interpretación, que debe reunir "el adjetivo «necesario», a los efectos del artículo 8, apartado 2, del CEDH, implica que esté en cuestión «una necesidad social imperiosa» y que la medida adoptada sea «proporcionada a la finalidad legítima perseguida»" (párrafo 83 de la sentencia)[590]

Así, llega a su determinación el Tribunal, si bien ponderando el interés que ha perseguido el Gobierno austriaco en su justificación, en su afán de transparencia para con la utilización de los fondos y retribuciones públicas, a "la cuestión de si la indicación del nombre de las personas afectadas junto con los ingresos que perciben es proporcionada a la finalidad legítima perseguida y si los motivos invocados ante el Tribunal de Justicia para justificar tal divulgación resultan pertinentes y suficientes"; siendo esa injerencia derivada de la norma nacional únicamente justificada según el artículo 8.2 del CEDH, "en la medida en que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por entidades sujetas al control del Rechnungshof, sino también de los nombres de los beneficiarios de dichos ingresos, sea a la vez necesaria y apropiada para lograr el objetivo de mantener los salarios dentro de unos límites razonables, extremo que ha de ser examinado por los órganos jurisdiccionales remitentes." Es decir, deja en manos de los Tribunales nacionales respectivos esa apreciación de fondo.[591]

Además establece que determinados preceptos de la Directiva son suficientemente precisos para ser invocados directamente por los particulares, y aplicables por los tribunales.[592]

[590] Concretamente, sentencia TEDH Rekvényi c. Hungría de 20 de mayo de 1999. Y sentencias del TEDH Gillow c. Reino Unido de 24 de noviembre de 1986 y Leander c. Suecia de 26 de marzo de 1987.
[591] Párrafos 86 y 90 de la sentencia. Elemento que se repite recurrentemente en los pronunciamientos del TJUE estudiados, por su labor de interpretación del sentido de la Directiva y no del fondo del asunto.
[592] Así según el párrafo 100 "los artículos 6, apartado 1, letra c), y 7, letras c) y e), enuncian (...) obligaciones incondicionales".

2. El marco de las comunicaciones electrónicas

Las comunicaciones electrónicas gozan de una regulación normativa propia independiente (pero vinculada) de la común de protección de datos en Europa, si bien se les aplica también ésta con carácter general. Hemos de ver aquí una tendencia también europea, a la especialización por determinados ámbitos (al igual que ocurre en la protección de la privacidad en las instituciones europeas o en los procesos de persecución penal), que recuerdan a la fragmentación propia del ámbito de protección estadounidense, que, sin embargo, y por efecto de atracción europea ha hecho esfuerzos de homogeneización en la protección de la privacidad en los últimos años. Hemos de decir que esa fragmentación se encuentra más justificada en la versión europea, por la especialidad propia de la materia en cuestión, algo que en la regulación americana no sucede, ya que es allí por norma general, y al revés, que cada materia tenga su apartado (como otros) de regulación para la protección de datos afectada. Sin olvidar que el marco de referencia general sigue operando como elemento supletorio y de remisión.

Debemos apuntar aquí este paquete normativo como hito importante en el camino del Derecho Derivado europeo en la materia, aún especial, relacionada con la protección de datos.

El marco de las comunicaciones electrónicas está formado por un conjunto normativo con especialidades de protección propias de ese ámbito. El cuerpo normativo está integrado por las siguientes normas (principalmente Directivas) empezando por la que otorga precisamente ese "marco":

-Directiva 2002/21/CE "Directiva marco";

-Directiva 2002/19/CE "Directiva de acceso";

-Directiva 2002/20/CE "Directiva de autorización";

-Directiva 2002/22/CE "Directiva de servicio universal";

-Directiva 2002/58/CE "Directiva sobre la privacidad y las comunicaciones electrónicas";[593]

- Reglamento (CE) no 1211/2009 por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE);

-Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles.[594]

2.1 Directiva marco

Se encarga de regular el marco armonizado de "los servicios de comunicaciones electrónicas, las redes de comunicaciones electrónicas y los recursos y servicios asociados"[595] y "fija misiones de las autoridades nacionales de reglamentación" dando una definición al efecto, que ocupa el amplio espectro de las comunicaciones por

[593] Las Directivas son:
Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco); Directiva 2002/19/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso); Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización); Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal); 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). Estas dos últimas modificadas por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores. Y la Directiva Marco, la de acceso y la de autorización que se modifican a su vez por la Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas
[594] Los Reglamentos son:
Reglamento (CE) nº 1211/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Oficina y; Reglamento (UE) nº 531/2012 del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión.
[595] Artículo 1.

"señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada".[596][597]

El otro gran aspecto de esta Directiva es la articulación y encargo de su cometido a través de las "Autoridades nacionales de reglamentación",[598] que también se ocuparán de las misiones asignadas por el resto de Directivas. Vemos aquí como la misión de supervisión y regulación sobre las entidades y empresas suministradoras de redes, equipos o servicios de este tipo pasan por las distintas autoridades nacionales, que se convierten en protagonistas de su ejecución. Estas Autoridades guiarán su actuación con el principio del derecho al recurso de la autoridad independiente a facilitar a "cualquier usuario o empresa suministradora de redes o servicios de comunicaciones electrónicas"[599]afectados, el principio de respeto y ejercicio efectivo del derecho al suministro de información y al principio de transparencia y consulta. Sin perder de vista el objetivo de armonización de la Directiva cual es (al igual que en la de protección de datos de 1995), el mercado común y su desarrollo. Y ello, vinculado al fomento de la competencia para velar por el "máximo beneficio en cuanto a posibilidades de elección, precio y calidad"[600], "suprimiendo los obstáculos" y "fomentando el establecimiento y desarrollo de las redes transeuropeas" y su desarrollo, vinculándolo a las garantías y promoción de los intereses de los ciudadanos de la Unión Europea. Además de garantizar el acceso al servicio universal de las comunicaciones, su integridad y seguridad y la información clara sobre las mismas; se procura "garantizar un alto nivel de protección de los datos personales y de la intimidad".[601][602]

[596] Artículo 2 letra a)
[597] En la sentencia del TJUE de 22 de diciembre de 2016 Fjarskipti hf. contra la Administración Islandesa de Correos y Telecomunicaciones (asunto E-6/16) se interpretan las definiciones y conceptos de red, red pública, y servicios de comunicaciones electrónicas de su artículo 2.
[598] Artículo 3
[599] Artículos 4 a 6
[600] Artículo 8.3
[601] Artículo 8.4
[602] Ver la *Electronic Communications Privacy Act* estadounidense tratada en este trabajo.

2.2 Directiva acceso

Regula el "acceso a las redes de comunicaciones electrónicas y recursos asociados, y su interconexión"[603]para establecer un marco regulador de las relaciones entre los suministradores de redes y servicios con la armonización del mercado común, también como objetivo, y velando por la no restricción de los servicios y su libre competencia, implicando obligaciones de transparencia y de no discriminación. En esta Directiva no observamos elementos de derivación o alusión a la protección de datos, siendo, dentro del paquete de telecomunicaciones, la Directiva de mayor orientación a la regulación del mercado.

2.3 Directiva autorización

En este caso se pone el foco en la autorización de los servicios y redes de comunicaciones electrónicas con un ánimo liberalizador, que es el espíritu que recorre el "paquete de telecomunicaciones", con la exigencia de una reglamentación mínima y la existencia de una autorización general o genérica que evite trabas de todo tipo.

En el sentido que nos interesa diremos que uno de los condicionantes que pueden imponerse para poder disponer de este tipo de autorización general y disfrutar de su aprobación (de los que enumera el anexo de la Directiva), está en el de la "Protección de los datos personales y la intimidad específica del sector de las comunicaciones electrónicas de conformidad con la 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"[604]

[603] Artículo 1.
[604] En su punto 7. Mención a una Directiva derogada que debemos entender ya referida a la Directiva sobre la privacidad y las comunicaciones electrónicas de 2002 que veremos más adelante.

2.4 Directiva servicio universal

Esta Directiva pretende garantizar unos determinados servicios obligatorios y derechos del usuario, dentro del concepto de servicio universal de comunicaciones electrónicas, quizá ante ese ánimo liberalizador del paquete de telecomunicaciones, que garantice una determinada calidad y precio asequible, y una red pública de comunicaciones electrónicas y su conexión, con especial atención a los consumidores discapacitados o con rentas bajas.

Dentro de los derechos que se garantizan podemos destacar el de la portabilidad del número de móvil, que podríamos verlo como antecedente del de portabilidad de datos, o el de los ya conocidos teléfonos gratuitos de emergencia en toda Europa ("el 112"), o el fomento de números de asistencia social con ánimo armonizante ("el 116").

En lo que a la privacidad respecta destacaremos la concreción dentro del Anexo I que establece servicios a observar por los suministradores, el de la "prohibición selectiva gratuita de llamadas salientes o de MMS o SMS, o, cuando sea técnicamente factible, de otras formas de aplicaciones similares, de tarificación adicional", que "es la facilidad en virtud de la cual el abonado puede suprimir de manera gratuita llamadas salientes o MMS o SMS, u otras formas de aplicaciones similares, de tarificación adicional de tipos definidos o dirigidas a tipos de números definidos, previa solicitud al operador designado que proporciona servicios telefónicos."[605]

2.5 Directiva sobre la privacidad y las comunicaciones electrónicas

Nos encontramos ante la Directiva específica en el paquete de telecomunicaciones que se encarga de la privacidad y la protección de datos en el ámbito de las comunicaciones electrónicas en Europa, abarcando las redes de Internet y de la telefonía móvil y fija. La Directiva fija su atención ya directamente en el respeto a los derechos fundamentales, en lo que será un anticipo del camino que seguirá el paquete de privacidad desde la

[605] Letra b del Anexo 1.

Directiva del 95, (más preocupada por el mercado) hacia el Reglamento de 2016, con mayor enfoque en la protección de derechos. Marca además su relación de complementariedad con la Directiva de 1995, relevo de esa armoniosa convivencia legal que ha sido retomado por el Reglamento.[606]

Dentro de las definiciones del artículo 2 nos parecen interesantes las aportaciones dadas con la Directiva de modificación de 2009, que, en una labor de seguimiento del avance tecnológico, nos presenta una mejorada redacción de lo que se entiende por "datos de localización", o añade la definitoria de "violación de los datos personales" en este ámbito. Como también hace con la de "violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad."[607]

Además de renovar la redacción en cuanto a la seguridad del tratamiento ofrecida por la Directiva. Así, nos dice, que, además de las "medidas técnicas y de gestión adecuadas", se abunda en un artículo 4.1bis estableciendo la obligación a los proveedores de que "como mínimo:

[606] Así el Considerando 2 de la Directiva: "La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta." Y concretamente su artículo 1 deja claro su ámbito de regulación en la "...la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas..."
Y el Considerando 10: "En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público." y el Considerando 173 del Reglamento "El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo".

[607] Artículo 2 letras c y h.
En este sentido debemos apuntar el Reglamento de ejecución que regula las notificaciones en estos casos: 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 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

-garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley,

-protegerán los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, y

-garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales." Y añadiendo una regulación más detallada para el caso de violación de datos personales."[608]

Además, la modificación de 2009 nos puede servir como ejemplo legislativo de aplicación del principio de rendición de cuentas. De conformidad con el artículo 4[609] ya modificado, la Directiva impone una obligación de aplicar una política de seguridad, en concreto. Por tanto, como dice el Manual de la Agencia de Derechos Fundamentales y el Consejo de Europa (2014, 84): "en lo que atañe a las disposiciones de seguridad de la Directiva, el legislador decidió que era necesario introducir un requisito expreso de contar con una política de seguridad y de aplicarla."

Es el artículo 5 el que, con carácter general, prevé la confidencialidad de las comunicaciones y de sus datos de tráfico. Prohibe en particular "la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo..."[610] Y vela por qué "únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho

[608] Artículo 4.1
Añadiendo al artículo 4 los apartados 3 a 5, con especial mención a la labor de la ENISA en este cometido.
[609] Nos lo dice así: "garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales".
[610] Artículo 5.1

abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento..."[611][612]

El artículo 6 nos dice con carácter general que los "datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación." Así como en el artículo 9 que para los datos de localización nos dice que "...sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados..."

El desvío automático de llamadas o las guías de abonados también reciben atención por la Directiva que permite un mayor control de los usuarios sobre los mismos. Y establece el consentimiento previo como requisito necesario para "la utilización de sistemas de llamada automática y comunicación sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa..."[613] si bien fuera de esos supuestos se deja a las legislaciones nacionales un margen de maniobra para garantizar que no se permitan "bien sin el consentimiento del abonado o el usuario, bien respecto de los abonados o los usuarios que no deseen recibir dichas comunicaciones"[614]. Prohibiéndose los mensajes ocultos en este ámbito.[615][616]

[611] Artículo 5.3 tras modificación operada en 2009, que resulta de mucha utilidad para el usuario en la evitación de lo que se denominan "cookies" y su rastreo.

[612] Podremos distinguir en tres las categorías de datos generados en las comunicaciones, siguiendo (ADFUE/CoE, 2014, 184): "los datos que constituyen el contenido de los mensajes enviados durante la comunicación; estos datos son estrictamente confidenciales; los datos necesarios para establecer y mantener la comunicación, denominados datos de tráfico, tales como la información sobre los interlocutores, tiempo y duración de la comunicación; dentro de los datos de tráfico, existen datos que hacen especial referencia a la localización del dispositivo de comunicación, denominados datos de localización…"

[613] Artículos 11 y 12.

[614] Artículo 13.

[615] Artículo 13.3 que continua "La elección entre estas dos posibilidades será determinada por la legislación nacional, teniendo en cuenta que ambas opciones deben ser gratuitas para el abonado o usuario."

El artículo 13.4: "Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente..." El artículo 13 es un artículo importante porque en él se sustancia la evitación del conocido como "Spam" en Europa.

Por lo tanto, podríamos resumir las principales características de la norma en la preponderancia que toma la figura del consentimiento y su exigencia, al igual que la importancia en la regulación de la protección de los datos del usuario ante la pérdida o accidente de seguridad junto con cualquier tratamiento ilícito, con especial atención a las políticas de seguridad del proveedor. De igual manera se hace hincapié en la obligación de los Estados miembros de velar por la confidencialidad de las comunicaciones y transmisiones electrónicas de sus ciudadanos.

Como buena ley de privacidad debemos recordar su limitación de aplicación, que sigue de cerca la de la Directiva del 95 y de las leyes de protección de datos en general, y que se sustancia, principalmente, "cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos..."[617]

2.6 La fallida Directiva sobre conservación de datos

La 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 en comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, que venimos analizando, nos sirve de ejemplo de la importancia de la protección de datos en el entorno de las comunicaciones electrónicas; además de servir, con su anulación, de ejemplo añadido sobre la demostración de la fuerza configuradora del TJUE en la protección de datos en la Unión.

La Directiva, que fue declarada inválida el 8 de abril de 2014, obligaba a los prestadores de servicios de comunicaciones electrónicas a mantener disponibles los ya vistos datos

Las modificaciones realizadas en la Directiva sobre la privacidad en las comunicaciones electrónicas en 2009 introdujeron ampliaciones de protección en el artículo 13 principalmente.

[616] Ver (Grupo del artículo 29, 2012)

[617] Artículo 15

de tráfico, con la finalidad de persecución de delitos graves, por un tiempo mínimo de seis meses hasta dos años, independientemente de la necesidad del prestador del servicio para su facturación o suministro del mismo.

Así, en la sentencia *Digital Rights Ireland Ltd* de 8 de abril de 2014, motivada por sendas peticiones de decisión prejudicial planteadas por la High Court de Irlanda y el Verfassungsgerichtshof de Austria, el TJUE va a considerar lo contenido en la Directiva como una injerencia "en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta", que "resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante (…) que sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta..."[618]

Este pronunciamiento del TJUE, junto con la sentencia Schrems, que veremos más adelante, marcan dos hitos en el derecho a la protección de datos, particularmente en lo que respecta a la relación transatlántica del mismo, entre Estados Unidos y la UE. Dejaremos apuntado aquí, junto con López Aguilar (2017) la importancia del TJUE en la efectiva construcción de ese constitucionalismo en la protección de datos europea.

2.7 Los Reglamentos

Los dos siguientes Reglamentos no tienen una incidencia regulatoria específica sobre protección de datos, si bien dentro del marco de regulación de comunicaciones electrónicas, nos parece oportuna su reseña, ya que se encargan de perfilar la estructura

[618] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros (Asuntos acumulados C-293/12 y C-594/12)

institucional que dará soporte a lo establecido en la regulación de esas comunicaciones electrónicas en el ámbito europeo.

El Reglamento (CE) no 1211/2009 por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), se encarga de la creación y construcción regulada de este organismo y de sus vinculaciones de coordinación con las autoridades reguladoras nacionales. Cuenta con las funciones propias de un organismo regulador de asesoramiento, emisión de recomendaciones y dictámenes, establecer buenas prácticas, fomentar la correcta reglamentación del sector etcétera. También se prevé un Consejo de Reguladores formado por el Organismo y las autoridades de regulación nacionales, una oficina de asistencia y un grupo de trabajo de expertos consultivo.

El Reglamento (UE) 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles, así como el Reglamento (CE) 717/2007 del Parlamento Europeo y del Consejo, de 27 de junio de 2007, relativo a la itinerancia en las redes públicas de telefonía móvil en la Comunidad y por el que se modifica la Directiva 2002/21/CE, fijan legalmente la aplicación efectiva de lo que se ha conocido como el fin del “roaming”, y se encargan de evitarles a los usuarios los precios excesivos en sus comunicaciones (llamadas, mensajes de texto o acceso a internet) cuando se desplacen por la Unión.

3. La protección de datos en las Instituciones Europeas. El Reglamento 45/2001.

Es posible que, con el Reglamento del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y los Organismos Comunitarios y a la libre circulación de estos datos, nos encontremos ante el primer intento (y consecución) de regulación integral plena, y sin mayor intervención nacional, de la protección de datos en la Unión. Y ello debido a la competencia propia de regulación de sus propias instituciones, y que la podría convertir en un anticipo, al menos de tipo formal, al Reglamento de 2016, con efectos frente a todos y sin mayor necesidad de desarrollo por los Estados miembros.

El Reglamento tiene como base el antiguo 286[619] del Tratado de la Comunidad Europa (y hoy en correspondencia con el artículo 16 del TFUE), y establece un sistema de protección de datos a nivel institucional comunitario, creando además el Supervisor Europeo de Protección de Datos para su control.

3.1 Objeto y Principios

Ya en su considerando 13 dejaba claro su objetivo la Norma: "Se trata de garantizar tanto el respeto efectivo de las normas de protección de los derechos y las libertades fundamentales de las personas como la libre circulación de los datos personales entre los Estados miembros y las instituciones y organismos comunitarios, o entre las instituciones y los organismos comunitarios, en el ejercicio de sus competencias respectivas." Y limita el Reglamento su ámbito "al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho

[619] Recordémoslo: "1. A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo.
2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes."

tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario"[620]

El Capítulo II va recogiendo los principios de la protección de datos que ya se preveían en la Directiva 95/46/CE, y que tienen su origen como vimos en el Convenio 108 del Consejo de Europa.

Así, se contemplan los principios de calidad de datos, que deberán tratarse de manera leal y lícita, para fines determinados, explícitos y legítimos, que sean datos adecuados, pertinentes y no excesivos, exactos y de conservación adecuada a sus fines. Reflejándose igualmente el principio de licitud del tratamiento, y regulándose la transmisión de los datos personales entre las instituciones o los organismos comunitarios o en el seno de dichas instituciones y organismos y la transmisión de datos personales a destinatarios; distintos de las instituciones y los organismos comunitarios, en este caso ya sí sujetas a la Directiva 95/46/CE. También, al igual que lo previsto en la Directiva para flujos extracomunitarios, se prevé la transmisión no sujeta a la Directiva 95/46/CE "cuando se garantice un nivel de protección suficiente en el país del destinatario o en la organización internacional destinataria, y los datos se transmitan exclusivamente para permitir el ejercicio de las tareas", y que son competencia del responsable del tratamiento.[621]

En el Reglamento también se prevén, al igual que en la Directiva, categorías especiales de datos ("origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.") así como la obligación de suministro de información al interesado cuando los datos hayan sido o no hayan sido recabados del propio interesado.[622]

[620] Artículo 3.1
[621] Artículos 4,5,7, 8 y 9.1
[622] Artículos 10,11 y 12

3.2 Derechos y Responsable del Tratamiento.

Igualmente se contemplan en el Reglamento los derechos ARCO (acceso, rectificación, cancelación y oposición)[623], con ligeras variaciones de denominación y alcance, como el caso del derecho al "bloqueo" del artículo 15, que parece un derecho de rectificación cualificado, motivado por las especiales condiciones tecnificadas de la relación con las instituciones. Las excepciones y limitaciones, en cambio, siguen el curso habitual de su justificación en razones de seguridad y orden público, con la persecución de la infracción penal como estandarte. Además de la protección del interesado o de los derechos y libertades de terceros o por razones de misión del poder público. Un condicionante importante en estas limitaciones se encuentra además en "la salvaguardia de un interés económico o financiero importante de un Estado miembro o de las Comunidades Europeas".[624]

Los principios de confidencialidad y seguridad del tratamiento y la diferenciación entre el responsable y el encargado del tratamiento también tienen cabida en el Reglamento. Fija de manera más pormenorizada el nombramiento y las funciones de los responsables de la protección de datos en el ámbito de cada institución y organismo comunitario, y que parece el antecedente más idéntico al delegado de protección de datos del Reglamento de 2016, al cual deberá notificar, el responsable del tratamiento, las operaciones de tratamiento "para un objetivo único o para varios objetivos relacionados entre sí".[625]

Para lo cual se extiende el artículo 24. Esta figura y sus funciones se desarrolla además en la Decisión de la Comisión 2008/597/CE, de 3 de junio de 2008, por la que se adoptan disposiciones de aplicación relativas al Responsable de la Protección de Datos de conformidad con el artículo 24, apartado 8, del Reglamento (CE) no 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.[626]

[623] Artículos 13 a 19
[624] Artículo 20
[625] Artículos 21, 22 y 23
[626] Artículo 25

De importante relevancia es la previsión de los controles previos a llevar por el Supervisor Europeo de Protección de Datos (SEPD) para los "tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance u objetivos". Sobre los mismos el SEPD emitirá dictamen en un plazo de 2 meses, y en caso de apreciar que el tratamiento pudiera constituir incumplimientos del Reglamento podrá adoptar medidas para impedir esa violación.[627]

Además se prevén las vías jurisdiccionales de recurso ante el TJUE y las reclamaciones administrativas ante el SEPD, que tendrá 6 meses para responder, siendo su silencio negativo. Igualmente se prevé una vía de recurso exclusiva para los empleados de las instituciones y organismos europeos.[628] Asimismo se establece todo un capítulo normativo para atender la regulación del tratamiento de datos personales en relación con la utilización de las redes internas de las instituciones y organismos.[629]

3.3 El Supervisor Europeo de Protección de Datos

El Reglamento se encarga también de la importante creación de la institución del Supervisor Europeo de Protección de Datos (SEPD),[630] como autoridad independiente, que "velará por qué los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios" (artículo 41); y que será nombrado de común acuerdo por el Parlamento Europeo y el Consejo sobre la base de una lista elaborada por la Comisión como resultado de una convocatoria pública de candidaturas (entre personas

---

[627] Artículo 27.
Establece una presunción de tales riesgos el apartado 2 del 27 en: "a) los tratamientos de datos relativos a la salud y los tratamientos de datos relativos a sospechas, infracciones, condenas penales o medidas de seguridad;
b) los tratamientos destinados a evaluar aspectos de la personalidad del interesado, como su competencia, rendimiento o conducta;
c) los tratamientos que permitan interconexiones entre datos tratados para fines diferentes, que no estén previstas en virtud de la legislación nacional o comunitaria;
d) los tratamientos destinados a excluir a personas de un derecho, una prestación o un contrato."
[628] Artículos 32 y 33
[629] Capítulo IV que ocupa los artículos 34 a 40
[630] Capítulo V que abarca los artículos 41 a 48
Pareciendo aquí también pionero en la dotación de independencia con claridad y desde el principio a la autoridad de protección.

cuya independencia esté fuera de toda duda y que posean una experiencia y competencia notorias) y para un mandato renovable de 5 años (artículo 42).[631]

Sus funciones se destacan en dos categorías principales: las de investigación y supervisión y en las de asesoramiento. Junto a ellas destacaremos su deber de colaboración. Igualmente se establecen importantes competencias como la posibilidad de imponer prohibiciones de tratamiento o someter los asuntos a las instituciones comunitarias. Deberá remitir un informe anual de actividad de carácter público al Parlamento Europeo, al Consejo y a la Comisión[632]

Por último, debemos destacar la reforma pendiente de la norma europea con la nueva propuesta de modificación de este Reglamento presentada por la Comisión, a raíz, entre otras cuestiones, de su necesario acompasamiento con el Reglamento General.[633][634]

3.4 Transparencia pública y protección de datos. La sentencia Bavarian Lager.

En relación con el Reglamento de 45/2001 encontramos la tensión jurídica entre la transparencia pública y sus normas de desarrollo y la legislación en materia de protección de datos.[635]

---

[631] Ver Decisión nº 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos. Así como la Decisión del Supervisor Europeo de Protección de Datos de 17 de diciembre de 2012 relativa a la adopción del Reglamento interno (2013/504/UE)

[632] Artículos 46, 47 y 48

En su página web podemos acceder a estos y otros informes, destacando el carácter transparente del organismo (Recuperada el 25 de agosto de 2018): https://edps.europa.eu/annual-reports_en

[633] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE . (Recuperada el 25 de agosto de 2018): https://ec.europa.eu/transparency/regdoc/rep/1/2017/ES/COM-2017-8-F1-ES-MAIN-PART-1.PDF

[634] Como ejemplo de desarrollo del Reglamento por parte de una Institución citaremos la Decisión del Consejo de 13 de septiembre de 2004 por la que se adoptan las normas de desarrollo del Reglamento (CE) no 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (2004/644/CE).

[635] En este sentido es de utilidad tener en cuenta algunos pronunciamientos provenientes del Consejo de Europa como el Convenio 205 (Consejo de Europa, Convenio sobre el Acceso a los Documentos Públicos, CETS nº 205, de 18 de junio de 2009. El Convenio aún no ha entrado en vigor.), previamente inspirado por los principios de la recomendación de de 21 de febrero de 2002 del Comité de Ministros del Consejo

En la sentencia Bavarian lager se define y perfila la protección de los datos en el contexto del acceso a los documentos de las instituciones de la UE teniendo como base la relación entre el Reglamento 1049/2001 (Reglamento de acceso a los documentos) y el Reglamento 45/2001 (Reglamento de protección de datos en las instituciones europeas).[636]

Bavarian Lager, es una empresa importadora de cerveza alemana a Reino Unido, que se ve con problemas en su distribución debido a que la Ley británica favorecía a los productores de cerveza de las islas, obligando a la Comisión a actuar debido al incumplimiento del derecho europeo. Bavarian Lager pide así parte del expediente que le venía afectando y del que era interesada directa a la Comisión, y más concretamente una copia de acta de una reunión a la que habían asistido representantes de la Comisión, las autoridades británicas y la Confédération des Brasseurs du Marché Commun (CBMC). La Comisión acuerda difundir documentos relacionados con esa reunión, si bien no da la información de cinco nombres que aparecían en el acta: dos se habían opuesto de manera expresa su identidad se revelara y los otros tres no pudieron ser contactados.

Con una Decisión de 18 de marzo de 2004, la Comisión desestima una nueva solicitud presentada por Bavarian Lager con objeto de obtener el acta completa, con alusión a la protección de la vida privada de esas personas.

Y es ahí cuando se interpone el conflicto jurídico ante el Tribunal de Primera Instancia, por parte Bavarian Lager[637], que anula esa decisión de la Comisión en sentencia de 8 de noviembre de 2007, al no apreciar perjuicio ni peligro para la vida privada de esas personas con la inclusión de sus nombres.

---

de Europa (Recomendación Rec(2002) a los Estados miembros sobre el acceso a los documentos oficiales). Siendo el equivalente al Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

[636] Sentencia del TJUE, Comisión Europea contra The Bavarian Lager Co. Ltd., de 29 de junio de 2010, (Asunto C-28/08) (apdos. 60, 63, 76, 78 y 79) sobre el Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión

[637] Asunto T-194/04, Bavarian Lager contra Comisión,

A esa decisión del Tribunal de Primera Instancia se presenta recurso de casación por parte de la Comisión, anulando el TJUE la sentencia previa. El TJUE declarando que el Reglamento de acceso a los documentos establece "un régimen específico y reforzado de protección de la persona cuyos datos personales pudieran, en su caso, divulgarse". Opinando que a esa transparencia prevista en el Reglamento de acceso y para los documentos que contienen datos personales, el Reglamento de protección de datos es plenamente aplicable. Dando el Tribunal también por buena la actuación de la Comisión de denegación de aquella solicitud de acceso al acta completa considerándola legítima, y considerando suficiente la versión primera suministrada con los nombres quitados. Exculpando también a la misma de la no ponderación en base a la insuficiencia de la petición de la empresa cervecera: "al no haber presentado Bavarian Lager ninguna justificación expresa y legítima ni ningún argumento convincente para demostrar la necesidad de la transmisión de dichos datos personales, la Comisión no pudo ponderar los distintos intereses de las partes implicadas"[638][639]

[638] Resultan interesantes las deliberaciones en el documento del Supervisor Europeo de Protección de Datos (SEPD, 2011), sobre el acceso público a los documentos que incluyen datos personales después de la sentencia (Recuperada el 25 de agosto de 2018):
https://edps.europa.eu/sites/edp/files/publication/11-03-24_bavarian_lager_en.pdf

[639] Como ejemplo de jurisprudencia del TEDH vinculada citaremos la sentencia Társaság a Szabadságjogokért contra Hungría, nº 37374/05, de 14 de abril de 2009; en la que una ONG de derechos humanos, solicita al Tribunal Constitucional húngaro acceso a la información relativa a través de un miembro del Parlamento. Solicitud de acceso que se desestima sobre la base de la protección de datos personales. La demandante recibe la consideración por el Tribunal de Estrasburgo de "vigilante social"en su actuación, mereciendo una equiparación en este sentido a la prensa. El Tribunal observa verdaderos obstáculos en el acceso a la información de interés público en Hungría que podrían hacer más difícil el trabajo de los medios de comunicación o actividades similares en el papel democrático y necesario de vigilancia pública para la sociedad, declarando la violación del artículo 10 del CEDH.

4. Especialidades en la protección de datos. La Directiva PNR y la Directiva sobre Ciberseguridad.

De igual manera en este recorrido normativo se regulan temas de especialidad jurídica en el tratamiento y en la protección del derecho que nos ocupa. Muy especialmente en el año 2016, junto al impulso ofrecido por el Reglamento General y también debido em parte a su consecuencia, se han aprobado instrumentos normativos que atienden situaciones especiales relacionadas con la protección de datos. Nos referimos así a dos importantes normas: la Directiva 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR). Y la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Junto a ellas, veremos en el capítulo siguiente la especialidad del contenido de la protección de datos en el ámbito penal, con la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

4.1 La Directiva sobre registro de datos de pasajeros (PNR)

Producto de un acuerdo sobre un texto transaccional que se culmina a finales de 2015 entre las instituciones de la U.E., el Parlamento Europeo la aprueba el 14 de abril de 2016 y el Consejo adopta la Directiva el 21 de abril de 2016.

La Directiva empieza fijándose en sus Considerandos (1,2 y 4) en su antecedente regulatorio, la “Decisión marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record — PNR) con fines policiales”, que el Tratado de Lisboa dejó obsoleta. Y en la Directiva 2004/82/CE del Consejo, de 29 de

abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, asi como en el "Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano" de 2010, que sirve de acicate a la aprobación de la Directiva.[640]

4.1.1 Objeto.

Se destacan los objetivos de la Directiva en el "de garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes" (Considerando 5), junto a su uso eficaz de los datos en su evaluación para separar efectivamente a los "transeúntes no sospechosos" de los que deban ser objeto de investigación habitual en los aeropuertos. La Directiva aporta en su anexo II las categorías de delitos graves a efectos de la misma. Se prevé una "unidad única de información" donde se deben transmitir los datos PNR, que debe llevar cada Estado miembro, cuyo coste y llevanza corresponde a los mismos, sin que esta obligación de seguridad recaiga sobre las compañías aéreas, y con respeto a los derechos fundamentales y a la protección de datos de los pasajeros (Considerandos 12 a 14).[641]

Después de dejar, como es preceptivo, a los Estados miembros la apreciación de los riesgos para la seguridad y las amenazas de terrorismo, junto a las medidas para que las compañías aéreas puedan atender a estos requerimientos, se establece que no se podrá tomar decisión con efecto jurídico en base a su tratamiento ni la evitación de las

[640] Un resumen en forma de aproximación crítica de la Directiva PNR lo encontramos en Bellanova (2018) del que destacaremos, además, su apunte sobre la influencia global de esta regulación de vigilancia.

[641] En el Considerando 15 nos dice además que: "...el objetivo de reflejar las legítimas necesidades de las autoridades públicas para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves, mejorando así la seguridad interior en la Unión y la protección de los derechos fundamentales y, en particular, el derecho a la intimidad y la protección de datos personales. Para ello se deben aplicar exigencias elevadas, conforme a la Carta de los Derechos Fundamentales de la Unión Europea («la Carta»), el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal («Convenio nº 108») y el Convenio para la protección de los derechos humanos y de las libertades fundamentales («el CEDH»). Dichas listas no deben basarse en el origen racial o étnico, religión o convicciones, opiniones políticas o de cualquier otro tipo, la pertenencia a un sindicato, la salud, vida u orientación sexual. Los datos PNR solo deben contener la información detallada sobre las reservas e itinerarios de viaje que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior."

obligaciones internacionales sobre asilo y ayuda al refugiado con coartada en ellos.[642] Elemento de indudable actualidad e importancia en la Unión Europea en estos últimos años, en lo que se ha venido a conocer como "la crisis de los refugiados" procedentes, en su mayoría, de Siria.

La importancia de los principios de la Jurisprudencia del TJUE en su protección de los derechos fundamentales y la intimidad también se refleja expresamente, asi como la obligación de intercambio de información, a través de la Europol, en investigación de delitos de terrorismo o delitos graves que tiene especial consideración (Considerandos 22, 23 y 24).

El período de conservación de los datos debe ser el necesario y proporcional a los fines de la investigación, debiendo los derechos nacionales de regulación respetar el derecho de protección de datos establecido en cada Estado miembro. Y tiene presente la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal o la que legislación que la sustituya (Considerandos 25 a 27). Conformidad y respeto con ella (al igual que con la CDFUE y el CEDH), que debe seguir también el ejercicio de los derechos ARCO y el de información sobre el tratamiento en este ámbito. Previsión que, igualmente, se contempla para las transferencias internacionales a terceros Estados (Considerandos 28 y 31). Espíritu de respeto que recorre toda la Directiva, que explicita de manera más definitiva cuando nos dice que "se ha limitado en lo posible el alcance de la presente Directiva pues permite conservar los datos PNR durante un período máximo de 5 años, tras el cual los datos deberán suprimirse; dispone que los datos deben despersonalizarse mediante

[642] El Considerando 20 nos dice: "Tomando plenamente en consideración el derecho a la protección de datos personales y el derecho a la no discriminación, no debe tomarse ninguna decisión que pudiera tener efectos jurídicos adversos para una persona o afectarle gravemente en razón únicamente del tratamiento automatizado de datos PNR..." y Considerando 21: "Los Estados miembros no podrán en ningún caso utilizar el resultado del tratamiento de datos PNR como razón para eludir sus obligaciones internacionales en virtud de la Convención de Ginebra sobre el Estatuto de los Refugiados de 28 de julio de 1951, modificada por el Protocolo de 31 de enero de 1967, ni para negar a los solicitantes de asilo unas vías jurídicas seguras y efectivas de acceso al territorio de la Unión con vistas a ejercer su derecho a la protección internacional."

enmascaramiento de los elementos de los datos tras un período inicial de seis meses, y prohíbe la recogida y utilización de datos sensibles." (Considerandos 36 y 37).

Ya en el articulado de la Directiva (artículos 1 y 2) se específica su objeto y ámbito de aplicación, regulando la transferencia y tratamiento de los datos PNR por las compañías aéreas de vuelos exteriores de la UE, así como su intercambio, en caso de investigación y persecución de delitos de terrorismo y otros delitos graves. Si se quisiera aplicar esta Directiva a vuelos interiores de la UE por un Estado miembro, éste deberá comunicarlo por escrito a la Comisión, que publicará esa notificación, y que podrá se revocable por el Estado miembro en cualquier momento. En el momento de esa notificación se aplicará la Directiva como si de vuelos exteriores se tratara.

Aquí la Directiva deja a los Estados miembros la importante prerrogativa de replegarse en su espacio aéreo y señalar a otro Estado miembro como elemento de destino o de procedencia, similar al de un tercer país, convirtiéndolo, vía notificación a la Comisión, en un espacio aéreo de mayor recelo que el propio, en una especie de selección de vuelos a la carta a los efectos de aplicación de la Directiva.

El tercer artículo se encarga de las definiciones, aclarándonos el concepto PNR o registro de nombres de los pasajeros como "una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades". Deriva la definición de terrorismo a los artículos 1 a 4 de la Decisión marco 2002/475/JAI, y los delitos graves al propio Anexo II de la Directiva.[643]

[643] En ambos casos se destaca su carácter amplio tanto en la definición de la Decisión marco, que contempla el terrorismo en su acepción más amplia, junto con las actividades ligadas o relacionados con él (ejemplo hurto, chantaje o libramiento de documentos administrativos si se demuestra su relación con el terrorismo) como en el listado del Anexo, que contempla la corrupción o el espionaje industrial por ejemplo como delitos graves.

4.1.2 Tratamiento y Responsabilidades de los Estados miembros.

Dentro del Capítulo segundo, bajo el título de "responsabilidades de los estados miembros", se prevé la "Unidad de Información sobre los Pasajeros («UIP»)", que será la autoridad antiterrorista designada por los mismos, y será la unidad responsable de la recolección e intercambio de los datos PNR; pudiendo establecerse entre dos o más Estados miembros una autoridad única para que actúe como UIP, en un tipo de cooperación reforzada a estos efectos en la protección de datos.

Las UIP designarán un responsable de protección de datos, y será la responsable del tratamiento de datos que reciba de las compañías aéreas y de la evaluación de los mismos, que se realizará de forma no discriminatoria y sus consecuencias "no perjudicarán el derecho de entrada de las personas que gocen del derecho de la Unión de libre circulación en el territorio del Estado miembro en cuestión" (artículos 4 a 6)[644]

Los Estados miembros mantendrán una lista de autoridades competentes para solicitar o recibir los datos PNR procedentes de las UIP, que podrán tratar posteriormente esos datos "únicamente con el fin específico de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves". (Artículo 7.4)

El artículo 8 establece la obligación de las compañías aéreas de suministrar los datos PNR "a la base de datos de la UIP del Estado miembro en cuyo territorio aterrizará o de cuyo territorio saldrá el vuelo". En caso de los datos API (*advance passenger information*) cuyo formato no coincida con el del PNR, corresponderá a los Estados miembros, y no a las compañías, facilitar los medios técnicos para garantizar su envío. Asegurándose igualmente el intercambio de información entre las UIP's de los Estados miembros concernidos por medio de cualesquiera vías de las establecidas para la cooperación entre Estados miembros (artículos 9 y 10). Además, la Europol tendrá

[644] Artículo 6, en su apartado 9, y en base a la Directiva 2004/38/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al derecho de los ciudadanos de la Unión y de los miembros de sus familias a circular y residir libremente en el territorio de los Estados miembros por la que se modifica el Reglamento (CEE) 1612/68 y se derogan las Directivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE y 93/96/CEE.

derecho a a solicitar los datos PNR y su procesamiento a la UIP respectiva, rigiéndose en todo caso por su normativa propia.[645]

Igualmente, para las transferencias internacionales se prevé su posibilidad por los Estados miembros siguiendo la Decisión marco 2008/977/JAI[646] o cuando sea necesario para el cumplimiento de los fines de la Directiva y se dan las condiciones de la misma. Incluso se prevé la transferencia "sin el consentimiento previo del Estado miembro del que fueron obtenidos los datos, se permitirán en circunstancias excepcionales y solamente si:

"a) son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país, y

b) el consentimiento previo no puede obtenerse a su debido tiempo." (Artículo 11).

Importante es la previsión del período de conservación de los datos PNR proporcionados por las compañías de vuelo a las UIP por éstas a un máximo de 5 años, y de 6 meses para proceder a su despersonalización "mediante enmascaramiento" que permitan no identificar directamente al pasajero. Tras esos 6 meses, solo se podrán divulgar los datos PNR completos en caso de necesidad por delitos de terrorismo y delincuencia grave y así lo disponga una autoridad judicial u otra autoridad nacional competente que verifique su concordancia de divulgación con el derecho nacional.[647]

De manera recurrente se remite en el artículo 13, específico en la referencia a la protección de datos personales, a la Decisión marco 2008/977/JAI (algo que también se hace, tal y como observaremos, en la Directiva 2016/680). Y también recurrentemente

[645] La Directiva cita expresamente la Decisión del Consejo 2009/371/JAI por la que se crea la Oficina Europea de Policía (Europol), si bien debemos entender ya la remisión al Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo. Un análisis crítico sobre este Reglamento desde el ámbito de la protección de datos lo encontramos en Blasi Casagran (2016) que califica esa protección como adecuada en el mismo.

[646] Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal

[647] Artículo 12.2 desarrollando los datos que permiten esa identificación directa en sus letra a) a f) (nombre, apellidos, dirección y datos de contacto, datos de pago, información de viajeros asiduos, observaciones que la permiten y datos API) y Artículo 12.3.

se remite a un “sin perjuicio de la aplicabilidad de la Directiva 95/46/CE” sobre los datos generales de los pasajeros. Se prohibirán por los Estados miembros los datos PNR “que revele el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona...”. Junto con la responsabilidad de aquellos en su tratamiento y la obligación de llevanza de registro al respecto. Junto con la necesidad de previsión por los Estados miembros de sanciones por incumplimiento y la actuación de revisión y control de la autoridad de control respectiva en su territorio. (Artículos 13, 14 y 15).

4.1.3 Ejecución.

Los capítulos tercero y cuarto fijan su regulación en las disposiciones de ejecución y en las disposiciones finales a seguir, previendo protocolos y formatos para las transmisiones de estos datos y las medidas técnicas para su utilización, junto con la asistencia del Comité (habitual ya en el paquete de protección de datos)[648]. Se establece la obligación de transposición “a más tardar el 6 de mayo de 2018” y revisión de la Comisión sobre la Directiva “a más tardar el 6 de mayo de 2022” (artículos 18 y 19), a la que se enviarán anualmente por parte de los Estados miembros el “conjunto de información estadística sobre los datos PNR comunicados a las UIP.”[649]

El Anexo I recoge los Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas que incluirán:

[648] Con referencia al Reglamento (UE) 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.

[649] Artículo 20 que incluirán al menos: “a) el número total de pasajeros cuyos datos PNR hayan sido recopilados e intercambiados; b) el número de pasajeros identificados para un examen ulterior.”
Asimismo en el siguiente enlace podremos comprobar su estado de transposición (a septiembre de 2018 Dinamarca, Grecia, España, Francia, Chipre, Países Bajos, Portugal, Rumanía, Eslovenia y Finlandia no están todavía al corriente en su obligación normativa de transposición) (Recuperado el 1 de septiembre de 2018):
https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=uriserv:OJ.L_.2016.119.01.0132.01.SPA

Localizador de registro PNR. Fecha de reserva/emisión del billete. Fecha(s) fechas de viaje prevista(s). Nombre(s) y apellido(s). Dirección y datos de contacto. Todos los datos de pago. Itinerario completo del viaje. Información sobre viajeros asiduos. Agencia de viajes/operador de viajes. Situación de vuelo del pasajero. Información PNR escindida/dividida. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados). Información sobre el billete. Datos del asiento, incluido el número. Información sobre códigos compartidos. Toda la información relativa al equipaje. Número de viajeros. Cualquier información API y todo el historial de cambios de los datos PNR.

4.2. La Directiva sobre Ciberseguridad.

Debemos realizar un previo comentario sobre la vinculación de esta Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, con la prioridad establecida por la Comisión en relación con su estratégica Agenda Digital dentro del Plan 2020, para, en particular, el desarrollo del Mercado Único Digital[650]. Y ello con el ánimo de no perder de vista que el mundo digital no puede multiplicar los derechos y contenidos que tenemos en el mundo real.

Esta Directiva, así, pone su foco de regulación en los incidentes de seguridad y su incremento como amenaza al funcionamiento de las redes y sistemas de información (internet principalmente), por la incidencia económica negativa que las mismas pueden tener para el mercado europeo, debido a su carácter transnacional. (Considerandos 1 a 4).

Los niveles de seguridad, recursos y capacidades son muy distintos entre los Estados miembros, siendo así necesario “un planteamiento global en la Unión que integre

[650] Como referencia bien resumida de la idea y su prioridad enlazamos la Comunicación de 6 de mayo de 2015 de la Comisión sobre el Mercado Único Digital al Parlamento, al Consejom al Comité Económico y Social y al Comité de las Regiones (Recuperado el 29 de agosto de 2018): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52015DC0192

requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales" (considerandos 6 y 7). Aplicándose por tanto a los prestadores de esos servicios, si bien con la excepción de los operadores de redes públicas de comunicaciones regidos por la Directiva 2002/21/CE[651] con requisitos específicos de seguridad e integridad, y de los prestadores de servicios de confianza definidos en el Reglamento (UE) 910/2014.[652]

Se contempla, asimismo, la posible legislación especial en la materia, por parte del derecho de los Estado miembros o del derecho de la Unión, como puede ser el del sector del transporte marítimo y fluvial o el de regulación y la supervisión del sector bancario y de las infraestructuras de los mercados financieros, que exigen importantes niveles de cautela y atención en la regulación de la seguridad de las redes y sistemas de información, lo que los hace tener un carácter diferenciada con leyes especiales propias (considerandos 9 a 15).

4.2.1 Objeto, definiciones y ámbito de aplicación.

Las disposiciones generales de la Directiva se establecen en el capítulo primero, siendo su objeto "lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión", con el fin de "mejorar el funcionamiento del mercado interior" con la obligación para los Estados miembros de adoptar una estrategia nacional de seguridad, al igual que la creación de un Grupo de cooperación y de red de equipos de respuesta a incidentes de seguridad informática (red de CSIRT). También deben establecer los requisitos de seguridad para los operadores de servicios esenciales y para los proveedores de servicios digitales y la obligaciones relacionadas para que los

[651] Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco)
[652] Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE

Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT, con las excepciones de aplicación vistas (artículo 1).

Es, por tanto claro, que el objetivo de esta Directiva es la armonización en la seguridad de la prestación de los servicios digitales, si bien de manera tal que no impida el normal tránsito europeo de ese mercado. Prueba de ello es que hasta el Considerando 63 no hace una mención expresa de los riesgos que estos incidentes tienen para la protección de datos.[653]

Es, asimismo, llamativa (como en las otras Directivas del paquete de protección) la remisión genérica a la protección de datos de carácter general a la Directiva de 1995, en lugar de al Reglamento de 2016 (artículo 2).

El artículo 4 se encarga de las definiciones de las que destacamos lo que se entiende por seguridad de las redes y sistemas de información en "la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos"; remitiéndose a otras normas en las especificaciones técnicas con carácter general. Entra también a perfilar el significado de elementos técnicos como el de servidor, motor de búsqueda o el servicio de computación en nube.[654]

Los criterios para identificar a los operadores de servicios esenciales los encontramos en una entidad que presta un servicio esencial para el mantenimiento de actividades

[653] Recordando aquí al objetivo de la Directiva del 95 con el flujo de datos del mercado interior.
Nos dice que "En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes y las autoridades responsables de la protección de datos han de cooperar e intercambiar la información sobre todos los asuntos pertinentes ante las violaciones de datos personales derivadas de incidentes"

[654] Como ejemplos diremos que para los términos de "servicio digital" o "especificación técnica" se remite a la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, o para el término "mercado en línea" a la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) 2006/2004 y la Directiva 2009/22/CE (Directiva sobre resolución alternativa de litigios en materia de consumo)

sociales o económicas cruciales, siendo la prestación de dicho servicio dependiente de las redes y sistemas de información, y que en caso de un incidente, tendría efectos perturbadores significativos en la prestación de dicho servicio (artículo 5.2)

Las listas de operadores deberán revisarse con regularidad por los estados miembros que las establecen y al menos cada 2 años a partir de mayo de 2018. Además se intercambiaran entre los Estados, en su obligación de cooperación entre sí. Igualmente se establece qué se considerará como efecto perturbador negativo por los Estados miembros en los siguientes factores intersectoriales (además de los específicos del sector). [655]

4.2.2 Marcos nacionales de seguridad de las redes y sistemas de información. Su armonización.

La Directiva se encarga además de la regulación de los marcos nacionales de seguridad de las redes y sistemas de información, con la exigencia a los Estados miembros de adopción de una estrategia nacional de seguridad para los sectores y servicios contenidos en los anexos de la Directiva en los que se deben dejar claro los objetivos y prioridades, el marco de gobernanza para lograrlos, la identificación de medidas e indicación de los programas, tanto de concienciación como de investigación relacionados con la estrategia; así como con el plan de evaluación de riesgos y una lista de los diversos agentes participantes en la ejecución de la estrategia (artículo 7.1 letras a) a g)).

[655] Según el artículo 6 serán:
"a) el número de usuarios que confían en los servicios prestados por la entidad de que se trate;
b) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad;
c) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública;
d) la cuota de mercado de la entidad;
e) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente;
f) la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio."
El Anexo II contempla los siguientes sectores: Energía (en sus división de Electricidad, Crudo y Gas), Transporte (en sus distintos medios aéreo, por ferrocarril, marítimo-fluvial y por carretera), Banca, Infraestructuras de los mercados financieros, Sector sanitario, Suministro y distribución de agua potable e Infraestructura digital.

El artículo 8 se fija en las Autoridades nacionales competentes y en el punto de contacto único: “el punto de contacto único ejercerá una función de enlace para garantizar la cooperación transfronteriza entre las autoridades de los Estados miembros y con las autoridades competentes en otros Estados miembros y con el Grupo de cooperación...”

El artículo 9 regula los Equipos de respuesta a incidentes de seguridad informática (CSIRT). Se prevé además de la cooperación nacional entre el punto de contacto único y los CSIRT del mismo Estado miembro sobre las obligaciones de la Directiva, la cooperación europea al respecto a la que se dedica el capítulo tercero. Se institucionaliza el Grupo de cooperación formado por representantes de los Estados miembros, la Comisión y la ENISA, con funciones propias de órgano consultivo cualificado y se crea la red de CSIRT nacionales con el principal cometido de la actuación coordinada y asistencia mutua entre los CSIRT de los diversos Estados miembros (artículo 10 y artículos 11 a 13).

Por tanto adquieren un importante papel, según la Directiva y ya en los Considerandos de la misma (19 a 26), la definición e identificación de los operadores de servicios esenciales, en este sentido, por los Estados miembros y los servicios a los que afecte, y la diferenciación de lo que es esencial o no en aquellos servicios donde estos caracteres se encuentren mezclados, y el establecimiento de cooperación cuando ese servicio se preste en dos o más Estados miembros. Todo ello, para dar como resultado “medidas nacionales para determinar qué entidades están sujetas a obligaciones en materia de seguridad de las redes y sistemas de información” (considerando 25). Y ello, junto con las medidas de los factores para determinar el impacto de esos incidentes en la seguridad de las redes, lo que implica planificar e implementar una “estrategia nacional de seguridad de las redes y sistemas de información que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar”; con designación (más de una) de la autoridad o autoridades a nivel nacional competente y responsable al respecto (considerandos 27 a 30).

Debe designarse, por tanto, un punto de contacto único nacional para facilitar la cooperación transfronteriza entre los Estados miembros, y las autoridades competentes o los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés de “computer security incident response teams”), siendo igualmente esencial

la cooperación entre los sectores público y privado. Al igual que la actuación de la ENISA[656] a nivel europeo en este campo, que da asistencia a los Estados miembros y les sirve de enlace con la Comisión. Existe, además, un Grupo de Cooperación entre los Estados y la Comisión, y resalta la utilidad que la compartición de los incidentes y la respuestas que se den a los mismos supone en la cooperación en su lucha efectiva en Europa, ya que nos encontramos ante un problema y reto de nivel global; con especial hincapié en los proveedores de servicios digitales por ser las empresas que están en el centro de toda esta actividad regulada en la Directiva. (Considerandos 31 a 55).

La Directiva entra, asimismo, en la regulación de armonización de los requisitos en materia de seguridad de los operadores de servicios esenciales, y el capítulo quinto en esos mismos tipos de requisitos para proveedores de servicios digitales, así como en su aplicación y observancia en los dos casos, añadiendo para el segundo caso la previsión de la jurisdicción en el Estado del establecimiento principal (artículos 14 a 18).

Se sigue el concepto de establecimiento principal del Estado donde esté instalado el proveedor de servicios digitales para atribuir la competencia judicial, con obligación de designación de representante en otros Estados donde opere. Con la remisión a la Comisión, y sus ya habituales posibles actos de ejecución delegados, para mantener el fin y criterio de armonización de la Directiva; la cual "observa los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído" (considerandos 64, 65 y 75).[657]

---

[656] La ENISA es la agencia con competencia sobre estos asuntos en Europa, con sede en Heraklion (Grecia) y regida por el Reglamento (UE) n.o 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.o 460/2004.

[657] La normalización o elaboración de directrices y orientaciones técnicas dirigidas a la aplicación convergente al igual que la notificación voluntaria para aquellas entidades no identificadas como operadores de servicios esenciales y que no sean proveedores de servicios digitales, también se recogen; junto con las preceptivas disposiciones finales propias de una directiva en el último capítulo octavo, aplicándose todas sus medidas partir del 10 de mayo de 2018. (Artículos 19 y 20 y Artículos 21 a 27).
Asimismo dedemos hacer referencia a su estado de transposición (A septiembre de 2018 Austría, Bélgica, Bulgaria, Irlanda, Grecia, España, Letonia, Luxemburgo, Países Bajos y Rumanía no la habián transpuesto todavía) que podemos seguir en el siguiente enlace (Recuperado el 1 de septiembre de 2018): https://eur-lex.europa.eu/legal-content/ES/NIM/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

5. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Un nuevo planteamiento.

5.1. Trabajos previos de la reforma

El documento de la Comisión[658] de evaluación de impacto sobre la aprobación del Reglamento y la modificación de la Directiva de protección de datos en Europa puede considerarse el "pistoletazo de salida" del cambio normativo que alumbraría al Reglamento europeo de protección de datos. Empezando por tanto su andadura en 2012 y resultando su proceso de aprobación de no mucha mayor agilidad y celeridad que el establecido para la aprobación en su momento para la Directiva.[659]

En el resumen suministrado por la propia Comisión[660] (2012) se observan los ejes, que, a partir de los estudios y conclusiones del Grupo de Trabajo previsto en el artículo 29 de la Directiva, vienen a articular las principales motivaciones para tan importante revisión legal a nivel europeo.

Nos hacemos eco de ellas manifestadas en las siguientes problemáticas:

Problema 1: Obstáculos que la fragmentación, la inseguridad jurídica y la aplicación poco coherente de las normas suponen para las empresas y las autoridades públicas (...)

Problema 2: Dificultades para que las personas físicas controlen sus datos personales (…)

Problema 3: Lagunas e incoherencias de la protección de datos personales en el ámbito de la cooperación policial y judicial en materia penal.

---

[658] El borrador del grupo de trabajo que da por iniciado el procedimiento de reforma del derecho a la protección de datos en Europa lo tenemos en el trabajo de evaluación de impacto de la Comisión bajo el título en inglés de: COMMISSION STAFF WORKING PAPER Impact Assessment /SEC/2012/0072 final. (Recuperado el 25 de agosto de 2018):
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072

[659] Recordémoslo, ocupó desde el año 1990 hasta 1995.

[660] Recuperado el 25 de septiembre de 2018:
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012SC0073

Presenta especial interés la alusión a la proporcionalidad y subsidiaridad en la motivación de la futura norma, admitiendo la inadecuación del marco normativo nacional para afrontar la realidad jurídica de la protección de datos en el momento actual. Y el fin último que justifica la necesidad proporcionada de la medida legal.[661]

Establece igualmente ya los objetivos políticos de la intervención legal, no solo en el aseguramiento y potenciación del mercado interior, sino en "aumentar la efectividad del derecho fundamental a la protección de datos" y en "reforzar la coherencia del marco de protección de datos de la UE, incluso en el ámbito de la cooperación policial y judicial en materia penal". Basculándose con especial significancia el peso de la motivación jurídico-política de la Norma hacia el foco de los derechos humanos y su efectividad personal, en comparativa con la Directiva, aun manteniendo el eje primigenio del mercado común armonizado y su mejora.

La opción por la que se decanta la Comisión, de las analizadas como posibles soluciones, es la de la modernización del marco jurídico por las razones principales de seguridad jurídica, la simplificación, clarificación y coherencia normativa.[662]

5.2 Propuesta de la Comisión

El nombre de la versión definitiva de la propuesta de la Comisión la de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) COM/2012/011 final - 2012/0011 (COD)[663]

[661] Comisión (2012, 4): "...en la situación actual, los Estados miembros no se bastan por sí solos para resolver los problemas, especialmente los derivados de la fragmentación de las legislaciones nacionales que dan aplicación al marco regulador de la protección de datos de la UE (...) Las medidas previstas son proporcionadas, puesto que entran dentro de las competencias de la Unión conforme se definen en los Tratados, y son necesarias para asegurar la uniformidad de aplicación de la legislación de la UE, garantizando con ello una salvaguardia efectiva y equitativa de los derechos fundamentales de los ciudadanos..."

[662] Comisión (2012, 5): opción 2 del documento complementada con medidas de las otras dos opciones en comparativa.

[663] Recuperado el 25 de agosto de 2018: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0011

Será bajo la responsabilidad de Vivianne Reding y la Dirección General de Justicia cuando se presenta esta propuesta del Reglamento de Protección de datos.[664]

La base jurídica de la propuesta se encuentra en el artículo 16 del TFUE. En cuanto al análisis de la subsidiariedad y proporcionalidad que estipula el 5.3 del TUE la Comisión lo deja claro el documento (Propuesta Comisión, 2012, 6-7): la protección de datos se protege mejor a escala europea. Así, nos dice que: "…el análisis de subsidiariedad indica la necesidad de adoptar iniciativas a escala de la UE por las razones siguientes:

– El derecho a la protección de datos de carácter personal, consagrado en el artículo 8 de la Carta de los Derechos Fundamentales, requiere el mismo nivel de protección de datos en toda la Unión. La ausencia de normas comunes de la UE provocaría el riesgo de que hubiera diferentes niveles de protección en los Estados miembros y restricciones en los flujos transfronterizos de datos personales entre los Estados miembros con distintas normas.

– Los datos personales se transfieren a través de las fronteras nacionales, tanto internas como externas, a ritmos cada vez más rápidos. Además, existen retos prácticos a la ejecución de la legislación de protección de datos y la necesidad de cooperación entre los Estados miembros y sus autoridades, que tiene que organizarse a escala de la UE para garantizar la unidad de aplicación del Derecho de la Unión. Por otra parte, la UE es la que está en mejores condiciones para garantizar de forma efectiva y coherente el mismo nivel de protección de los ciudadanos cuando sus datos personales se transfieren a terceros países.

– Por sí solos, los Estados miembros no pueden mitigar los problemas que se plantean en la situación actual, especialmente los debidos a la fragmentación de las legislaciones nacionales. Por tanto, existe una necesidad específica de establecer un marco armonizado y coherente que permita una adecuada transferencia de datos personales a

[664] (Propuesta Comisión, 2012) Diario Oficial de la Unión Europea, L 119, 4 de mayo de 2016.
Hemos de decir que la propuesta de Reglamento va de la mano de la propuesta de Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos ya que comparten el mismo marco jurídico de reforma.

través de las fronteras interiores de la UE, al tiempo que se garantiza una protección efectiva a todas las personas físicas en la UE.

– Las iniciativas legislativas de la UE propuestas serán más efectivas que acciones similares adoptadas a nivel de los Estados miembros debido a la naturaleza y magnitud de los problemas, que no se circunscriben al ámbito de uno o varios Estados miembros."

De especial interés, e íntimamente relacionado con ese cimiento constitucional que apuntábamos en el Capítulo I, nos parece su memoria sobre derechos fundamentales afectados que, en forma de resumen, nos relatan juegan un papel muy importante en la legislación a aprobar (Propuesta Comisión, 2012, Punto 3). Nos lo establece de la siguiente manera:

"Resumen de las cuestiones relativas a los derechos fundamentales

El derecho a la protección de los datos de carácter personal se establece en el artículo 8 de la Carta de los Derechos Fundamentales, en el artículo 16 del TFUE y en el artículo 8 del CEDH. Como subrayó el Tribunal de Justicia de la UE, el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad. La protección de datos está estrechamente ligada al respeto de la vida privada y familiar establecido en el artículo 7 de la Carta. Ello se refleja en el artículo 1, apartado 1, de la Directiva 95/46/CE, que establece que los Estados miembros garantizarán la protección de las libertades y de los derechos fundamentales de las personas físicas, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de datos personales.

Otros derechos fundamentales potencialmente afectados y consagrados en la Carta son los siguientes: la libertad de expresión (artículo 11 de la Carta); la libertad de empresa (artículo 16); el derecho a la propiedad y especialmente a la protección de la propiedad intelectual (artículo 17, apartado 2); la prohibición de toda discriminación, y en particular la ejercida por razón de raza, orígenes étnicos, características genéticas, religión o convicciones, opiniones políticas o de cualquier otro tipo, discapacidad u orientación sexual (artículo 21); los derechos del menor (artículo 24); el derecho a un alto nivel de protección de la salud humana (artículo 35); el derecho de acceso a los

documentos (artículo 42); el derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47)."

La propuesta de la Comisión sigue de cerca para el establecimiento de las definiciones las de la Directiva de 1995, que estará bien presente como antecedente de mucho peso, si bien se introducen algunas novedosas como la de "violación de los datos personales" basada en el artículo 2, letra h), de la Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE,[665] o aquellos sobre datos relacionados con la salud (genéticos, biométricos…). También novedad es la introducción de la definición de establecimiento principal o representante o que se considera por "niño", basada en la Convención de las Naciones Unidas sobre los Derechos del Niño.[666]

Como nos indica el documento (Propuesta Comisión, 2012, 9) resaltamos que "en la definición de consentimiento se añade el criterio «explícito» para evitar un paralelismo con consentimiento «inequívoco» que se preste a confusión y con el fin de dotarse de una definición única y coherente", o la introducción de nuevos elementos adicionales en el capítulo de los principios como el principio de transparencia.

El artículo 13 de la propuesta sigue de cerca establecidos en la letra c) del artículo 12, letra c), de la Directiva del 95/46/CE, ampliándolos a todos los destinatarios, "incluidos los corresponsables y coencargados del tratamiento", o en referencia al 15 de la propuesta que "dispone el derecho de acceso del interesado a sus datos personales y añade nuevos elementos, como la obligación de informar a los interesados sobre el periodo de conservación"

El original de la propuesta ya preveía en su artículo 17 el "derecho al olvido", perfilando su contenido y sus condiciones de ejercicio, elemento que será motivo de diferentes propuestas y enmiendas por parte de las diferentes instituciones comunitarias. Igualmente el artículo 20 de la propuesta es el que establece el derecho del interesado a

[665] Ver páginas 379-380 del trabajo. Directiva modificada por la Directiva 2009/136/CE

[666] En este sentido Van der Hof (2014) se hace eco de la cada vez mayor importancia de regulación del uso de Internet por los menores en Europa, en particular con la introducción de protección específica en el nuevo paquete de protección de datos, y sobre todo en su ánimo de seguir el espíritu de la Convención de las N.U de 1989. Si bien considera de posibles efectos limitados esta protección dudando de qué la mayor dotación de responsabilidad a los menores asegure en ellos una concienciación efectiva de los riesgos.

no ser objeto de una medida basada en la elaboración de perfiles. Vincula así la propuesta la facultad de limitación por parte de la Unión o de los Estados miembros de estos derechos directamente "en las obligaciones que emanan de la Carta de los Derechos Fundamentales y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, interpretados por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos." (Propuesta Comisión, 2012, 10).

Además, la propuesta para el artículo 28 introduce la obligación de conservar la documentación relativa a las operaciones de tratamiento para los responsables y encargados del tratamiento, en lugar de la notificación general a la autoridad de control del 18 y del 19 de la Directiva. Y el 31 y 32 de la propuesta introducen la obligación de notificar las violaciones de los datos personales, y la evaluación de impacto de la protección de datos para tratamientos de riesgo, en el artículo 33. Además de la nueva figura del delegado de protección de datos en los artículos 35 y 36.

Las importantes referencias a los códigos de conducta y a la posibilidad de establecer mecanismos de certificación, y sellos de garantía en materia de protección de datos, también se presentan en la propuesta de la Comisión como elementos de novedad.

Ahondamiento regulatorio se da respecto a la previsión de las transferencias internacionales de datos, precisamente motivado por los diversos pronunciamientos judiciales y observación de la realidad jurídica (si bien la sentencia Schrems no estaba todavía sustanciada). Dándole fuerza ejecutiva importante la propuesta a la Comisión.

La influencia de la OCDE es innegable en la redacción de la Comisión en estos aspectos, reconociéndolo así: "el artículo 45 establece explícitamente mecanismos de cooperación internacional para la protección de los datos de carácter personal entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se considera que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 12 de junio de 2007." (Propuesta Comisión, 2012, 13)

Igual abundamiento se observa en la regulación de las autoridades de control y parecida influencia reconocida por la Comisión, en este caso para el Tribunal de Justicia, sobre todo para decantarse por la plasmación definitiva de su componente necesario de independencia.[667]

Otra novedad importante presente en el documento presentado por la Comisión está en el mecanismo de coherencia y su regulación a la que le presta atención en los artículos 57 a 63, al igual que la extensa regulación propuesta sobre recursos y apelaciones.

También es de destacar la atención a las disposiciones especiales con las que se ve el derecho de protección de datos obligado a mantener una relación diferenciada. Así la conciliación del mismo con el derecho a la libertad de expresión (siguiendo también aquí la influencia del Tribunal de Justicia, concretamente en el caso Satamedia); o las salvaguardias específicas para el tratamiento con fines sanitarios, son dos de los elementos principales en este sentido. Reconociéndose también la especialidad de los tratamientos sobre empleo o para fines históricos, estadísticos y de investigación científica. (Propuesta Comisión, 2012, 17)

Si bien se lamenta el Supervisor Europeo de Protección de Datos[668] de que no se haya avanzado igualmente en esa forma de Reglamento Europeo en la materia que trata la Directiva sobre protección de datos en el ámbito de la aplicación penal (las otras Directivas que forman parte del paquete de reforma). Critica asimismo la falta de una mayor exhaustividad en el desarrollo integral de la protección de datos. Digamos que el Supervisor pedía aún más en la concreción normativa, sin cerrar del todo los campos incoherentes de protección con su conjugación nacional.

[667] (Propuesta Comisión, 2012, 13) Cita el documento concretamente la sentencia de 9 de marzo de 2010, de Comisión contra Alemania en el asunto (C-518/07)

[668] Supervisor Europeo de Protección de Datos (2012). Resúmen en castellano disponible (Recuperado el 25 de agosto de 2018) en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:52012XX0630(01)

5.3 Continuación de la tramitación del Reglamento

Tras la emisión de los dictámenes preceptivos en el procedimiento, de los que destacaremos, el aludido primer dictamen del Supervisor Europeo de Protección de Datos y las opiniones del Comité Económico y Social y del Comité de las Regiones, se produce una sucesión de debates en el seno del Consejo el 6-7 de diciembre de 2012, y a lo largo de 2013 (8 de marzo, 6 de junio, 7 de octubre y 6 de diciembre) así como el 4 de marzo de 2014. En 2014 el Parlamento Europeo aprueba su dictamen y manifiesta su posición en primera lectura con numerosas enmiendas al texto (12 de marzo de 2014).[669]

Pasando de nuevo al Consejo, que a lo largo de 2014 se reúne en otra serie de reuniones informales al igual que en el año anterior (6 de junio, 10 de octubre y 4 de diciembre). En marzo y junio de 2015 se vuelven a producir debates en el Consejo, que ofrece una declaración de los propósitos del proyecto normativo que resumiremos en sus titulares: "Un continente, una ley, el Reglamento establecerá un único conjunto de normas en materia de protección de datos válido en toda la UE (...) Derechos adicionales y reforzados: el derecho al olvido se verá consolidado(...) Normas europeas en territorio europeo: las empresas con sede fuera de Europa tendrán que aplicar las mismas normas cuando ofrezcan servicios en la UE (...) Mayores poderes de las autoridades nacionales independientes de protección de datos (...) «ventanilla única» para las empresas y los ciudadanos..."[670][671]

---

[669] Comité Económico y Social Europeo (2012) y Comité de las Regiones (2012). Recuperado el 25 de agosto de 2018: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52012AE1303

[670] Como así lo anuncian en su nota de prensa de 15 de junio de 2015 dada en Luxemburgo. Recuperada el 25 de agosto de 2018: http://europa.eu/rapid/press-release_IP-15-5176_es.htm

[671] En este sentido resulta de interés Fernández Conte y León Burgos (2016, 43-50) que relatan los pormenores de las tramitación del Reglamento y sus diferentes "tomas y dacas" institucionales, hasta su aprobación definitiva.

Como elemento llamativo de su análisis aludiremos a la referencia a que incluso hay una película documental sobre la tramitación parlamentaria y la intensa actividad lobbistica al respecto, contenida en la obra cinematográfica "Democracy" del director David Bernet (p. 44). O la información sobre la "impresionante cantidad de enmiendas" presentadas a 11 de marzo de 2013 (p. 45). Destacando la labor del Comité LIBE en el Parlamento Europeo y del Grupo DAPIX en el Consejo, y con la exitosa aproximación del método de trabajo de "enfoques parciales generales" y la importancia de las "reuniones tripartitas informales" hasta llegar a la posición común. Que podemos traducir en que se ha llegado al texto publicado a base de muchas reuniones de orden del día concreto entre representantes determinados de las tres instituciones, hasta formar un elemento normativo único pactado.

5.4 Finalización de la Tramitación.

Tras el segundo dictamen del Supervisor Europeo de Protección de Datos[672], y a lo largo de la primera mitad de la tramitación, se van sucediendo debates en el Consejo que irán perfilando la redacción definitiva del texto, para terminar en la adopción de la comunicación de la Comisión al Parlamento Europeo sobre la posición del Consejo en fecha 11 de abril de 2016. En la comunicación, la Comisión se muestra satisfecha porque el Consejo[673] ha seguido sus posicionamientos sobre la norma. Si bien difieren en la incidencia del Reglamento sobre el "acervo Schengen", ya que la Comisión considera las modificaciones operadas a su propuesta como una oportunidad perdida para el desarrollo del mismo. Emite así una declaración al respecto: "La Comisión lamenta la modificación operada en su propuesta inicial, con la supresión de los considerandos 136, 137 y 138, relativos al acervo de Schengen. La Comisión considera que, especialmente en lo que respecta a visados, control de las fronteras exteriores y retornos, el Reglamento general de protección de datos supone un desarrollo del acervo de Schengen para los cuatro Estados asociados a la ejecución, aplicación y desarrollo de dicho acervo…" (Comisión, 2014)[674]

Por último, y en fecha 14 de abril, el Parlamento emite resolución de adopción del Reglamento, que tras un par de sesiones de ulteriores debates en el Consejo, llega a la firma conjunta de los dos Presidentes de las instituciones en fecha 27 de abril de 2016.[675][676]

---

[672] Supervisor Europeo de Protección de Datos (2015)

[673] Debates en el Consejo de 28 de enero de 2016; 8 y 10 de febrero de 2016; 17 y 31 de marzo de 2016; 5,6 y 8 de abril de 2016.

[674] En su punto 3: "La Comisión apoya este acuerdo dado que se ajusta a los objetivos de su propuesta. El acuerdo mantiene la naturaleza del instrumento jurídico propuesto por la Comisión (…) La posición del Consejo confirma el enfoque de la Comisión respecto del ámbito de aplicación territorial del Reglamento(...)Al seguir el enfoque de la Comisión, el acuerdo refuerza los principios del tratamiento de datos (por ejemplo, minimización de datos) y los derechos de los interesados, incluyendo el derecho al olvido y el derecho a la portabilidad y desarrollando aún más los derechos existentes, tales como el derecho a la información y el derecho de acceso (…) El acuerdo también preserva y desarrolla en mayor medida el enfoque basado en el riesgo ya presente en la propuesta de la Comisión."
Como nos informan Conte Fernandez y León Burgos (2016, 49): "El Parlamento y el Consejo alcanzaron un acuerdo informal necesario. Posteriormente se ratificó oficialmente por el Consejo en su sesión de 12 de febrero de 2016. El texto se sometió a los juristas lingüistas del Consejo para su revisión y, solo después fue elevado a aprobación definitiva. Tal aprobación tuvo lugar el 8 de abril…"

[675] Resolución legislativa del Parlamento Europeo, de 14 de abril de 2016, respecto de la Posición del Consejo en primera lectura con vistas a la adopción del Reglamento del Parlamento Europeo y del

Para finalizar, apuntaremos aquí que el capítulo décimo del Reglamento se encarga de los actos delegados y de ejecución sobre la Comisión, que "entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán". Y mencionaremos igualmente el Capítulo Undécimo de las disposiciones finales de la norma, que deroga la Directiva 95/46/CE "con efecto a partir del 25 de mayo de 2018", no imponiendo el Reglamento obligaciones adicionales a las de la Directiva 2002/58/CE sobre comunicaciones electrónicas en redes públicas de comunicación de la Unión.[677]

En este sentido, el Comité de las Regiones (2012, Punto 11) planteaba dudas en el ámbito de la subsidiariedad y la proporcionalidad así como en la adopción de actos delegados:

"Se han planteado dudas sobre:

—el alcance de la competencia legislativa de la Unión Europea en virtud del artículo 16, apartado 2, del TFUE, que limita la búsqueda de una plena armonización en el ámbito del tratamiento de datos por parte de los organismos públicos y plantea cuestiones si se extiende a situaciones internas en relación con la propuesta de Directiva para el ámbito policial y judicial;

—el nivel de abstracción de la normativa, que sería comparable al de una Directiva de la Unión Europea pero que, debido a la falta de instrumentos de aplicación de los Estados miembros, proporciona una seguridad jurídica demasiado escasa; el hecho de facultar a

---

Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva95/46/CE (Reglamento general de protección de datos) (05419/1/2016 – C8-0140/2016 – 2012/0011(COD))

[676] Como resumen de la importancia de esta nueva propuesta y aprobación del paquete legislativo de Protección de datos nos fijamos en las palabras de Juan Fernando López Aguilar (2015, 31) (eurodiputado y miembro de la Comisión del PE participante en su discusión) que nos dice que "el "Data Protection Package" expresa como ninguna otra iniciativa hasta la fecha el salto hacia adelante efectuado por el Tratado de Lisboa en lo que se refiere a la dimensión constitucional de la UE (…)desde el punto de vista político, no se recuerdan muchas otras iniciativas europeas (quizá solo la nueva Directiva del Tabaco…) que hayan suscitado tanta presión política a todo lo ancho de la UE y sus EE.MM, originada por la acción de los lobbys industriales y corporativos..."

[677] Apartado 5 del artículo 92, Artículo 94 y Artículo 95.

la Comisión Europea para adoptar actos delegados, según estipula el artículo 86, en cuestiones que no son de detalle, lo que resulta problemático..."[678]

El Reglamento deja en vigor, asimismo, los acuerdos internacionales conformes a Derecho de la Unión suscritos antes del 24 de mayo de 2016, y establece la obligación de informe de la Comisión al Parlamento y al Consejo "a más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años", de evaluación y revisión del Reglamento, y más en particular sobre asuntos de mayor incidencia y responsabilidad de la Comisión, como son las transferencias internacionales de datos y los mecanismos de cooperación y coherencia. La Comisión podrá igualmente proponer reformas legislativas sobre otros actos jurídicos de la Unión en materia de protección de datos.[679]

El Reglamento que entró en vigor a los 20 días de su publicación es aplicable (de manera directa y obligatoriamente en todos sus elementos como buen Reglamento) desde el 25 de mayo de 2018 (artículo 99).

5.5 Objeto del Reglamento

El inicio de la norma no deja lugar a dudas sobre la voluntad y espíritu de plasmación jurídica de la protección de datos en Europa: "la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental..."[680]

Los 173 Considerandos de la norma vienen a anticipar y motivar el desarrollo articulado de la misma y se pueden definir asimismo por bloques de interés que van estableciendo con antelación los elementos de ideas fuerza que el extenso Reglamento transmite como nuevo paradigma de la protección de datos y la privacidad en Europa.

Así, los Considerandos con alusión de motivación jurídica sobre el texto a los derechos fundamentales y libertades personales, crecen en gran medida con respecto a la Directiva de 1995, fundamentando ya directamente el Reglamento en esa concepción.

[678] Esto sería explicación para la adopción del instrumento Reglamento y no el de Directiva, pero es claro que solo puede ser un Reglamento de base que necesita de actos delegados para su plenitud normativa.
[679] Artículos 96, 97 y 98
[680] Considerando 1

Así nos dice el Considerando 4: "el tratamiento de datos personales debe estar concebido para servir a la humanidad..."[681]

Ya el propio informe del Comité Económico y Social Europeo (2012) sobre el Reglamento fija su atención en la intersección de fundamentación en la naturaleza del texto propuesto. Así, en el punto 2.3 se nos dice que "la propuesta sobre la que se consulta al CESE se sitúa en la encrucijada de dos de las principales orientaciones jurídico-políticas y político-económicas de la UE", para continuar sustanciando la iniciativa en ese espíritu por un lado anclado en el artículo 8 de la CDFUE, y por otro en la Agenda digital para Europa y, más en general, en la Estrategia Europa 2020[682]. Es decir, vertiente derecho fundamental y vertiente mercado único. Llama la atención que el CESE circunscriba el Reglamento dentro de la protección de los derechos fundamentales, haciendo mucho más hincapié en esta faceta que en la que pudiera suponer la propuesta de Reglamento de cara a los efectos económicos y al mercado. Estableciendo un llamativo posicionamiento la defensa prioritaria del elemento derecho fundamental de la norma con ventaja a su utilidad como instrumento de mercado.[683]

Así, y como ya hemos apuntado, fundamentando los primeros Considerandos la protección de datos como derecho fundamental irrenunciable (1,2 y 4) y el reconocimiento del precedente armonizador del mercado común de la Directiva y el carácter de utilidad para el mercado que indudablemente el Reglamento contiene (3 y 5), se van delimitando esos bloques de exposición previa de la Norma.

La necesidad acuciante motivada por la realidad tecnológica y por la Globalización, se presentan justificantes de la, ya no armonización de legislaciones, sino de la propia

[681] Así con mención expresa o indirecta a esa fundamentación, que atraviesa transversalmente toda la norma: Considerandos 1,2,4,10,11,13,16,19,32,35,38,39,51,52,53,54,59,63,65,66,67,71,73,75,78,79, 84,86,94, 104,114,117,137,141,142,143,153 y 156.

[682] Puntos 2.3.1 y 2.3.2 del informe.

[683] Puntos 3.7 y 3.8 del informe

En este sentido consultar también el Dictamen del Comité Económico y Social Europeo (2011) sobre la "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea." Recuperado el 16 de agosto de 2016: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011AE0999&from=ES

adopción de la figura reglamentaria europea para la correcta protección del derecho. Así nos dice el Considerando 6 que "la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial"; o el Considerando 10: "para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros".

Ya en el articulado del Reglamento, y en el capítulo I de "Disposiciones Generales" se establece el objeto y el ámbito de aplicación de la Norma. Son las personas físicas las destinatarias de la misma, sus derechos y libertades fundamentales, y su derecho a la protección de datos particularmente, dentro de la Unión. Si bien sin que esa protección sea motivación de restricción o prohibición para el flujo de esos datos en la Unión.[684]

Debemos destacar también las objeciones críticas que presentó el Comité de las Regiones (2012) al texto original, en este caso a su estructura institucional: "el Comité de las Regiones opina que el Reglamento afecta de manera desproporcionada a los

[684] Artículo 1. Observándose un ánimo de mayor generalidad hacia la privacidad como concepto amplio. Así nos dice Piñar Mañas (2016, 56), "la aprobación de la CDFUE ha sido decisiva en la redacción del Reglamento General de Protección de Datos. La consideración de la protección de datos como derecho fundamental y el artículo 8 de la Carta están en la base misma del Reglamento…"
Igualmente nos resume bien Arenas Ramiro (2015, 324) el leit motiv jurídico del Reglamento: "La voluntad de la Propuesta de Reglamento no es otra que unificar criterios, evitar la fragmentación jurídica y ofrecer una mayor seguridad mediante la elaboración de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento de la libre circulación de los datos y del mercado (…)La Propuesta de Reglamento busca garantizar el derecho a la protección de datos de los ciudadanos europeos teniendo en cuenta la existencia de Internet, su carácter internacional y la repercusión económica que conlleva. Estamos pues ante un importante avance en el fortalecimiento del derecho a la protección de datos personales, en el control de los ciudadanos de sus datos personales, en la generación de una mayor confianza. Pero estamos ante un derecho que no acaba aquí, que tiene una dimensión internacional y un carácter transversal que no poseen otros derechos, y de ahí la necesidad de coherencia y armonización en este terreno..." (Arenas Ramiro, 2015, 368)

organismos públicos y sigue siendo ambiguo en lo que respecta a sus competencias y en el ámbito del Derecho laboral. El Reglamento contiene además para los organismos públicos a nivel regional y local una serie de obligaciones (por ejemplo, mayores exigencias en materia de documentación, la obligación de garantizar la portabilidad de los datos, entre otras), que no se corresponden con mejoras considerables en lo que respecta a los derechos...” O indicando la necesidad de incentivos para la correcta consecución de los objetivos de la norma: “serán necesarios instrumentos incentivadores destinados a los responsables del tratamiento de datos para recompensar sus esfuerzos en la protección de datos...”, y ofreciendo una visión de mayor laxitud con las garantías de protección que el texto presenta, y que se aparta de la postura del CESE (punto 8): “(el Comité de las Regiones) advierte del peligro de que, en el afán por reforzar la protección de los datos personales, se coarte en exceso el ejercicio de los ciudadanos del derecho a disponer libremente de ellos en la medida en que se les niega la posibilidad de dar su consentimiento...”[685]

[685]Dictamen del Comité de las Regiones (2012). Recuperado el 25 de agosto de 2018: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012AR0625&from=ES

CAPÍTULO TERCERO

CONTENIDO DE LOS DERECHOS PROTEGIDOS EN LA PROTECCIÓN DE DATOS EUROPEA Y SUS PROCEDIMIENTOS.

Pasamos ahora a ocuparnos del contenido sustancial de la protección de datos en Europa, principalmente a través de la norma que es presente y futuro de la misma en la Unión. En el anterior capítulo ya presentábamos el Reglamento como culminación directa y última de la privacidad europea tras el precedente determinante de la Directiva en ese itinerario de protección jurídica. Veremos además, en este contenido, la jurisprudencia y algunas consideraciones institucionales relacionadas en cada uno de sus campos, así como su vinculación con el importante antecedente de la Directiva.

1. Definiciones de la Protección de Datos.

En primer lugar nos situaremos conceptualmente sobre las definiciones que se vienen a dar en el Reglamento sobre protección de datos, que acoge, en buena medida la terminología jurídica ya acuñada por la Directiva de 1995, y la labor de interpretación que sobre esos conceptos ha ido pergeñando el TJUE, en el tiempo que dista entre una y otra norma.

El artículo 2 de la Directiva nos presentaba las definiciones, que regirían la norma, y que vienen a plasmar por vez primera en el Derecho europeo y, de manera todavía más novedosa, en su Derecho Derivado, conceptos (hoy ya clásicos) de la protección de datos, que venían a asentar buena parte de la inspiración motivada por el Consejo de Europa y su Convenio 108, así como el histórico vertebrador de otras organizaciones

internacionales influyentes en la materia, como la OCDE, o los pronunciamientos de Naciones Unidas. Si bien con novedades propias importantes de la propia Directiva.[686]

Por tanto, la Directiva en su momento supuso asimismo una novedad de introducción terminológica en la protección de datos personales, estableciendo la definición de los términos de "datos personales" así como la de su "tratamiento" y el "responsable" y "encargado" del mismo. Igualmente el concepto separado de "fichero" y el de "tercero", "interesado" y "consentimiento" de este. En cuanto a las personas implicadas en ese tratamiento de datos, que afianzada la distinción de la Directiva en cuanto a sujetos activos: el "responsable" del tratamiento que será cualquier persona también jurídica (y en la realidad sobre todo jurídica y Administración Pública) que tenga por así decirlo la justificación jurídica para el uso (fines y medios) de esos datos. Y el "encargado" del mismo que sería la persona que trate esos datos por cuenta del responsable.

Personas implicadas como elementos de tipo más pasivo serían el "tercero", considerando como tal a toda persona distinta de los anteriores ("responsable y encargado"), y del propio titular de los datos. El "destinatario", toda persona a la que vayan dirigidos esos datos. Y el propio interesado titular de los datos, que podría adquirir una vertiente activa en el momento de ejercitar sus derechos (acceso, rectificación oposición...), y sobre todo en el momento de su consentimiento que pone en juego y permite todo el juego y ciclo del tratamiento. Esta estructura definitoria de la Directiva queda traspasada prácticamente en su totalidad al Reglamento General, que vendrá a matizar ese conjunto.

Así, el artículo 4 del Reglamento, actualmente, se encarga de manera profusa (llegando hasta 26) de establecer las definiciones, y presenta algunas novedades respecto de la Directiva, junto con un ánimo de pormenorización que pretende dejar claro los contornos que aquella pudiera haber dejado poco delimitados. También es conocedor asimismo el legislador europeo de la jurisprudencia de delimitación sobre los conceptos de la protección de datos europea, a la que aludimos en el siguiente epígrafe.

Así, por ejemplo, para los datos da una definición amplia en "toda información sobre una persona física identificada o identificable" y también amplía la del tratamiento en

[686] Ver parte primera de este trabajo.

"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no..."[687]. E introduce como novedad la de "elaboración de perfiles" en "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física..." o "seudonimización" como aquel tratamiento "de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional..."[688] Así como la inclusión de definiciones de datos genéticos o datos biométricos. O el mayor ánimo de definición detallada en el concepto de "tratamiento transfronterizo" o "objeción pertinente y motivada"[689] o la referencia al "servicio de la sociedad de la información", tal y como se define en la letra b) del apartado 1 del artículo 1 de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.[690][691]

Hace también la Norma importante definición en los Considerandos 36 y 37 sobre el "responsable del tratamiento en la Unión" y su "establecimiento", que "debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables", que desvincula al hecho del tratamiento de datos.[692]

[687] Definiciones 1 y 2
[688] Definiciones 4 y 5
[689] Definiciones 13 y 14
[690] Definiciones 23, 24 y 25
[691] Los datos son "anonimizados" si ya no incluyen identificadores; en cambio, son "pseudonimizados" si los identificadores están encriptados. A diferencia de los datos "anonimizados", los datos pseudonimizados son datos personales (ADFUE7 CoE, 2014, 39).
Ver en este sentido (Grupo del artículo 29, 2007, 22).
[692] "Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal..."

1.1 La labor interpretadora del TJUE sobre la definición de "datos personales"

El revelador y muy interpretado judicialmente[693] artículo 2 de la Directiva, precedente necesario del artículo 4 del Reglamento, nos dice:

"A efectos de la presente Directiva, se entenderá por:

a) «datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b)«tratamiento de datos personales,, («tratamiento,»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c)"fichero de datos personales" ("fichero")[694]: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d)responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos, personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias

[693] Sobre la importatntísima labor del TJUE, no ya solo en la construcción definitoria de la protección de datos europea sino como garante general de la misma debemos reseñar a Rallo Lombarte (2017).

[694] La enmienda 14 del Parlamento Europeo quería eliminar, como nos ilustra Heredero Higueras (1997, 72), la palabra fichero por el término "datos" por considerarla superada, si bien se mantuvo.
Hemos de decir que el concepto no parece todavía superado ya que se mantiene en el número 6 del artículo 4 del nuevo REPD.

nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

e) encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f)"tercero", la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g)"destinatario": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h)"consentimiento del interesado",: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan."

En la sentencia del Tribunal de Justicia (Sala Tercera) de 17 de julio de 2014, del caso YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S. (asuntos acumulados C-141/12 y C-372/12), se interpreta el concepto de "datos personales" del artículo 2, junto con el 12 y 13 de la Directiva (entrando en juego además el 8 y el 41 de la CDFUE), en su posible extensión para el derecho de acceso a solicitantes de residencia.[695]

[695] Peticiones de decisión prejudicial planteadas por el Rechtbank Middelburget y el Raad van State.
Es el caso de solicitantes de residencia temporal en los Países Bajos, contra el Ministro de Inmigración, Integración y Asilo de aquel país, motivado por la tramitación de la solicitud de esos permisos y los datos que los mismos contienen en sus expedientes, así como la comunicación de los mismos a los solicitantes. Uno de los demandantes, tras la desestimación de su solicitud, reclamó la "minutas" o conjunto de datos que obraban en su expediente, documentación que también le fue denegada, sobre la cual alega judicialmente a su derecho.

La pregunta elevada respecto a este demandante (YS) es la siguiente: “1) ¿Son los datos reproducidos en la minuta relativos al interesado datos personales en el sentido del artículo 2, letra a), de la Directiva [95/46]?

2) ¿Es el análisis jurídico que figura en la minuta un dato personal en el sentido de la disposición antes citada?

3) En el supuesto de que el Tribunal de Justicia confirmase que los datos antes mencionados son datos personales, ¿está obligada la autoridad pública/de tratamiento a dar acceso a esos datos personales en virtud del artículo 12 de la Directiva [95/46] y del artículo 8, apartado 2, de la Carta?

4) En este contexto, ¿puede el interesado invocar directamente el artículo 41, apartado 2, letra b), de la Carta y, en caso de respuesta afirmativa, debe interpretarse la expresión “dentro del respeto de los intereses legítimos de la confidencialidad del proceso de toma de decisiones” que figura en el mismo en el sentido de que puede denegarse el derecho de acceso a la minuta por ese motivo?

5) Cuando el interesado solicita acceder a la minuta, ¿debe facilitar la autoridad pública/de tratamiento una copia de dicho documento para dar cumplimiento, de este modo, al derecho de acceso?”

Los litigios relativos a los demandantes M y S se fundan en similares resoluciones denegatorias de acceso a esa “minuta” de datos, con variaciones propias de cada uno de los casos.

En primer lugar y en contra de las posturas de los gobiernos neerlandés, checo y francés personados en el proceso, que consideran el análisis jurídico de la minuta no incluido, el Tribunal considera indudable el carácter de datos personales[696] de los controvertidos en el caso, citando la sentencia Huber. Si bien el análisis de derecho, aunque está basado sobre los mismos datos y no sea un análisis en abstracto, no tiene esa consideración de dato personal, no teniendo los demandantes derecho a conocer su contenido para posible

[696] Párrafo 38: ”...no plantea dudas que los datos relativos al solicitante del documento de residencia que figuran en una minuta, como su nombre, fecha de nacimiento, nacionalidad, sexo, etnia, religión e idioma, son una información que se refiere a esa persona física, que es identificada en esa minuta, en particular, por su nombre, y que deben calificarse, en consecuencia, como «datos personales»”

apreciación de incorrecciones o rectificaciones (dando aquí si la razón a los referidos gobiernos).[697]

Y se les reconoce el derecho de acceso a la minuta pero en el sentido de poder hacerse una idea completa, ya que, conforme a la Directiva se "dispone de un derecho de acceso a todos los datos personales que le conciernan que sean objeto de tratamiento por las autoridades administrativas nacionales, en el sentido del artículo 2, letra b), de la Directiva. Para dar cumplimiento a este derecho, basta con facilitar a dicho solicitante una idea completa de esos datos en forma inteligible, es decir, permitiéndole conocer dichos datos y comprobar que son exactos y son tratados de conformidad con esta Directiva para que pueda, en su caso, ejercer los derechos que dicha Directiva le confiere". Descartándose además las pretensiones de los demandantes basadas en el genérico "derecho a la buena administración" del artículo 41 de la CDFUE ante las autoridades nacionales, basado en su mero permiso de residencia.

Otra sentencia de importante interpretación en este ámbito definitorio es la sentencia del Tribunal de Justicia (Sala Cuarta) de 11 de diciembre de 2014.[698]

El literal de la pregunta en la sentencia (párrafo 18 de la sentencia) es: "la utilización de un sistema de cámara de vídeo instalado en una vivienda familiar con el fin de proteger

[697] Párrafos. 41 a 48. Particularmente el 46. "En estas circunstancias, extender el derecho de acceso del solicitante del documento de residencia a ese análisis jurídico no ayudaría, en realidad, al objetivo de dicha Directiva, consistente en garantizar la protección del derecho a la intimidad de ese solicitante en lo que respecta al tratamiento de sus datos, sino al objetivo de garantizarle un derecho de acceso a los documentos administrativos, que, sin embargo, la Directiva 95/46 no contempla."

[698] František Ryneš contra Úřad pro ochranu osobních údajů. (Asunto C-212/13). Procedimiento prejudicial en el que se interpreta el artículo 3 de la Directiva, concretamente en cuanto al concepto de "ejercicio de actividades exclusivamente personales o domésticas", y en una controversia jurídica entre el señor Ryneš y la Úřad pro ochranu osobních údajů), la Agencia de protección de datos checa).
Petición de decisión prejudicial planteada por el Nejvyšší správní soud.
Los hechos motivadores del conflicto proceden de la instalación de una cámara fija por parte del señor Ryneš en el portón de su casa, y que grababa imágenes de la entrada de su vivienda y alrededores de manera fija, con la voluntad de mantener su persona y bienes seguros. Tras la instalación de la cámara y tras una rotura de cristales en su vivienda con un tirachinas, las imágenes captaron a dos sospechosos que fueron llevados a enjuiciamiento penal, reclamando uno de ellos por la posible ilegalidad de las grabaciones, y al señor Ryneš como responsable de ese tratamiento de datos. Argumento que fue admitido por el Tribunal sustanciador, si bien el señor Ryneš recurrió, siendo el Tribunal Supremo checo el que interpone la pregunta de interpretación.

los bienes, la salud y la vida de los propietarios de la vivienda, ¿puede calificarse de tratamiento de datos personales "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas" a efectos del artículo 3, apartado 2, de la Directiva 95/46 […], aunque tal sistema de videovigilancia cubra también el espacio público?"

Tras ir admitiendo el TJUE el carácter indubitado del carácter de dato personal (imágenes) y de tratamiento de datos (grabaciones) que se dan en el caso, establece, en coincidencia con las conclusiones del Abogado General, que la captación de imágenes del espacio público queda fuera de esas actividades meramente domésticas.[699]

Por último, debemos citar la novedosa sentencia del Tribunal de Justicia (Sala Segunda) de 19 de octubre de 2016. Patrick Breyer contra Bundesrepublik Deutschland. Que se centra en la interpretación del concepto de datos personales del artículo 2 y su relación con la letra f) del artículo 7 de la Directiva, y que dilucida la consideración de la dirección de protocolo de Internet como dato personal y la problemática de la conservación por un proveedor de servicios de medios en línea enfrentado a la normativa nacional que no permite la toma en consideración del interés legítimo perseguido por el responsable del tratamiento.[700]

El señor Breyer accede a varios portales de internet de organismos oficiales federales alemanes, los cuales, para evitar "ataques piratas" tienen por norma el registro de las consultas en ficheros, almacenando datos que incluyen los términos de la consulta y el protocolo IP del ordenador desde el que se realizan. El ciudadano alemán presenta recurso contencioso-administrativo reclamando la prohibición de la conservación de su dirección IP, dándosele parcialmente la razón en apelación en cuanto al reconocimiento de su IP como dato personal. Si bien el asunto llega al Tribunal Supremo del país en casación, sobre la controversia principal de que el IP permita identificar a una persona.

Terminando la duda en cuestión prejudicial:

[699] Párrafo 33: "En la medida en que una vigilancia por videocámara como la controvertida en el litigio principal se extiende, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente «personal o doméstica".
[700] Petición de decisión prejudicial planteada por el Bundesgerichtshof.

"1) ¿Debe interpretarse el artículo 2, letra a), de la Directiva 95/46/CE en el sentido de que una dirección IP registrada por un prestador de servicios [de medios en línea] en relación con un acceso a su sitio de Internet constituye para éste un dato personal desde el momento en que un tercero (en este caso, un proveedor de acceso) disponga de los datos adicionales que permiten identificar al interesado?

2) ¿Se opone el artículo 7, letra f), de [dicha Directiva] a una disposición nacional con arreglo a la cual un prestador de servicios [de medios en línea] sólo puede recoger y utilizar los datos personales de un usuario sin su consentimiento cuando sea necesario para ofrecer y facturar el uso concreto del medio en línea por ese usuario, y con arreglo a la cual el objetivo de garantizar el funcionamiento general del medio en línea no puede justificar la utilización de esos datos tras la conclusión de cada operación de uso concreta?"

Nos encontramos ante el caso de una IP dinámica, cuya identificación y asimilación con una persona es menos clara que para las IP estáticas, (que no requerirían de información adicional para esa asimilación personal). El Tribunal empieza por reconocer esa lógica, si bien va a lo largo de la sentencia enfocando su respuesta final. Así, nos dice que: "el hecho de que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a Internet de ese usuario, no parece que pueda excluir que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea constituyan, para éste, datos personales"[701]; llegando a la conclusión, a la luz de la información y hechos aportados al proceso, que "parece que el proveedor de servicios de medios en línea dispone de medios que pueden utilizarse razonablemente para identificar, con ayuda de otras personas, a saber, la autoridad competente y el proveedor de acceso a Internet, al interesado sobre la base de las direcciones IP conservadas. Interpretando en este sentido e incluyendo el hecho controvertido como dato personal según la Directiva y expresándolo así:"...una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal…"[702]

[701] Párrafo 44
[702] Párrafos 48 y 49

Responde asimismo el TJUE a la segunda cuestión en el sentido de que existe oposición de la norma alemana con el artículo 7 letra f) de la Directiva por disponer de manera más limitada en su dictado el alcance del principio de la norma europea común, ya que como nos dice la sentencia "debe recordarse igualmente que el artículo 7, letra f), de la mencionada Directiva se opone a que un Estado miembro excluya de manera categórica y generalizada la posibilidad de someter a un tratamiento determinadas categorías de datos personales, sin permitir una ponderación de los derechos e intereses en conflicto en cada caso concreto". Ponderación que parece no permitir la ley germana.[703]

[703] Párrafos 62 a 64

2. Ámbito de aplicación

2.1 Ámbito de aplicación material

La aplicación material del Reglamento se encuentra en el "tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero..."[704] Si bien quedan fuera los datos "en actividades fuera del Derecho de la Unión; en actividades comprendidas en el ámbito del capítulo 2 del título V del TUE[705]; actividades exclusivamente personales o domésticas y las provenientes de "autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención" (reproduciendo sustancialmente el ámbito de la Directiva de 1995).

Por tanto, excluidas de ese ámbito de aplicación tenemos las actividades fuera de la competencia del Derecho de la Unión, las actividades de política exterior y de seguridad común realizadas por los Estados miembros y las actividades personales o domésticas, así como las actividades de persecución penal.

En los considerandos también tenemos regulación importante relacionada con el ámbito de aplicación de la Norma[706], destacando que se ve dirigida únicamente a las personas físicas "independientemente de su nacionalidad o de su lugar de residencia", cuya protección "debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas" y siguiendo la habitual no aplicabilidad por razones "relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional" o "al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión". Tampoco se ocupa "en el curso de una actividad exclusivamente personal o doméstica", y explicita la norma que "entre las actividades

[704] Artículo 2
[705] Que se encarga de las "Disposiciones específicas sobre la política exterior y de seguridad común".
[706] Considerandos 14 a 21

personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades." Ahora bien, ello no implica que, como responsables del tratamiento de datos, los titulares de esas redes sociales no se encuentren sujetos a la norma. Así continúa "no obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas".

También se contempla la clásica diferenciación de aplicación en el ámbito penal, que se regirá por la Directiva que acompañe el paquete normativo europeo de reforma de protección de datos.[707]

En relación con la aplicación del Reglamento se vienen a establecer también elementos importantes en los considerandos 20 y siguientes, para la delimitación de lo que se considera "tratamiento de datos" y sus principios, que se manifiesta sustancial en el Reglamento, y que se va diferenciando en función de los elementos de ese tratamiento. Así la ubicación legal del tratamiento para su aplicación y que hace activarse a la norma, se contempla en un Considerando que nos dice que: "todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión..."[708]

Siguiendo la jurisprudencia asentada por el TJUE, establece "las actividades de tratamiento" como elemento a seguir para la aplicación del Reglamento, con el ánimo de garantizar la protección[709]. Cobra especial interés la seudonomización de los datos, siempre en relación con el concepto de persona identificada e identificable, no aplicándose el Reglamento a personas fallecidas[710]. A partir del Considerando 31 se

[707] Considerando 19 y Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

[708] Considerando 22

[709] Considerando 23

[710] Considerandos 26 a 30

encarga la Norma del consentimiento al tratamiento de datos, que empieza a darle forma en el Considerando 32: "el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal...".[711] Para encargarse luego de sus aristas en función de la finalidad del tratamiento (investigación, datos genéticos, salud), y con la novedad de la mención específica a los niños del Considerando 38.[712]

2.1.1 La sentencia Lindqvist y el ámbito de aplicación material[713]

La sentencia Lindqvist, si bien compitiendo en importancia con la posterior sentencia Costeja/Google, es la que viene marcando, entre otras determinaciones elementales, la aplicación (material) de la protección de datos en Europa, de manera asentada y a la que nos referíamos en los anteriores párrafos. La sentencia, con múltiples recorridos y aristas, y a la que podríamos calificar como "sentencia multinivel" en la protección de datos en Europa, porque abarca elementos múltiples de interpretación, vendrá a asentarse en este Reglamento normativamente, como hemos apuntado. Ya que era un clásico de referencia aplicable en el derecho europeo de la privacidad.

Sentencia que parte de cuestión prejudicial solicitada por el tribunal sueco Göta hovrätt, sobre el procedimiento penal entablado contra la catequista Bodil Lindqvist, y en relación con la publicación de datos en Internet y la compatibilidad con la Directiva 95/46 para el caso de una protección más rigurosa de esos datos personales en la

[711] Considerandos 31 a 35

[712] Ya en los primeros considerandos de la norma se advierte ese ánimo excepcionalista, tan propio de la legislación de la Privacidad, en algunos supuestos en relación con el consentimiento en el tratamiento de datos Asi el C. 31 "Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros..."

[713] Sentencia del Tribunal de Justicia de 6 de noviembre de 2003 (Asunto C-101/01).

normativa de un Estado miembro (presentando observaciones además de la Comisión, los Gobiernos neerlandés y británico).[714]

La sentencia recoge las 7 preguntas sobre el asunto realizadas por el Tribunal sueco, que implican una buena labor de interpretación por el Tribual de Luxemburgo, de las que en este apartado nos interesa concretamente la segunda y la tercera, relacionadas con el ámbito de aplicación:

"1) ¿Constituye una conducta comprendida en el ámbito de aplicación de la Directiva [95/46] la designación de una persona -con su nombre o con su nombre y número de teléfono-en una página web de Internet? ¿Constituye un "tratamiento total o parcialmente automatizado de datos personales" el hecho de que en una página web de Internet realizada personalmente se relacione a una serie de personas junto con datos y afirmaciones relativas a su situación laboral y a sus aficiones?

2) En caso de respuesta negativa a la cuestión anterior, ¿constituye un "tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero", contemplado en el artículo 3, apartado 1, de la Directiva, la conducta consistente en publicar en un sitio Internet diversas páginas web referidas específicamente a una quincena de personas, con enlaces entre dichas páginas que hacen posible la búsqueda por nombre de pila?

En caso de respuesta afirmativa a alguna de estas cuestiones, el hovrätt formula además las siguientes cuestiones:

3) ¿Debe considerarse excluida del ámbito de aplicación de la Directiva [95/46] por estar comprendida en alguna de las excepciones enumeradas en el artículo 3, apartado 2, la conducta consistente en divulgar datos de esta naturaleza acerca de los compañeros de trabajo en una página web privada, siendo los datos accesibles a todos aquellos que conozcan la dirección de dicha página?"[715]

[714] A la señora Lindqvist se le acusa en proceso penal en su país por haber infringido la ley sueca de protección de datos al publicar sin su consentimiento en Internet datos de colaboradores voluntarios, al igual que ella, en una parroquia protestante y ello en interpretación del artículo 3, 8 9, 13 y 25 de la Directiva.

[715] Siendo las siguientes preguntas las siguientes:

"4) ¿Constituye un dato relativo a la salud que, con arreglo al artículo 8, apartado 1, no puede ser objeto

Para la primera cuestión se responde en interpretación del artículo 3.1 de la Directiva. El Tribunal incluye los datos del caso sin duda en la definitoria de datos personales. Y de igual manera su ubicación en los parámetros del "tratamiento de datos".[716]

Para la tercera cuestión, y que es la que más nos interesa en este apartado del ámbito de aplicación, sigue la interpretación del 3 de la Directiva, en este caso de sus excepciones del apartado 2, y de si los hechos pudieran encuadrarse en ellas. El Tribunal citando su sentencia de 20 de mayo del mismo año antes analizada, deja claro que "las actividades voluntarias o religiosas como las que realiza la Sra. Lindqvist no pueden equipararse a las actividades citadas en el primer guión del artículo 3, apartado 2"(las no comprendidas en el ámbito de aplicación del Derecho comunitario) ni tampoco se incluye en la excepción del segundo guión (el ejercicio de actividades exclusivamente personales o domésticas)

Para la cuarta pregunta entra ya en juego el artículo 8, estableciendo lógicamente que una lesión en el pie (dato sobre una persona colaboradora de la parroquia revelado por Lindquist) "constituye un dato personal relativo a la salud."[717]

---

de tratamiento la divulgación en una página web de la circunstancia de que un compañero de trabajo, designado por su nombre, se ha lesionado el pie y está en situación de baja parcial?
5) Según la Directiva [95/46], la transferencia de datos personales a países terceros está prohibida en determinados casos. ¿Constituye una transferencia a países terceros en el sentido contemplado en la Directiva [95/46] el hecho de que una persona divulgue datos personales en una página web que está almacenada en un servidor en Suecia, de modo que los datos personales resultan accesibles a nacionales de países terceros? ¿Sigue siendo idéntica la respuesta si, por lo que se sabe, ningún nacional de un paístercero ha accedido efectivamente a dichos datos o si el servidor en cuestión se encuentra físicamente situado en un país tercero?
6) ¿Puede considerarse en un caso como el presente que las disposiciones de la Directiva [95/46] implican una restricción contraria al principio general de libertad de expresión, o a otras libertades y derechos vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales?"
Finalmente el hovrätt formula la siguiente cuestión:
"7) ¿Puede un Estado miembro, en una situación como la expuesta en las anteriores cuestiones, otorgar una protección más amplia a los datos personales o extender el ámbito de aplicación de la Directiva [95/46], aunque no se dé ninguna de las circunstancias enunciadas en el artículo 13?»"

[716] Párrafo 24"...Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones..."
Y Párrafo 25 "...De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole..."

[717] Párrafo 51
En este sentido ver la opinión del SEPD (2012) que abogaba por evitar la excepción doméstica en las redes sociales.

2.2 El ámbito de aplicación territorial

El Reglamento establece la definición del ámbito territorial en su artículo 3 como las actividades con "establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no..." Además de "al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión." O en un lugar "en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público"[718]

La novedad se aprecia con respecto a los artículos 3 y 4 de la Directiva donde ya se aplica al tratamiento que se realice aún fuera de la UE, debido a los nuevos tiempos de prestaciones de servicios habituales y generalizados suministrados por entidades y empresas con sede fuera de la Unión (principalmente Estados Unidos). E independientemente de que medie pago o no.[719]

En este sentido compartimos la percepción del profesor Ripol Carulla (2016, 95), que concluye en relación con el artículo 3 y sus disposiciones sobre aplicación territorial, que son "claras, racionales y simples" siguiendo el criterio de la Comisión.

En este sentido, debemos mencionar que el artículo 4 de la Directiva, que se viene encargando de las pautas de aplicación sobre el derecho nacional aplicable, se vino a interpretar por la sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de

[718] Artículo 3, punto 2 y punto 3.

[719] En este sentido sigue posturas garantistas como la del informe de European Digital Rights EDRI (2012, 6) y claramente influido por la sentencia Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Asunto C-131/12.

2015, caso Weltimmo s.r.o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság,[720] que tiene reflejo en ese artículo 3 del nuevo Reglamento. El Reglamento en este artículo unifica y expande el ámbito de aplicación material, como hemos visto "independientemente de que el tratamiento tenga lugar en la Unión o no...". Se comprueba así, una vez más, la influencia de la jurisprudencia del Tribunal en la legislación europea, y en la adopción del Reglamento como ley general, que hace perder a aquel artículo de la Directiva su razón de ser.

La sentencia referida venía a responder una petición de decisión prejudicial planteada por la Kúria húngara, interpretando junto al referido artículo 4 de La Directiva, en su apartado 1, también el artículo 28, en sus apartados 1, 3 y 6.

En el litigio una sociedad eslovaca (Weltimmo) gestiona una web de venta de muebles en Hungría, que en un plazo de un mes pasa de anuncios gratuitos a anuncios de pago. Ello provoca que muchos anunciantes soliciten la baja del servicio, no atendida por la empresa, que sigue cobrando los servicios. Reclamándose a la Agencia húngara de protección, impone ésta una multa a la empresa eslovaca, que a su vez recurre judicialmente esa sanción al Tribunal contencioso de Budapest y en casación a la Kuria (Supremo) húngara, que con dudas sobre el Derecho nacional aplicable, acude al Tribunal de Luxemburgo, diseccionadas en 8 preguntas.

De la diáspora legal que puede suponer la regulación de Internet, y de la necesidad de un criterio, al menos europeo, en cuanto a un marco general de protección, da constancia el párrafo 16 de la sentencia en la comprobación de las pruebas aportadas por la Autoridad de control húngara.[721]

[720] Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015. Asunto C-230/14 Weltimmo s.r.o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság.

[721] La sentencia nos dice que: "De tales elementos resulta, primero, que dicha autoridad tuvo conocimiento, de manera informal, por su homóloga eslovaca, de que Weltimmo no ejercía ninguna actividad donde radicaba su domicilio social, en Eslovaquia. Por otra parte, Weltimmo desplazó dicho domicilio, en reiteradas ocasiones, de un Estado a otro. Segundo, Weltimmo desarrolló dos sitios de anuncios inmobiliarios, redactados exclusivamente en húngaro. Abrió una cuenta bancaria en Hungría, destinada al cobro de sus créditos, y dispuso de un apartado de correos en dicho Estado miembro, para sus asuntos corrientes. El correo se recogía regularmente y se remitía a Weltimmo por vía electrónica. Tercero, eran los propios anunciantes quienes debían no sólo inscribir los datos relativos a sus inmuebles en el sitio de Weltimmo, sino también suprimirlos de dicho sitio si no deseaban que siguieran figurando en él una vez transcurrido el plazo de un mes señalado."

Las primeras seis preguntas se contestan conjuntamente por el Tribunal, que las resume en que: "el órgano jurisdiccional remitente pregunta, en esencia, si los artículos 4, apartado 1, letra a), y 28, apartado 1, de la Directiva 95/46 deben interpretarse en el sentido de que, en circunstancias como las controvertidas en el litigio principal, permiten a la autoridad de control de un Estado miembro aplicar su legislación nacional sobre protección de datos al responsable del tratamiento, cuya sociedad está registrada en otro Estado miembro y que gestiona un sitio de Internet de intermediación inmobiliaria que anuncia inmuebles situados en el territorio del primero de esos dos Estados". Respondiendo el Tribunal primero que sobre el Derecho aplicable (aplicable al responsable de dicho tratamiento) hay que estar a lo dispuesto en el artículo 4, que se estableció su ámbito de manera extensa, y que al igual que en la sentencia Google Costeja no puede interpretarse restrictivamente, precisamente por la naturaleza de los derechos y libertades a los que la Directiva se enfoca proteger. También se aplica ello en la concepción flexible del "establecimiento del tratamiento", indicando además la evidencia de actividad "real y efectiva en Hungría" por parte de la empresa. Siendo así relevante las actividades y su tratamiento para el Derecho aplicable, que es por tanto el húngaro, sin que lo sean la nacionalidad de los propietarios de los bienes inmuebles (aún también húngaros)[722]

Ello, resulta importante porque el Tribunal antepone el bien jurídico a proteger (el de datos personales) y el derecho de las personas en su ejercicio de protección, a la nacionalidad del propietario (y de la propiedad), para establecer el Derecho aplicable. Otorgando preeminencia a la protección de datos como derecho humano que como derecho dimanante de la propiedad, en este caso.

La séptima cuestión se refiere a la determinación de la autoridad de control competente para el caso. En este caso, el tribunal siguiendo el criterio acertado del Abogado General, vincula la actuación de las autoridades de control al territorio del estado miembro de la misma, por razones y "exigencias derivadas de la soberanía territorial del Estado miembro de que se trate, del principio de legalidad y del concepto de Estado de

[722] Párrafos 19 a 42

Derecho se desprende que el ejercicio de la potestad sancionadora". En lo que su actuación de investigación sí está íntimamente relacionada con el derecho aplicable.[723]

Para la octava cuestión el Tribunal ratifica que la versión húngara de la Directiva en su referencia "adatfeldolgozás" (procesamiento de datos), tiene el mismo sentido que el término "adatkezelés" (tratamiento de datos).

Por tanto, es de destacar esta sentencia en su importancia sobre todo por el anclaje que hace del derecho aplicable de la protección de datos, en el ámbito jurídico de la realización del tratamiento de los datos. Si bien la Autoridad de control está dependiente en todo caso de ese Derecho aplicable, aún con capacidad de comunicación y notificación a su homólogo nacional competente.[724]

En este sentido, debemos destacar la evolución que supone desde la Directiva el Reglamento sobre la concreción de la legislación nacional aplicable, cuya determinación propia de la Directiva, no se producen ya en el Reglamento, precisamente por su carácter normativo unificador, tal y como nos refiere De Miguel Asensio (2017, 78-79).

[723] Párrafos 42 a 60.

[724] "El artículo 4 (…) debe interpretarse en el sentido de que permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que éste ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento."

"En el supuesto de que la autoridad de control de un Estado miembro que entiende de unas denuncias, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, llegue a la conclusión de que el Derecho aplicable al tratamiento de los datos personales de que se trata no es el Derecho de ese Estado miembro, sino el de otro Estado miembro, el artículo 28, apartados 1, 3 y 6, de esa misma Directiva debe interpretarse en el sentido de que dicha autoridad de control sólo podría ejercer en el territorio de su propio Estado miembro las facultades efectivas de intervención que se le han conferido conforme al artículo 28, apartado 3, de la citada Directiva. Por lo tanto, no puede imponer sanciones basándose en el Derecho de ese Estado miembro al responsable del tratamiento de tales datos que no está establecido en dicho territorio, sino que, con arreglo al artículo 28, apartado 6, de la misma Directiva, debe instar la intervención de la autoridad de control dependiente del Estado miembro cuyo Derecho es aplicable."

2.2.1 La sentencia Verein für Konsumenteninformation contra Amazon EU

Relacionada con este cambio adaptado a los tiempos está la más actual sentencia del Tribunal de Justicia (Sala Tercera) de 28 de julio de 2016. Verein für Konsumenteninformation contra Amazon EU Sàrl. Asunto C-191/15.[725]

En esta sentencia, se entra a interpretar no solo la Directiva de Protección de Datos sino también los reglamentos Roma I y Roma II sobre obligaciones contractuales y extracontractuales.

Amazon EU con sede en Luxemburgo es demandada por Verein für Konsumenteninformation (Asociación de consumidores austriaca especialmente legitimada en la defensa de los derechos de estos) por supuestas cláusulas contrarias a las leyes comerciales austriacas. Principalmente a raíz de la duda sobre el derecho aplicable, se formula la cuestión del Tribunal Supremo de Austria, de la que en su cuarta pregunta in fine se sustancia la duda sobre interpretación de la Directiva que nos interesa de cara a este trabajo:

"4) Con independencia de la respuesta que se dé a las cuestiones anteriores:

(…) b) El tratamiento de datos personales realizado por una empresa que en el marco del comercio electrónico celebra contratos con consumidores residentes en otros Estados miembros, independientemente del Derecho que, en otro caso, fuera aplicable, ¿se somete exclusivamente, con arreglo al artículo 4, apartado 1, letra a), de la Directiva 95/46, al Derecho del Estado miembro en que se encuentra el establecimiento de la empresa y se produce el tratamiento de los datos, o debe ésta también respetar la normativa sobre protección de datos de los Estados miembros a los que dirige su actividad comercial?".

[725] Petición de decisión prejudicial planteada por el Oberster Gerichtshof.

La respuesta del Tribunal a este respecto se sustancia en los apartados últimos de la sentencia[726], en los que empieza aclarando el Tribunal que "se desprende que un tratamiento de datos efectuado en el marco de las actividades de un establecimiento se rige por el Derecho del Estado miembro en cuyo territorio esté situado dicho establecimiento"[727], que, siguiendo razonamientos anteriores del propio Tribunal, se extiende a cualquier actividad real y efectiva ejercida con instalación estable; sin que ello signifique la necesariedad de una filial ni sucursal debiendo evaluarse "tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en el Estado miembro de que se trate..."[728]. Remitiéndose para esa apreciación al Tribunal competente de la jurisdicción nacional de que se trate (en este caso austriaca) para determinar "si Amazon EU efectúa el tratamiento de los datos en cuestión en el marco de las actividades de un establecimiento situado en un Estado miembro distinto de Luxemburgo"[729]. Y ello aún cuando fuera en otro estado miembro, remitiéndose al ejemplo expuesto por el Abogado General en sus conclusiones que afirmaba que "si el órgano jurisdiccional remitente demostrara que el establecimiento en el que Amazon EU efectúa el tratamiento de esos datos está situado en Alemania, el Derecho alemán debería regir ese tratamiento."[730]

2.2.2 La sentencia Costeja contra Google y el ámbito de aplicación territorial

La sentencia[731] a la que se viene aludiendo en el propio Reglamento y que quizá ha sido el elemento jurisprudencial de mayor influencia en su redacción, es la sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, surgida en respuesta a petición de decisión prejudicial planteada por la Audiencia Nacional española, y que si bien viene a interpretar preceptos de la Directiva 95/46/CE y los artículo 7 y 8 de la CDFUE, la debemos reseñar aquí por su influencia configuradora en el Reglamento.

[726] Párrafos 72 a 81
[727] Párrafo 74
[728] Párrafo 77
[729] Párrafo 79
[730] Párrafo 80
[731] Sentencia Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Asunto C-131/12.

Sentencia de grandes implicaciones en la privacidad europea y en la conformación del derecho humano a la protección de datos en Europa, implicando no solo la interpretación de la Directiva, sino una más amplia e integral de la CDFUE y del CEDH, elaborando y enlazando un derecho general de contenido y ejercicio mejorado.

El señor Costeja González y la AEPD, demandan a Google, a raíz a de una reclamación previa del interesado a la Agencia en relación con una información suya sobre embargo de sus bienes por deudas con la Seguridad Social de más de 10 años atrás, que aparecía destacada en el periódico La Vanguardia, al incluir sus datos en el global motor de búsqueda. La AEPD desestima la pretensión respecto al periódico catalán ya que estaba amparada por Ley, que exigía ese tipo de publicación en periódicos de gran tirada en su momento, para mayor concurrencia de licitadores a la subasta de esos bienes. En cambio sí estima la reclamación contra Google como responsable de ese tratamiento de datos, que recurre a la Audiencia Nacional, que a su vez realiza al Tribunal de Luxemburgo tres preguntas de largo contenido y alcance iniciando la cuestión prejudicial:

"1) ¿Por lo que respecta a la aplicación territorial de la Directiva [95/46] y, consiguientemente de la normativa española de protección de datos:

a) Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la [Directiva 95/46], cuando concurra alguno o algunos de los siguientes supuestos:

– cuando la empresa proveedora del motor de búsqueda crea en un Estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes del Estado, o

– cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa, o

– cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto

al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria? [732]

2) Por lo que respecta a la actividad de los buscadores como proveedor de contenidos en relación con la [Directiva 95/46]:

a) En relación con la actividad [de Google Search], como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos", contenido en el art. 2.b de la [Directiva 95/46]?

b) En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita:

¿Debe interpretarse el artículo 2.d) de la [Directiva 95/46], en el sentido de considerar que la empresa que gestiona [Google Search] es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?

c) En el caso de que la respuesta anterior fuera afirmativa:

¿Puede la [AEPD], tutelando los derechos contenidos en el art. 12.b) y 14.a) de la [Directiva 95/46], requerir directamente [a Google Search] para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?[733]

d) En el caso de que la respuesta a esta última pregunta fuera afirmativa:

¿Se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene esos datos se haya publicado lícitamente por terceros y se mantenga en la página web de origen?"

[732] En esta misma cuestión se formulan tres preguntas más que se hace innecesario reproducir por agotarse con la contestación del Tribunal a esta letra a).
[733] Esta tercera pregunta la analizaremos en la parte referida al derecho al olvido.

El TJUE, valiéndose de las comprobaciones mercantiles de la Audiencia Nacional sobre Google y su intrincado de filiales tanto por razón de la materia como del territorio, viene a simplificar a Google como responsable del tratamiento, dando la razón a demandantes, a varios Gobiernos personados y a la Comisión. Viene, así, a ser determinante el ejercicio de la actividad y no tanto por el establecimiento de la empresa.[734]

Da además el Tribunal especial relevancia en la interpretación amplia del asunto, precisamente por el valor jurídico de los bienes y derechos en juego. En concreto el derecho a la intimidad. Vincula y resalta ya el objetivo de la Directiva no solo en la instrumentación armoniosa de las legislaciones nacionales para el mejor funcionamiento del mercado común, sino también en la protección eficaz de los derechos fundamentales en Europa.[735]

Y lo hace estableciendo jurídicamente lo obvio: que el negocio (y por tanto la actividad) de Google se está dando en un Estado miembro, estableciendo que ya el propio resultado y surgimiento de la búsqueda es un tratamiento de datos en sí. Vincula, por tanto, plenamente la total aplicación y efectividad de la Directiva al caso que se juzga.[736]

---

[734] Párrafo 47: "El Sr. Costeja González, los Gobiernos español, italiano, austriaco y polaco y la Comisión consideran que, habida cuenta del vínculo indisociable entre la actividad del motor de búsqueda gestionado por Google Inc. y la de Google Spain, ésta debe considerarse un establecimiento de aquélla, en el marco de cuyas actividades se lleva a cabo el tratamiento de datos personales" y par. 52 "...como subrayaron, en particular, el Gobierno español y la Comisión, el artículo 4, apartado 1, letra a), de la Directiva 95/46 no exige que el tratamiento de datos personales controvertido sea efectuado «por» el propio establecimiento en cuestión, sino que se realice «en el marco de las actividades» de éste."

[735] Párrafo 5: "Además, visto el objetivo de la Directiva 95/46 de garantizar una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, ésta expresión no puede ser objeto de una interpretación restrictiva " y par, 54 "...el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se eludiera esta protección, estableciendo un ámbito de aplicación territorial particularmente extenso".

[736] Párrafo 56: "... las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable..." y párrafo 57 "...la propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos..."
Y Párrafo 58: "En tales circunstancias, no se puede aceptar que el tratamiento de datos personales llevado a cabo para el funcionamiento del mencionado motor de búsqueda se sustraiga a las obligaciones y a las garantías previstas por la Directiva 95/46, lo que menoscabaría su efecto útil y la protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas que tiene por objeto garantizar..."

Es, en la respuesta a la segunda cuestión, donde se establece el "alcance de la responsabilidad del gestor de un motor de búsqueda", y se perfila el nuevo ejercicio del derecho a la protección de datos en Europa, en lo que se ha venido a conocer como "Derecho al olvido", que versa sobre la eliminación de la vinculación a una persona con webs y sitios de Internet a través de su nombre. Google aducía que el interesado se dirigiera directamente al sitio de edición de esa información para eliminar esa información, si bien los demandantes y algunos Gobiernos, así como la Comisión, mantienen una posición contraria.[737]

A la respuesta de ello, y previa vinculación de los derechos que se pueden ejercer a la luz de la Directiva en vinculación con los derechos fundamentales (concretamente el derecho de oposición a un tratamiento con las excepciones ponderables de los artículos 7, 12 y 14 de la Directiva), para establecer la significativa incidencia de las búsqueda en Internet en los mismos.[738]

Y no deja en este caso el Tribunal al arbitrio del Juez nacional esta ponderación (como se da en otras sentencias), sino que establece un principio jurisprudencial de prevalencia para la protección de datos de las particulares, con mención solo a las posibles excepciones en personas de relevancia pública. Hace efectiva también la posible intervención de las Agencias de protección y órganos judiciales para estos casos,

[737] Párrafo 65: "El Sr. Costeja González, los Gobiernos español, italiano y polaco y la Comisión consideran que la autoridad nacional puede ordenar directamente al gestor de un motor de búsqueda que retire de sus índices y de su memoria intermedia información que contiene datos personales publicada por terceros, sin dirigirse previa o simultáneamente al editor de la página web. Además, a juicio del Sr. Costeja González, de los Gobiernos español e italiano y de la Comisión, el que dicha información se publicara de forma lícita y que siga figurando en la página web de origen carece de relevancia sobre las obligaciones de dicho gestor con arreglo a la Directiva 95/46. En cambio, para el Gobierno polaco, este hecho le libera de sus obligaciones."

[738] Párrafo 80 "... un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate..."

directamente a los motores de búsqueda y no al editor de la información. Debido también a la propia naturaleza de la información en Internet.[739][740]

Concluye de esta manera el Tribunal en la determinación de una nueva dimensión jurídica en el ejercicio de los derechos de protección, como es el derecho al olvido y que analizaremos separadamente un poco más adelante.

[739] Párrafo 81: "Vista la gravedad potencial de esta injerencia, es obligado declarar que el mero interés económico del gestor de tal motor en este tratamiento no la justifica. Sin embargo, en la medida en que la supresión de vínculos de la lista de resultados podría, en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, es preciso buscar, en situaciones como las del litigio principal, un justo equilibrio, en particular entre este interés y los derechos fundamentales de la persona afectada con arreglo a los artículos 7 y 8 de la Carta. Aunque, ciertamente, los derechos de esa persona protegidos por dichos artículos prevalecen igualmente, con carácter general, sobre el mencionado interés de los internautas, no obstante este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública."

[740] Estando esta sentencia a nuestro entender íntimamente ligada en su razonamiento jurídico a la realidad del momento. Párrafo 84: "...habida cuenta de la facilidad con que la información publicada en un sitio de Internet puede ser copiada en otros sitios y de que los responsables de su publicación no están siempre sujetos al Derecho de la Unión, no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet."

3. El Tratamiento; principios y condiciones para su licitud.

La Directiva vino dejando a los Estados la determinación de la licitud del tratamiento, si bien dentro de los límites del marco de referencia que exige la propia Directiva[741]. Establecía así el artículo 6 de la misma los criterios normativos de calidad de los datos a seguir y a tratar, que, en su apartado 1 vendría a determinar a los Estados los requisitos del tratamiento:

"Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos."

[741] Capítulo II (artículos 5 a 21) que contiene el grueso normativo de la Directiva y el Artículo 5, contemplándose las limitaciones en la sección II del Capítulo.

Artículo, como se puede comprobar, inspirado en los artículos 5 a 8 del Convenio 108 del Consejo de Europa. Nos dice así el artículo 5 del Convenio 108 que los datos objeto de tratamiento:

"a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado."

La legitimidad de esos datos a tratar, por tanto, se configura:

– Respecto al interesado en su previo consentimiento inequívoco, o en su necesariedad para la ejecución de un contrato suscrito por él o para proteger su interés vital.

– En el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.

– Las necesidades de interés público o la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.[742]

[742] Artículo 7 de la Directiva.

El Reglamento no se aparta de los principios marcados por la Directiva y nos enlaza con esa idea del tratamiento, sus requisitos y condiciones necesarias. Que son, al fin, los principios del derecho a la protección de datos, que nos determinan las reglas de recogida, tratamiento y cesión de los mismos, en base a la privacidad del ciudadano. (Puyol Montero, 2016, 135-150)

Ya los Considerandos[743] del Reglamento nos dicen que el tratamiento debe ser lícito, leal y transparente, pasando el Reglamento a definir aún más sus principios y contornos, y sobre todo su relación con el consentimiento que lo avala y los fines del mismo. Es lícito en el caso de que "los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho..."[744], es decir, una base jurídica en sentido amplio[745]. Consentimiento demostrable por el responsable del tratamiento y dado libremente. También es lícito "cuando sea necesario en el contexto de un contrato" o "cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física", y con base en el Derecho de la Unión o de los Estados miembros "se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos."[746]

En el articulado, el Capítulo II del Reglamento viene encargándose de los principios del tratamiento y del consentimiento del mismo. El tratamiento debe cumplir los siguientes principios (artículo 5): los de licitud, lealtad y transparencia, el de minimización de datos, es decir, que los mismos sean adecuados, pertinentes y limitados a los fines del tratamiento. Y ellos junto al tradicional principio de exactitud.

Igualmente se viene a contemplar el principio limitación del plazo de conservación, de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento. Al igual que los principios de integridad y

[743] Considerandos 39 a 50 del Reglamento.
[744] Considerando 40
[745] Según el Considerando 41: "...esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate..."
[746] Considerando 44, 45 y 46

confidencialidad. Por último, el principio de responsabilidad proactiva adquiere una nueva envergadura en el Reglamento.

3.1 Licitud del tratamiento: el consentimiento y la necesidad democrática o legal.

El artículo 6 del Reglamento define la licitud en el tratamiento vinculándola directamente a los siguientes elementos: consentimiento, la obligación legal o contractual, la protección del interés vital del interesado o de otra persona física, para el cumplimiento del interés público o en el ejercicio de poderes públicos y a la satisfacción de intereses legítimos del responsable del tratamiento con el límite de los derechos y libertades fundamentales del interesado; si bien este último se puede salvar para tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Asi, fuera de la condición del consentimiento y de la amparada por el Derecho de la Unión o de los Estados miembros "que constituya una medida necesaria y proporcional en una sociedad democrática",[747] para la validez del tratamiento nos encontramos con las exigidas por la seguridad pública y del Estado, la defensa y demás vinculadas con el ejercicio del poder público, incluyendo la ejecución de demandas civiles[748]. El fin distinto del original del consentimiento recabado, se debe determinar, por tanto, compatible por el responsable del tratamiento ponderando la relación entre los mismos, el contexto, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior y las garantías que se den.

Interesante es, ya en los Considerandos de la Norma, la preeminencia de los derechos y libertades del interesado sobre el interés legítimo del responsable del tratamiento, aún siendo base jurídica para el tratamiento. Ese interés legítimo se va, en todo caso, perfilando en el Reglamento, si bien de manera cautelosa y con ánimo de pormenorización.[749]

[747] Limitación habitual, como hemos apuntado, contenida en el CEDH (ver pag. 200).
[748] El punto 4 del artículo 6 se remite a las enumeradas en el 23.1
[749] Considerando 47: "...Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma

En el importante artículo 6 se observa el tipo general de condicionante al tratamiento y además las múltiples excepciones sobre ese consentimiento que se basan no ya en las propias fijadas en el Reglamento, sino en las que se puedan determinar sobre la base decisoria del responsable del tratamiento, confiando a su ponderación de buen juicio. Aquí la regla básica del funcionamiento de protección comparte mucho del recurso a la excepción legal de casos que vimos en la regulación americana, basada en las necesidades del ágil comercio y del funcionamiento de la autoridad pública.

Las condiciones del consentimiento se completan en el artículo 7, que deberá ser demostrable, por escrito, condición esta que se vincula al contexto, con la posibilidad de retracto en cualquier momento, y libre. Estableciéndose en el artículo 8 las condiciones especiales para el consentimiento de los niños o menores de 16 años, en los cuales la autorización "en relación con la oferta directa a niños de servicios de la sociedad de la información" será del que ejerza la patria potestad o tutela.[750]

3.2 El asunto Huber y las necesidades del interés público[751]

Previamente a la aprobación del Reglamento y en interpretación del artículo 7 de la Directiva (principalmente en su letra e)), nos encontramos con la importante sentencia del Tribunal de Justicia (Gran Sala) de 16 de diciembre de 2008 del asunto Huber contra Alemania. En ella el TJUE viene a interpretar el concepto de "necesidad" pública esgrimido y que podría ser invocado de manera recurrente por los poderes públicos

razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin..." o Considerando 49: "Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales..."

[750] Compárese la diferencia con la COPPA americana que establece la edad de 13 años, si bien ese límite es el que marca el Reglamento hasta el cual cada Estado podrá bajar por ley esa necesidad de autorización.

[751] Sentencia del Tribunal de Justicia (Gran Sala) de 16 de diciembre de 2008. Heinz Huber contra Bundesrepublik Deutschland (Asunto C-524/06)

nacionales en Europa, y que da pie a determinaciones en aspectos de calado relacionados y transversales en la Unión como el principio de no discriminación.

El señor Huber, austriaco residente en Alemania pide la cancelación de sus datos en el Registro Central de Extranjeros alemán. La letra e) del artículo 7 de la Directiva habla del tratamiento de datos que "es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento".

El asunto ofrece implicaciones, no solo en lo relativo a la protección de datos sino en aquellas relacionadas con el desarrollo de la ciudadanía europea y con la libertad de circulación, que, como se observa, están íntimamente relacionadas con aquella. El señor Huber solicitó esa cancelación en el tratamiento porque se consideraba discriminado respecto de los nacionales alemanes, a la hora de ejercitar en suelo alemán su profesión de agente de seguros. Es el Tribunal Superior de lo Contencioso-Administrativo del Land de Norte de Renania-Westfalia el que plantea la cuestión de interpretación del derecho comunitario.

Las preguntas fueron, según recoge la sentencia:

"«1) El tratamiento con carácter general de datos personales de ciudadanos extranjeros de la Unión, en un Registro Central de Extranjeros, ¿es compatible con la prohibición de toda discriminación por razón de la nacionalidad respecto de ciudadanos de la Unión que ejerzan su derecho a circular y residir libremente en el territorio de los Estados miembros (artículo 12 CE, apartado 1, en relación con los artículos 17 CE y 18 CE, apartado 1?

2) ¿Es compatible tal tratamiento con la prohibición de restringir la libertad de establecimiento de los nacionales de un Estado miembro en el territorio de otro Estado miembro (artículo 43 CE, apartado 1)?

3) ¿Es compatible tal tratamiento con] el requisito de necesidad previsto en el artículo 7, letra e), de la Directiva 95/46 ?»"

El Tribunal, tras confirmar estar ante un tratamiento de datos personales en aplicación de la Directiva, entra a analizar el concepto de "necesidad" de la letra e) del artículo 7, para el tratamiento. Recuerda que el objetivo último de la Directiva está en la aproximación de legislaciones y su no conducción a una disminución de las protecciones a los ciudadanos europeos[752]; si bien también asume las limitaciones que "por razones de orden público, de seguridad pública o de salud pública"[753] en las que se pueden escudar los Estados, y declara que "un Registro de ese tipo no podrá contener más información que la que resulte necesaria al mencionado fin" y que para el caso estadístico "tal objetivo requiere únicamente el tratamiento de información anónima".[754] Para interpretar finalmente que[755] "a la luz de la prohibición de toda discriminación por razón de la nacionalidad:

– si contiene únicamente los datos necesarios para la aplicación de dicha normativa por las autoridades mencionadas, y

– si su carácter centralizado permite una aplicación más eficaz de dicha normativa en lo que atañe a los ciudadanos de la Unión que no sean nacionales de dicho Estado miembro." Y continuando en los siguientes párrafos estableciendo una importante determinación de lo que supone el estatuto de ciudadano europeo y la libertad de circulación y de establecimiento aplicadas al caso, y relativas a la no discriminación, y resumido al final de la sentencia en la oposición del Tribunal "a que un Estado miembro instaure, en aras de combatir la delincuencia, un sistema de tratamiento de datos personales específico para los ciudadanos de la Unión que no sean nacionales de dicho Estado miembro."[756]

[752] Párrafos 43 y 46
[753] Párrafo 56
[754] Párrafos 59 y 65
[755] Párrafo 66
[756] Párrafos 69 a 81

3.3 El Consentimiento[757]

Pasamos ahora a detenernos en el concepto y contorno del consentimiento, que siguiendo el Manual de la Agencia Europea de Derechos Fundamentales y del Consejo de Europa (2014) para su validez debe reunir los siguientes requisitos:

"-no se debe haber sometido al interesado a ninguna presión para que diera su consentimiento;

-el interesado deberá haber sido debidamente informado sobre el objeto y las consecuencias de su consentimiento; y

- el ámbito de aplicación del consentimiento deberá ser razonablemente concreto (…)" (ADFUE/CoE, 2014, 61)

Además debe darse "de forma inequívoca. Esto significa que no debería quedar ninguna duda razonable de que el interesado deseaba comunicar su aceptación para permitir el tratamiento de sus datos. La deducción del consentimiento de la simple inactividad no constituye un consentimiento inequívoco, por ejemplo". Y además considera el consentimiento como válidamente libre: "si el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no se consienta" (ADFUE/CoE, 2014, 62).

Sigue apuntando el Manual (2014, 64) que sobre el carácter informado del consentimiento: "el interesado deberá contar con la suficiente información antes de tomar su decisión. El que la información sea suficiente sólo puede determinarse caso por caso. Normalmente, el consentimiento informado incluirá una descripción precisa y fácilmente comprensible de la cuestión que requiere dicho consentimiento y, además, un resumen de las consecuencias del consentimiento o de la falta del mismo…"Así como el de su característica de específico: "para que sea válido, el consentimiento también debe

[757] Sobre la figura del consentimiento es interesante la consulta de la opinión del Grupo del artículo 29 (2011)

ser específico. Esto va estrechamente unido a la calidad de la información que se facilita sobre el objeto del consentimiento" (ADFUE/CoE, 2014, 65).[758]

Sobre el consentimiento y sus límites, la sentencia del Tribunal de Justicia (Sala Tercera) de 24 de noviembre de 2011[759] resuelve cuestión prejudicial presentada por el Tribunal Supremo español e interpreta el artículo 7, letra f) en relación con el efecto directo de la Directiva e implicando a la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su instrumento ejecutivo de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre.[760]

Las dos entidades consideran que hay un requisito añadido por el Real Decreto en infracción del artículo 7 f) de la Directiva: el de que los datos consten en fuentes accesibles al público como excepción al consentimiento inequívoco del interesado, y así el TS invoca la cuestión al TJUE.

La síntesis de las preguntas es: " 1) ¿Debe interpretarse el artículo 7, letra f), de la Directiva 95/46 […] en el sentido de que se opone a una normativa nacional que, no mediando consentimiento del afectado y para permitir el tratamiento de sus datos de carácter personal que resulte necesario para satisfacer un interés legítimo del responsable o de los terceros a los que se vayan a comunicar, exige además de que no se lesionen los derechos y libertades fundamentales de aquel que los datos consten en fuentes accesibles al público?

2) ¿Concurren en el mencionado artículo 7, letra f), las condiciones que exige la jurisprudencia del Tribunal de Justicia [...] para atribuirle efecto directo?"[761]

Para la primera pregunta, y recordando el Tribunal de Luxemburgo que el octavo considerando de la Directiva es el de "equiparar el nivel de protección de los derechos y libertades de las personas por lo que se refiere al tratamiento de datos personales en

[758] Referenciando además en apoyo de la argumentación la sentencia del TJUE, en el asunto C-543/09, Deutsche Telekom AG contra Alemania, de 5 de mayo de 2011.
[759] Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado. Asuntos acumulados C-468/10 y C-469/10
[760] Concretamente en los artículos 3j) y 6.1 de la L.O. sobre fuentes accesible al público y el consentimiento del afectado para el tratamiento de sus datos y el 10 del Reglamento del 2007 igualmente referido a ese consentimiento en su desarrollo.
[761] Párrafo 22.

todos los Estados miembros" así como que "la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa"[762]; afirma el Tribunal que los parámetros del marco del artículo 7 deben ser respetados precisamente por ese fin armonizador de la Directiva en la protección de datos en Europa. Llegando el Tribunal a la interpretación inequívoca de que el 7 f) de la Directiva se opone a esa normativa nacional en el sentido expuesto por construir y excluir categorías de datos (las establecidas en fuentes accesibles al público).[763] Y para establecer el efecto directo de la letra f) del artículo 7 como "una disposición suficientemente precisa para poder ser invocada por un particular y aplicada por los órganos jurisdiccionales nacionales".[764]

Podemos decir que, en este caso, el Tribunal interpreta una "pasada de frenada" garantista por parte del legislador español, en la protección de la privacidad, que escapa al fin de armonización, que precisamente persigue la Directiva. Recuerda así, que Europa se construye con la generación de derechos pero a un ritmo similar, en bloque, a pesar de la posible ralentización de la defensa de la privacidad, en este caso, de los españoles.

Esta línea legislativa de "regla de equilibrio de intereses" se sigue sustancialmente, como hemos visto, por el artículo 6 del Reglamento, que no debía separarse mucho en este sentido del artículo 7 f) de la Directiva, ya que como acabamos de comprobar en esta sentencia, el Tribunal de Justicia le otorga efecto directo.[765]

[762] Párrafos 28 y 29 remitiéndose a la sentencia Lindqvist y Párrafo 32.

[763] Párrafo 41 y párrafo 42 que nos dice "debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes."

[764] Párrafos 52 a 55.

[765] En este sentido resulta de interés la respuesta de la AEPD en informe de su Gabinete Jurídico (número 0195/2017) al respecto planteada por la Asociación Española de Banca.

3.4 Categorías especiales de tratamientos.

El Reglamento se encarga, en su artículo 9, del tratamiento de las categorías especiales de datos personales cuya norma general es la prohibición de tratamiento con sus excepciones de aplicación. Los datos afectados por esa prohibición son aquellos "que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos", siempre que se dirijan a identificar a una persona física, o los "datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales" en todo caso.

Las excepciones que salvan esa prohibición son equivalentes a las establecidas para el artículo 6, con algunos añadidos a los contenidos en él, como que sean tratados por "fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical"; o sean "datos personales que el interesado ha hecho manifiestamente públicos",[766] o por necesidades de interés público específicas propias de la medicina o de la salud pública. Dejando el artículo abierta la puerta a los Estados para mayor restricción en cuanto a datos genéticos, datos biométricos o datos relativos a la salud.[767]

Este artículo 9 coincide esencialmente con el artículo 8 de la Directiva en su categorías especiales de datos en sus tratamientos, que prohíbe igualmente los que revelen origen, convicciones políticas, religiosas, pertenencia a sindicatos o relativos a salud o sexualidad. Igualmente recoge su posibilidad de excepción por consentimiento explícito o para la protección de derechos u obligaciones laborales o el interés vital del interesado u otra persona o "el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical" o "el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos, o

[766] Letras d) y e) del artículo 9.1

[767] Letra i) del artículo 9.1. Así el artículo 9.4:"Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial"[768][769]

También se excluye la prohibición para los datos médicos cuando lo justifique el diagnóstico o la prestación médica o la gestión de los servicios sanitarios, o en general por los Estados por motivos de interés público importantes (apartados 3 y 4 del artículo 8).

Los artículos 10 y 11 del Reglamento reconocen la especialidad del tratamiento de los datos "relativos a condenas e infracciones penales" y de los que "no requieren o ya no requieren la identificación de un interesado por el responsable". Sólo podrá llevarse a cabo el primer caso "bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados". Y para el segundo "no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación."[770]

Especialidad que ya se revestía en la Directiva en "el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad" y aquellos "con fines exclusivamente periodísticos o de expresión artística o literaria."[771]

3.5 El tratamiento y la libertad de expresión y de información.

La excepción relativa al derecho de información y su tratamiento especial a la que acabamos de referirnos (fines periodísticos y expresión artística) se mantiene en el Reglamento, si bien como situación específica de tratamiento y a través de los Estados, en un obligado llamamiento a los mismos para su conciliación, pasando esta clave de

[768] Letras de a) a e) del punto 2 del artículo 8 de la Directiva.
[769] Igualmente sobre la coincidencia del artículo 8 con el artículo 6 del Convenio 108 respecto al reconocimiento de esos especiales datos "sensibles" tenemos la opinión del Grupo del artículo 29 (2011)
[770] El Derecho de la Unión se encarga de esta especialidad del artículo 10 en el propio paquete de protección de datos teniendo como resultado la Directiva 2016/680 sobre protección de datos en el ámbito de las infracciones penales, de la que nos ocuparemos más adelante.
[771] Apartado 5 del artículo 8 y artículo 9

bóveda de relación entre derechos a la actuación legal nacional. Así lo establece en su artículo 85 (alejado del artículo 9 en la estructura normativa): "los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria."

Y ello se realiza incorporando esa actuación nacional debida al Reglamento, por la delimitación interpretativa del Tribunal de Justicia. Así, siendo esta relación un tema recurrente en la protección de datos europea, pondremos como ejemplo jurisprudencial importante sobre estos aspectos, y enmarcado en las previsiones del artículo 9 de la Directiva, la sentencia del Tribunal de Justicia (Gran Sala) de 16 de diciembre de 2008 en el caso Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy (Asunto C-73/07).[772]

La petición parte del Tietosuojavaltuutettu finlandés (mediador encargado de la protección de datos), y la Tietosuojalautakunta finlandesa (comisión de protección de datos), por tratamientos de datos en su actividad de supervisión de actividades llevadas a cabo por las dos empresas que se relacionan en la sentencia (Markkinapörssi Oy asi como Satamedia yo). Tras sucesivas instancias es el *Korkein hallinto-oikeus* (Tribunal Supremo de lo contencioso-administrativo) el que plantea la cuestión prejudicial. La Comisión y los gobiernos finlandés, estonio, portugués y sueco presentan asimismo observaciones.

El litigio principal versa sobre la posible contradicción entre las exigencias de privacidad de la Directiva y el derecho a la información de tipo fiscal de los ciudadanos. Una contradicción que se manifiesta entre la Ley finlandesa de transposición y la Ley de Publicidad de las actividades de la Administración Pública (entre las que se encuentra la actividad tributaria).[773]

[772] Petición de decisión prejudicial planteada por el Korkein hallinto-oikeus de Finlandia, que interpreta el articulo 9 y el 3.1 de la Directiva.

[773] Ley sobre los datos personales [henkilötietolaki (523/1999)], de 22 de abril de 1999 y la Ley sobre la publicidad de las actividades de la Administración [laki viranomaisten toiminnan julkisuudesta (621/1999)], de 21 de mayo de 1999, respectivamente.

Las empresas implicadas tenían, como actividad principal, suministrar ese tipo de información a un periódico especializado en publicar ese tipo de información fiscal del contribuyente finlandés, cobrando por ese servicio de "intermediación informativa". Aquellas al periódico y el periódico a los usuarios interesados en la misma.

La pregunta del alto Tribunal finlandés es la siguiente:

"1) ¿Puede considerarse "tratamiento de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva […] la actividad consistente en:

a) recoger tales datos de los documentos públicos de la administración fiscal relativos a los rendimientos del trabajo y del capital y al patrimonio de las personas físicas, y tratarlos para su publicación,

b) publicarlos por orden alfabético y por tipos de rentas, en listas pormenorizadas clasificadas por municipios,

c) cederlos en discos CD-ROM para que sean utilizados con fines comerciales,

d) tratarlos en un servicio de mensajes de texto (SMS) que permite a los usuarios de teléfonos móviles, enviando el nombre y el municipio en el que reside una persona física, recibir información relativa a los rendimientos del trabajo y del capital, así como al patrimonio de esa persona?

2) ¿Debe interpretarse la Directiva […] en el sentido de que puede considerarse que las diversas actividades mencionadas anteriormente en la cuestión 1, letras a) a d), constituyen un "tratamiento de datos personales realizado con fines exclusivamente periodísticos", en el sentido del artículo 9 de la Directiva, si se tiene en cuenta que los datos que se han recogido, y que se refieren a más de 1.000.000 de contribuyentes, proceden de documentos que son públicos en virtud de la normativa nacional sobre acceso a la información? ¿Es pertinente para el análisis del presente asunto el hecho de que la finalidad primordial de dicha actividad consista en publicar los datos de que se trata?

3) ¿Debe interpretarse el artículo 17 de la Directiva […], en relación con los principios y la finalidad de la Directiva, en el sentido de que se opone a la publicación de datos que se han recogido con fines periodísticos y a su cesión con fines comerciales?

4) ¿Puede interpretarse la Directiva […] en el sentido de que quedan totalmente excluidos de su ámbito de aplicación los ficheros nominativos que únicamente contienen información ya publicada tal cual en los medios de comunicación?".

El Tribunal va desgranando en sus respuestas la pregunta. En primer lugar, establece el carácter inequívoco de encontrarnos ante datos personales y un tratamiento de los mismos.[774] Para seguir contestando a la cuarta pregunta en el sentido de que esa posible excepción (ya que es uno de los casos en los que no se aplicaría la Directiva), apreciando que esas actividades de excepción del 3.2 en el primer guión del precepto "son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares...", y en el segundo guión "actividades que se inscriben en el marco de la vida privada o familiar de los particulares". Para concluir que no están comprendidas en ese marco de excepción de la Directiva.[775]

Para la segunda pregunta, y que afecta a la interpretación del artículo 9 de la Directiva, el Tribunal dilucida sobre si estamos ante "actividades de tratamiento de datos personales ejercidas exclusivamente con fines periodísticos". En su contestación el Tribunal se remite a su línea de interpretación de que esa conciliación entre la libertad de información y la protección de datos corresponde apreciarlas y ejercerlas a los distintos estados miembros[776]. Si bien establece algunas consideraciones al respecto, como son que "las exenciones y excepciones previstas en el artículo 9 de la Directiva se aplican no sólo a las empresas de medios de comunicación, sino también a toda persona que ejerza una actividad periodística", y que, en principio, el "hecho de que se publiquen datos personales con ánimo de lucro" no lo excluye. Considera además "el soporte en el que se transmiten los datos" como no determinante para esa apreciación en

[774] Párrafos 35 a 37
[775] Párrafos 41 y 42
[776] Estas determinaciones coinciden sustancialmente con las Conclusiones de la Abogado General Juliane Kokott, presentadas el 8 de mayo de 2008.

estos tiempos. Para concluir que las actividades del litigio principal sí están ubicadas como actividad exclusivamente periodística de la prevista en el artículo 9 de la Directiva.[777]

Debemos seguir apuntando aquí que la construcción jurisprudencial de la protección de datos se sigue sustanciando, hasta esa fecha, como elemento de armonización del mercado común, sin mayor implicación jurídica de los derechos fundamentales en su justificación y objeto normativo. Así, como nos dice la profesora González Fuster (2012, 52) "el Tribunal de Justicia ha tratado casi siempre la interpretación de la normativa de protección de datos de la UE sin referirse en absoluto a la existencia de un derecho fundamental a la protección de datos de carácter personal de la UE. El derecho brilla por su ausencia en el instrumento jurídico más importante sobre protección de datos jamás aprobado por la UE".

[777] Párrafos 58 a 62

4. Los Derechos del interesado.

Los clásicos derechos de acceso, rectificación, cancelación y oposición, conocidos por su ya también clásico acrónimo "ARCO", vienen a ser el conjunto armonizado de derechos que conectan directamente a los ciudadanos con su capacidad de control sobre sus datos y el tratamiento de los mismos. Definiéndolos de manera elocuente y certera el Tribunal Constitucional español como el "haz de facultades que integra el contenido del específico derecho fundamental a la protección de datos personales".[778]

El Capítulo III del Reglamento[779] se ocupa de los derechos del interesado, y además de estos clásicos derechos ARCO de la protección de datos, observa algunas determinaciones conectadas, como la vinculada transparencia del tratamiento, y las limitaciones a los mismos.

Elementos que siguen de cerca las valoraciones del segundo Dictamen del SEPD (2015) sobre el Reglamento, que enfocaba su consejo principalmente hacia "el aumento de la transparencia, unos derechos de acceso y una portabilidad de datos más avanzados y unos mecanismos de exclusión efectivos sentarán las bases y serán una condición previa para que los usuarios puedan ejercer un mayor control sobre sus datos, además de contribuir a unos mercados más eficientes para los datos personales, que beneficien tanto a los consumidores como a las empresas..."[780]

El Reglamento también se encarga, en sus Considerandos, de desgranar estos derechos de acceso, rectificación, supresión y oposición, para contemplar directamente el "derecho al olvido" como medio de ampliación del derecho de supresión[781]. Se reconoce además la portabilidad de datos como novedad y con el reforzamiento de su garantía para el usuario permitiéndosele que lo "reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del

[778] Sentencia 292/2000, de 30 de noviembre de 2000.
[779] Artículos 12 a 23.
[780] Puntos 6.1 y 6.2 del Resumen Ejecutivo del Informe SEPD (2015).
[781] A partir del Considerando 59. Principalmente en el Considerando 66.

tratamiento...".[782] También se contempla de manera directa la opción de oposición "si los datos personales son tratados con fines de mercadotecnia directa" o a la elaboración de perfiles basados en sus datos. Estos derechos tendrán sus consiguientes limitaciones y restricciones siempre con arreglo "a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales".[783]

4.1 Limitaciones

Las limitaciones suponen un espacio común en el Capítulo del Reglamento[784] para los derechos en él contenidos, cuando "tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática", para lo siguiente: salvaguardar la seguridad, la defensa, la prevención, investigación, detección o enjuiciamiento de infracciones penales y su ejecución, otros objetivos importantes de interés público general de la Unión o de un Estado miembro[785], la independencia judicial, las normas deontológicas en las profesiones reguladas, la función, aún ocasional, de autoridad pública, la protección del interesado o de los derechos y libertades de otros y por último incluso la ejecución de demandas civiles.

Estas limitaciones del artículo 23 del Reglamento responden, como ya hemos visto también en la parte dedicada al CEDH y a la CDFUE, al carácter del derecho a la protección de datos como derecho limitado. Esa premisa se recoge ya también en la Directiva, donde además se observa esa limitación, al igual que en el Reglamento, en base al derecho prevalente de otros.[786]

[782] Considerando 67: "Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet..."
[783] Considerando 70 a 73.
[784] Sección 5 (artículo 23).
[785] Es de destacar el particular economicismo dado a ese interés público, ya que continúa con "en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social".
[786] Ver Artículo 9 del Convenio 108.

El artículo 13 de la Directiva, que vendrá a reproducir sustancialmente el artículo 23 del Reglamento, es el que establece en aquella la posibilidad de excepción, tan habitual por otro lado en la legislación americana, y que por la materia podríamos ubicar como determinación de excepción general en la protección de la privacidad. Las limitaciones se podrán esgrimir por los Estados cuando se afecte a la salvaguardia de:

"a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) la función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas."

En relación con estas excepciones y limitaciones debemos citar la sentencia del Tribunal de Justicia (Sala Tercera) de 7 de noviembre de 2013. Institut professionnel des agents immobiliers (IPI) contra Geoffrey Englebert y otros (Asunto C-473/12).[787]

Sentencia motivada por la demanda del IPI, un organismo cercano a lo que se puede entender por un Colegio Profesional de Agentes Inmobiliarios, que tiene además capacidad, en el ejercicio de sus funciones, para contratar detectives privados en sus labores de investigación. El señor Englebert, junto con otros, se ve afectado por un procedimiento de este tipo, dejando la duda en el Tribunal mercantil de Charleroi sobre el valor probatorio en este tipo de procedimientos, preguntando al Tribunal Constitucional belga, que a su vez se lo cuestiona al TJUE a la luz de la Directiva.

[787] Petición de decisión prejudicial por la Cour constitutionnelle de Bélgica

Y lo hace de la siguiente forma: "1) ¿Debe interpretarse el artículo 13, apartado 1, letra g), in fine, de la Directiva [95/46] en el sentido de que deja a los Estados miembros la libertad de prever –o no– una excepción a la obligación de información inmediata establecida en el artículo 11, apartado 1, cuando esta excepción resulte necesaria para proteger los derechos y libertades de terceros o[, por el contrario,] los Estados miembros están sometidos a restricciones en esta materia?

2) Las actividades profesionales de los detectives privados, reguladas por el Derecho interno y ejercidas al servicio de autoridades habilitadas para denunciar ante los tribunales cualquier infracción de las disposiciones que protegen un título profesional y regulan una profesión, ¿están comprendidas, según las circunstancias, en la excepción prevista en el artículo 13, apartado 1, letras d) y g), in fine, de la Directiva [95/46]?

3) En caso de respuesta negativa a la segunda cuestión, ¿es compatible el artículo 13, apartado 1, letras d) y g), in fine, de la Directiva [95/46] con el artículo 6 [TUE], apartado 3, y más concretamente con el principio de igualdad y de no discriminación?"

Tras declarar el Tribunal la pertinencia interpretativa de los artículos citados para el caso en cuestión (primera pregunta) resuelve lo sustancial de las otras dos en el encuadre de excepción que posibilita el artículo 13 apartado 1 letra d) de la Directiva[788], pero precisamente por tratarse del encargo de un organismo regulado y regulador de los agentes de la propiedad inmobiliaria, y particularmente por ese carácter que se le da en Bélgica al organismo IPI y a sus funciones.[789]

[788] Párrafo 47 "...Sería imposible que los detectives privados ejercieran eficazmente su actividad al servicio del IPI si tuvieran que divulgar su identidad y los motivos de sus investigaciones antes incluso de interrogar a las personas a quienes investigan..."

[789] Párrafo 50: "...es preciso señalar que las normas relativas al acceso a una profesión regulada forman parte de las normas de deontología. De ello se deduce que las investigaciones sobre las actuaciones de personas que infringen dichas normas haciéndose pasar por agentes inmobiliarios están comprendidas en el ámbito de aplicación de la excepción establecida en el artículo 13, apartado 1, letra d), de la Directiva 95/46."

Lo interesante de la sentencia es que, por un lado, califica a las excepciones del artículo 13 en su transposición por los Estados como facultativas y no obligadas, en la medida en que restringen por determinada razón nacional el derecho que pretende armonizar la Directiva. Y por otro, se refiere a elementos de "externalización" para esa función pública de prevención e investigación de las infracciones contrarias a la deontología en las profesiones reglamentadas, que también viene amparada en la extensión de esa excepción.

4.2 El derecho de información y de acceso.

El artículo 13 y 14 del Reglamento fijan la información que debe suministrase en cuanto a la existencia del tratamiento y los datos afectados por él, diferenciándose si la misma se ha obtenido del interesado o no. Con una información de suministro preceptivo al interesado (13.1 y 14.1). Y otra también necesaria relacionada con los principios de lealtad y transparencia (13.2 y 14.2), estableciéndose además la forma de suministro en el segundo caso (14.3), destacando su "plazo razonable" como idea principal. El 14.5 presenta los casos en que no se aplican las previsiones del artículo, como son que el interesado ya disponga de la información, que la comunicación de la misma "resulte imposible o suponga un esfuerzo desproporcionado", o "esté expresamente establecida por el Derecho de la Unión o de los Estados miembros", o la información deba seguir siendo confidencial.[790]

El derecho de acceso que implica el "derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen", y siendo así, el acceso a los mismos está contenido en el artículo 15 del Reglamento e implica conocer los fines del tratamiento, las categorías de los datos implicados y sus destinatarios, el plazo previsto de conservación de los datos, la posibilidad de rectificación y el derecho a la misma, así como el de reclamación a la autoridad de control, información sobre datos no obtenidos del interesado y la existencia de "decisiones automatizadas, incluida la elaboración de perfiles". Igualmente tendrá

[790] En este sentido resulta interesante consultar a Hernández Corchete (2016)

derecho a información sobre transferencia internacional de los datos y a obtener copia del tratamiento de los datos.

La Directiva ya regulaba la información que debe darse al interesado en caso de que el tratamiento y los datos necesarios se recaben de él directamente o no. Coincide en la identidad del responsable del tratamiento, los fines del mismo y otra información tal y como los destinatarios o la existencia de derechos de acceso y rectificación.

Además, venía a consagrar el derecho de acceso de los interesados a sus datos y la obligación de la atención a su ejecución al responsable del tratamiento. En el que se incluye el derecho de rectificación y supresión o bloqueo.[791]

Así, el artículo 12 a) de la Directiva habla de "los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

— la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen..."

Si bien, como nos explica el Manual de la Agencia de Derechos Fundamentales y el Consejo de Europa (2014, 119), respecto al derecho de información "la Directiva no deja claro si el derecho de acceso a la información concierne al pasado y, en su caso, a qué periodo del pasado. En ese sentido, tal como ha subrayado la jurisprudencia del TJUE, el derecho de acceso a los propios datos no puede quedar limitado de forma indebida por limitaciones temporales"

Este derecho de acceso e información se ha visto interpretado de manera importante por el Tribunal de Justicia. Podremos establecer varios casos en los que el Tribunal de Justicia ayuda a perfilar los contornos de este derecho.

[791] Artículos 10, 11 y 12

Como primer ejemplo interpretativo relacionado con este derecho citaremos la sentencia del Tribunal de Justicia (Sala Tercera) de 7 de mayo de 2009, en el caso College van burgemeester en wethouders van Rotterdam/E.E. Rijkeboer (Asunto C-553/07).[792]

La sentencia se produce en interpretación del artículo 12 de la Directiva, que regula el marco de ese derecho de acceso. El señor Rijkeboer, en base a la norma de tipo general de transposición y Ley relativa a la protección de datos personales holandesa (Wet bescherming persoonsgegevens), solicita al ayuntamiento de su municipio de residencia anterior (College van burgemeester en wethouders) "una relación de todas las comunicaciones a terceros de información relativa a él, procedente de la base de datos de padrón municipal, efectuadas durante los dos años anteriores a su petición". Resulta que la Ley reguladora del Padrón en los Países Bajos establece el límite temporal de un año para ese tipo de acceso al tratamiento de datos. Y ahí se muestra servido el litigio, con reclamación del ciudadano, recurso judicial posterior, planteándose de esa manera la duda europea del Tribunal neerlandés.

Expresándola así: "La limitación legal de la comunicación de datos al año anterior a la solicitud, ¿es compatible con el artículo 12 […] letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos y a su libre circulación, interpretado en relación con el artículo 6, apartado 1, letra e), de la citada Directiva y con el principio de proporcionalidad?"

El Tribunal, tras una serie de consideraciones sobre los datos en juego y el tipo de tratamiento de datos que se presenta en el caso, entra directa y claramente en la interpretación del artículo 12. Establece que corresponde a los Estados fijar ese equilibrio de excepción que la suficiente flexibilidad de la Directiva les permite. En este caso referido al plazo que pueda considerarse una carga excesiva para el responsable del tratamiento de los datos. Y al Juez nacional la apreciación de esa conveniencia.[793]

[792] Petición de decisión prejudicial planteada por el Raad van State (Países Bajos)
[793] Párrafos 62 a 64

Si bien esta vez sí entra el Tribunal en interpretar que el espíritu del artículo de la Directiva va referido a que el derecho de acceso pueda ejercitarse no solo para los datos que están siendo objeto de tratamiento en el presente (como alegaban el College, y los gobiernos neerlandés, checo, español y del ReinomUnido), sino también para el tratamiento en el pasado (tal y como propugnaban la Comisión y el Gobierno griego). Y sobre todo que para el caso concreto "una normativa que limita la conservación de la información sobre los destinatarios o las categorías de destinatarios de los datos y el contenido de los datos transmitidos, al período de un año, limitando correlativamente el acceso a dicha información, si bien los datos principales se conservan durante mucho más tiempo, no constituye un justo equilibrio entre el interés tutelado y la obligación discutida, a menos que pueda demostrarse que un período de conservación más largo constituiría una carga excesiva para el responsable del tratamiento. Corresponde al juez nacional efectuar las comprobaciones necesarias." Deja así clara la contradicción de ese límite temporal estatal con el espíritu de la norma europea.[794]

Otro ejemplo lo tenemos en la sentencia del Tribunal de Justicia (Sala octava) de 12 de diciembre de 2013 (Asunto C-486/12). Del demandante X contra Países Bajos.[795]

El demandante, que prefiere mantenerse en el anonimato, trata de ejercer su derecho a conocer si existe un tratamiento de sus datos por parte de un responsable en el tratamiento de los mismos. En este caso un municipio holandés y en relación con una infracción de tráfico de esta persona. En la Ley neerlandesa y para estos casos se prevé el cobro de una tasa por la certificación administrativa del órgano municipal. Tras sucesivos recursos llega la cuestión por parte del Tribunal preguntado sobre si se puede entender excesiva la tasa que se plantea en el procedimiento administrativo.

[794] Párrafo 70: "...Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a ésta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la Directiva y, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento..."
Interpretación garantista que va más allá de las incompatibilidad condicionada de ese plazo que expresa el Abogado General Dámaso Ruiz-Jarabo Colomer en su escrito de conclusiones presentadas en fecha 22 de diciembre de 2008.

[795] Petición de decisión prejudicial planteada por el Gerechtshof te 's-Hertogenbosch de Países Bajos

Así las cosas el Tribunal entra a reflexionar jurídicamente (indirectamente) sobre la importancia de la traducción jurídica en la construcción del Derecho de la Unión. Al establecer que el término neerlandés para excesivo podría conducir a error. No dándose esa circunstancias en las demás versiones traducidas de la Directiva.[796]

Si bien una única versión lingüística de la Directiva aprecia el Tribunal, siendo algo reiterado, no puede ser aval de interpretación de la misma, precisamente por la necesidad de uniformidad del Derecho de la Unión. Establece que en versiones distintas a la lengua neerlandesa de la Directiva y de las mismas, no se puede deducir el carácter gratuito del ejercicio de ese derecho del ciudadano[797], interpretándose la Directiva "en el sentido de que no se opone a la percepción de gastos por la comunicación de datos de carácter personal por una autoridad pública."[798]

Pasa así el Tribunal a contestar sobre qué gastos pueden considerarse excesivos para el ejercicio del derecho de conocimiento y acceso del artículo 12. Esos criterios se dejan al buen arbitrio de los Estados, si bien con la determinación de que no constituyan un obstáculo a su ejercicio. Para realizar, acto seguido, un contorno de interpretación bastante aproximado en que "para garantizar que los gastos percibidos con ocasión del ejercicio del derecho de acceso a los datos de carácter personal no sean excesivos a efectos de esa disposición, el importe de esos gastos no debe exceder el coste de la comunicación de dichos datos".[799]

Por último, citaremos la sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015[800], en la que se interpretan los artículos 10 y 11 de la Directiva, referidos a la información a los interesados, en relación con las excepciones y limitaciones del

[796] Párrafo 18: "Es preciso observar que la versión en lengua neerlandesa del artículo 12, letra a), de la Directiva 95/46 utiliza la expresión «bovenmatige vertraging of kosten». Esa formulación podría dar a entender que el término«bovenmatige» («excesivo») se refiere únicamente a los plazos («vertraging»), sugiriendo así que el derecho a obtener la comunicación de las informaciones previstas en esa disposición debería poder ejercerse sin gastos."
[797] Párrafos 19 y 20.
[798] Párrafo 23.
[799] Párrafo 31.
[800] Asunto Smaranda Bara y otros contra Președintele Casei Națională de Asigurări de Sănătate y otros. Petición de decisión prejudicial planteada por la Curtea de Apel Cluj, (asunto C-201/14).

Artículo 13 (concretamente en lo establecido para la transmisión por una administración pública de un Estado miembro de datos fiscales personales para su tratamiento por otra administración pública).

El caso proviene de un litigio entre la señora Bara y la Caja Nacional del Seguro de Enfermedad rumana (Aseguradora pública) y la Agencia Tributaria de aquel país, y en relación con la legalidad de la transmisión de los datos fiscales relativos a sus ingresos en concepto de pago de atrasos de cotizaciones al régimen de seguro de enfermedad.

El tribunal de apelación rumano plantea cuatro dudas jurídicas al TJUE, que, tras declarar la inadmisibilidad de las primeras tres cuestiones, responde sobre la pertinencia de esa transmisión de datos entre organismos públicos en la cuarta[801] pregunta:

"¿Puede tratar los datos personales una autoridad que no era destinataria de los mismos, si dicha operación crea, de modo retroactivo, un perjuicio patrimonial?"

En cuanto a la respuesta, el Tribunal va dejando meridianamente claro la necesidad de informar de la transmisión y del tratamiento de datos al interesado por parte de los organismos públicos implicados en su gestión, quedando fuera el caso de las excepciones contempladas en el artículo13. Concluye que no está, de esa forma, amparada la normativa rumana en litigio, y en el sentido que ocupa a la sentencia, por esas posibles excepciones nacionales, y declara el TJUE aquellas opuestas a los artículos de la Directiva.

Incidencia especial hace esta sentencia en que las normativas nacionales "que permiten a una administración pública de un Estado miembro transmitir datos personales a otra administración pública y el subsiguiente tratamiento de esos datos, sin que los interesados hayan sido informados de esa transmisión ni de ese tratamiento", son contrarias al dictado de la Directiva.[802]

[801] Las tres primeras se declaran inadmisibles "por no guardar relación con el objeto del litigio principal".
[802] Párrafo 46.

4.3 El Derecho de oposición.

El derecho de oposición del interesado al tratamiento de sus datos, así como el de no verse afectado en sus derechos ("no verse sometidas a una decisión con efectos jurídicos sobre ellas"), por ese tratamiento se recogen ya expresamente en la Directiva[803]como obligaciones concretas para los Estados. Si bien se permite cuando los intereses del interesado no se pongan en juego, porque "se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo"; o "esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado."[804]

La sentencia Costeja contra Google marca un hito en la interpretación del artículo 14 de la Directiva y de los derechos de oposición y de supresión, llevándolos a un nuevo estadio, que se ha venido a conocer como "derecho al olvido". Debido a las nuevas puertas que abre la sentencia y a su recogida explícita en el REPD, nos remitimos a esa parte del trabajo para su estudio. Si bien debemos apuntar algunos elementos que se vinieron dando previamente en pronunciamientos sobre el alcance de estos derechos, concretamente por el Consejo de Europa.

Así, sobre el derecho de oposición a las decisiones individuales automatizadas resulta interesante el pronunciamiento sobre el perfilado por parte del Comité de ministros del Consejo de Europa, en la Recomendación (2010) 13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento

[803] Artículos 14 y 15.

[804] Apartado segundo del artículo 15

El Artículo 14 de la Directiva en opinión de Heredero Higueras (1997, 153) "no define un derecho general del interesado a oponerse al tratamiento de los datos sino (...) a dos supuestos o modalidades de un posible derecho general de oposición..." Siendo el derecho general propio del derecho francés y que es sustituido por dos modalidades específicas.

automatizado de datos de carácter personal en el contexto de la creación de perfiles. Concretamente en su artículo 5, apartado 5.[805]

Vemos que la Directiva establece un derecho específico de oposición, con un artículo concreto, al uso de sus datos con fines de marketing directo en la letra b) del artículo 14. Marcando una pauta que se convierte en tradición jurídica ya en el REPD.

Respecto a este derecho, a pesar de su novedad en su introducción en el Derecho Derivado europeo, parece seguir la Recomendación sobre marketing directo del Consejo de Europa, de mediados de los años 80: Recomendación Rec (85)20 a los Estados miembros sobre la protección de los datos personales utilizados con fines de marketing directo, de 25 de octubre de 1985, con particular atención a lo establecido en el artículo 4.1.[806]

4.4 El Derecho de rectificación y el de supresión. Especial referencia al Derecho al olvido.

El Reglamento en su artículo 16 se encarga del derecho de rectificación[807]y en su artículo 17 del de supresión, incluyéndose en él como categoría diferenciada del mismo el "derecho al olvido", que se caracteriza como un derecho de supresión con consideración especial.

La supresión deberá realizarse sin dilación indebida en las siguientes circunstancias por el responsable del tratamiento: cuando los datos "no sean necesarios en relación con los fines" o se retire el consentimiento por el interesado.

[805] Recuperado el 27 de agosto de 2018: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd2a

[806] Principalmente en su artículo 21 y con referencia expresa en los Considerandos 50, 59,73 y 156 Recuperado el 27 de agosto de 2018l: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336

[807] En la Directiva no había un artículo específico para el derecho de rectificación.

También en el caso de que el interesado se oponga, y no haya motivos legítimos prevalentes para su tratamiento, o bien en el supuesto de que los datos se hayan tratado ilícitamente, o bien cuando deban suprimirse por una obligación legal. Por último, debemos señalar el caso de los datos obtenidos “en relación con la oferta de servicios de la sociedad de la información” de los niños.

El derecho al olvido, cuya denominación específica como tal fue rechazada por el Parlamento Europeo en la tramitación del Reglamento, tiene una importancia práctica de gran calado, ya que podrá permitir por ejemplo la supresión de los datos en redes sociales cuando los usuarios de den de baja del servicio (Álvarez Caro, 2016, 255).

La autora Mónica Arenas Ramiro (2014, 332) nos perfila este ejercicio del derecho a la protección de datos en su vertiente del derecho al olvido. Sin destacarlo como nuevo derecho, ya que se remonta a Francia y a una sentencia de su corte de casación de 20 de noviembre de 1990. Ofreciéndonos la visión, con la que coincidimos, de que estaríamos ante una nueva facultad y no ante un nuevo derecho en sí mismo.

Concluye la autora, tras su análisis de las conclusiones del Abogado General previas a la sentencia Costeja, que “en Europa, si no es de la mano de una “remodelación del marco jurídico sobre el tratamiento de los datos personales, creemos que la protección de este derecho tendría que venir de la mano de su reconocimiento como facultad integrante del derecho fundamental a la protección de datos personales garantizado por la Carta de Derechos Fundamentales de la Unión Europea...” (2014, 335-337)

Las limitaciones al derecho de supresión aparecen en el punto 3 si el tratamiento es necesario para “ejercer el derecho a la libertad de expresión e información”, para “el cumplimiento de una obligación legal”, bien por “razones de interés público en el ámbito de la salud pública” o “con fines de archivo en interés público, fines de

investigación científica o histórica o fines estadísticos" o para la "formulación, el ejercicio o la defensa de reclamaciones".[808]

El artículo 18 reconoce el derecho a la limitación del tratamiento en unas determinadas condiciones, como son: que el interesado impugne la exactitud de los datos en plazo, o para tratamiento lícito prefiera el interesado la limitación a la supresión, o no sean datos necesarios ya para el responsable del tratamiento pero sí para el interesado para reclamaciones o durante el intervalo de verificación de motivos legítimos prevalentes en caso de que el interesado haya ejercitado su derecho a oposición al tratamiento.

Esa limitación del tratamiento podrá salvarse si así lo consiente el interesado o "para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro" (segundo punto del artículo 18).

Estos derechos de rectificación, supresión y limitación deben ser objeto de notificación al interesado por el responsable del tratamiento.[809]

Estos derechos que estaban ya dentro del marco de los derechos ARCO, normativizado principalmente en el artículo 12 de la Directiva[810], con el derecho de acceso como "punta de lanza", tal y como hemos visto, venían ya dotando de facultades importantes a los interesados, si bien a través de la normativa de los Estados miembros, hasta la efectiva aplicación y entrada en vigor del REPD.

---

[808] Interesante aportación nos presenta Simón Castellano (2012) que lo define "como el derecho a equivocarse y a volver a empezar, que se concretaría en las facultades de cancelación y oposición frente a tratamientos de datos personales divulgados vía Internet que se producen sin el consentimiento del titular o sin otra causa legítima que justifique su difusión".
Igualmente interesante el artículo de Azurmendi (2015) sobre el "derecho al olvido para los europeos": O igualmente Arenas Ramiro (2014) sobre el Caso Costeja.
También tenemos la visión general de Rallo Lombarte (2015, 704) que nos dice que "El debate sobre el derecho al olvido en Internet nada tiene que ver con el fin de la memoria, con prescindir del pasado, con el falseamiento de la historia o con la supuesta instauración de un filtro censor universal al ejercicio del derecho a la información. Sólo lecturas interesadas pueden pretender confundir a quienes se aproximan a este debate de buena fe y aprovecharse de las dificultades que plantea un conocimiento cabal de los muchos impactos que Internet produce en la realidad que nos envuelve". Haciéndose eco de las palabras de la Comisaria Reading en su defensa del derecho y en su introducción en la propuesta de la Comisión: ""Dios perdona y olvida pero la web nunca" (2015, 708).
[809] Artículos 18.3 y 19.
[810] En su letra b)

4.4.1 El Derecho de rectificación y supresión y el Tribunal Europeo de Derechos Humanos.

Nos pararemos aquí en algunas interpretaciones sobre estos derechos realizadas por el TEDH, sobre la base del artículo 8 del CEDH, y que nos sirven además de ejemplo de la estructura jurídica multinivel europea.[811]

En la sentencia del TEDH, Cemalettin Canli contra Turquía, (nº 22427/04, de 18 de noviembre de 2008), por el que el demandante se ve reconocido como víctima de la violación del artículo 8 CEDH, ya que, si bien había sido enjuiciado en dos procedimientos penales, en ninguno había resultado condenado. Después de ser detenido de nuevo, la policía lo calificaba en un informe como miembro de dos organizaciones ilícitas. El Tribunal, calificando los datos dentro de la esfera de la vida privada, y poniendo de relieve la poca fiabilidad y efectiva sustanciación de la protección de los registros policiales implicados en el caso, declara la violación del Convenio y manda la indemnización de 5.000 euros al demandante por los efectos de esa contravención.[812]

En la sentencia del TEDH, Segerstedt-Wiberg y otros contra Suecia, 8nº 62332/00, de 6 de junio de 2006), cinco ciudadanos suecos reclaman conocer sobre los registros policiales de seguridad de su país respecto a su filiación a partidos (liberales y comunistas). Analizando la Ley sueca, el Tribunal da por bueno esa recogida y registro de datos en orden a las especiales circunstancias de seguridad que se amparaban por la norma. Si bien respecto a algunos demandantes consideran excesivo el mantenimiento en el tiempo de esos registros, como en el caso de Per Nygren, de ideas oscilantes entre el comunismo y el nazismo, proviniendo la información de una reunión política en

[811] Al respecto, y teniendo en cuenta que analizaremos seguidamente la sentencia Costeja contra Google del TJUE.
[812] Apartados 33, 42 y 43 de la sentencia.

Varsovia en 1967, visto el tiempo transcurrido el Tribunal no ve razonables ni suficientes ya las razones de seguridad nacional aducidas. Igual solución ofrece en el caso del demandante Herman Schmid, parlamentario europeo de 1999 a 2004 en el grupo de Izquierda Unitaria (GUE/NGL) y miembro del partido de la Izquierda sueca, sobre registros mantenidos sobre él por la policía de Malmö entre 1963 y 1975, sobre supuestas actividades ilícitas en manifestaciones, cuando pertenecía a asociaciones estudiantiles universitarias de izquierdas.[813]

Como ejemplo de rectificación podemos citar la sentencia del TEDH, Ciubotaru contra Moldavia, (nº 27138/04, de 27 de abril de 2010), en la que el demandante, un escritor y profesor de francés, solicita a las autoridades moldavas el cambio de su antigua documentación de identidad soviética, donde se indicaba su etnicidad moldava por el de rumana, que le es denegada por falta de motivación y prueba. Aun considerando válida la petición de pruebas por un Estado para que se demuestre el origen de una persona, el Tribunal considera que no se cumplen las obligaciones de protección positiva por parte de Moldavia para garantizar el respeto de la vida privada del demandante, que, además, había presentado elementos de prueba objetivos y objetivables a esa pertenencia "como la lengua, el nombre, la empatía y otros". El hecho de pedirle pruebas de la "rumanidad" de alguno de sus padres, (más con la historia de Moldavia y Rumania), y la supresión de identidades nacionales de manera oficial en la época soviética, constituían obstáculos insalvables establecidos por las autoridades moldavas, incumpliendo así con aquellas obligaciones de respeto y defensa de la vida privada de las personas, y del señor Ciubotaru en particular.[814]

4.4.2 La Sentencia Costeja contra Google y el derecho al olvido.

Debemos recordar, en primer lugar, la cuestión expresa de la sentencia que motiva la generación de este nuevo ejercicio de la protección, y que se establece por la Audiencia Nacional en su tercera pregunta al Tribunal de Justicia:

[813] Apartados 89 y 90
[814] Apartados 51, 58 y 59

"3) Respecto al alcance del derecho de cancelación y/oposición en relación con el derecho al olvido se plantea la siguiente pregunta:

¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la [Directiva 95/46] comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"

Para establecer jurídicamente el Tribunal esta nueva dimensión en el ejercicio del derecho a la protección de datos en Europa, en primer lugar relacionándolo con el ámbito material con el que viene relacionado el asunto. Y expresándolo así la sentencia en su par. 88: "... el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita."

Y sobre todo, a partir de la contestación a la tercera expresa pregunta sobre este nuevo ejercicio en la protección de datos europea, el ejercicio del derecho al olvido. Que se establece, esta vez, en su necesidad de ponderación y apreciación de las circunstancias por el Juez nacional para su óptimo ejercicio[815]. Si bien esta nueva dimensión del ejercicio de la protección de datos se fundamenta directamente por el Tribunal en los artículo 7 y 8 de la CDFUE, y en su prevalencia.[816]

[815] Párrafos 89 a 99

[816] "... los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa

4.5 El derecho a la portabilidad de los datos.

El novedoso derecho a la portabilidad de los datos se reconoce en el artículo 20, y consiste en poder el interesado recibir "en un formato estructurado, de uso común y lectura mecánica" sus datos por el responsable del tratamiento, siempre que esté se base en el consentimiento, y esté efectuado en formato electrónico.

El clásico derecho de oposición "en cualquier momento, por motivos relacionados con su situación particular", se contempla en el artículo 21, extendiéndose a aquellos perfiles elaborados por la "mercadotecnia directa". Con él relacionado, se encuentra el artículo 22 que promulga el "derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles", que puede no aplicarse por necesidades contractuales, por autorización del Derecho de la Unión o de los Estados miembros o por consentimiento explícito.[817]

En este sentido Delgado Valle (2014, 454) nos habla del derecho al recuerdo, ofreciendo un punto de vista diferente y definiéndolo, en clara sintonía con la filosofía de la portabilidad de los datos que es al fin y al cabo el derecho a llevar uno consigo su expediente personal telemático ya sea el "online" y el "offline"; como "el derecho de toda persona física o jurídica, a la conservación de sus comunicaciones, informaciones, aportaciones literarias, pictóricas, gráficas, contenido audiovisual o cualquier otra forma de propiedad intelectual o industrial de su pertenencia que haya subido, creado, almacenado o indexado en un servicio online". Definición como vemos de ampliación del derecho de protección y no necesariamente contradictoria ni con el derecho al olvido ni con la protección de datos en su perspectiva general.

---

persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate."

[817] Según alguna doctrina una tipo de derecho de acceso "versión premium" (Miralles, 2012).

5. El Responsable y el Encargado del tratamiento.[818]

Entramos ya en la parte del estudio del ámbito subjetivo del derecho a la protección de datos, de quien atiende y cómo se vigila el respeto de este bien jurídico y sus derechos relacionados.

El Capítulo IV del Reglamento regula al responsable y al encargado del tratamiento[819]. En él se respira permanentemente el principio anglosajón de "Accountability".[820]

El artículo 24 del Reglamento prescribe la obligación, con carácter general para el responsable del tratamiento, de aplicar todas las medidas "técnicas y organizativas apropiadas" para que se cumplan las estipulaciones del Reglamento, entre las que se destacan, cuando sean proporcionadas a los fines del tratamiento, las "oportunas políticas de protección de datos", aceptándose los códigos de conducta o mecanismos de certificación para esa finalidad[821]. En este sentido, cobra singular relevancia la

[818] Previamente debemos apuntar para el buen entendimiento de la figura del responsable del tratamiento la imponente obra monográfica de Duran (2016, 57), que nos aclara que "este concepto, inexistente en la génesis del derecho a la privacidad que se encuentra en el derecho anglosajón y en el Convenio de Roma de 4 de noviembre de 1950 para la protección de los Derechos Fundamentales y las Libertades Públicas (CEDH), se abre camino en las primeras leyes europeas que datan de los años setenta (…) En EE.UU. se verá que la regulación de la privacidad, a nivel federal, no ha establecido una categoría formal de responsable asimilable a la que se incorporará en la normativa europea. Los motivos son, primero, porque el principal sujeto obligado a respetar este derecho es el Estado, por lo que se entiende que es más fácilmente definible. Un segundo motivo es porque, en este país, se ha optado por establecer un sistema de protección de la privacidad consistente en leyes federales sectoriales, destinadas al sector privado, solo para determinados colectivos de sujetos obligados".
Encontrándonos así ante una construcción jurídica verdaderamente europea: "Esto significa que el concepto es una disposición de derecho de la UE que no remite expresamente al derecho de los Estados miembros para determinar su sentido y alcance y que será objeto en toda la UE de una interpretación autónoma y uniforme" (2016, 116).

[819] Ver en este sentido el Dictamen 1/2010 del Grupo del Artículo 29 (2010, 9) sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento, que considera el concepto de responsable del tratamiento como un concepto autónomo del derecho comunitario.

[820] Sobre el concepto de "accountability" Butin, Chicote y Le Métayer (2014). Al que también aludimos en la primera parte de este trabajo.

[821] Recordemos el artículo 3.1 aplicándose el Reglamento "en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no..."

"protección de datos desde el diseño y por defecto" contemplada en el artículo 25[822], destacándose la medida técnica de "seudonimización" en los mismos. El artículo 26 prevé la corresponsabilidad en el tratamiento para dos o más responsables que determinarán "de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones", acuerdo cuyos aspectos esenciales deberán ponerse a disposición del interesado, siendo igualmente susceptibles los responsables de ser enfrentados por el interesado en los derechos reconocidos en el Reglamento.

El ámbito territorial del Reglamento en este sentido se refuerza en el artículo 27 con la designación por escrito de representante ante la Unión, si bien no es aplicable para el tratamiento ocasional, siempre que, a pesar de que no sea habitual, "no incluyan el manejo a gran escala de categorías especiales de datos", y "sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas", ni tampoco a las autoridades u organismos públicos. Parece en esta última salvedad que los organismos públicos de fuera de la Unión son totalmente fiables.

Ese representante se establecerá en "los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios" al que se le delega la gestión de los mismos.

El artículo 28 del Reglamento regula la figura del encargado del tratamiento, que será elegido por el responsable del tratamiento entre personas "que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas", sin que éste pueda subcontratar la actividad en otro encargado "sin la autorización previa por escrito, específica o general, del responsable". Esta relación será una relación jurídica

[822] La Privacidad por diseño es una construcción teórica de la profesora canadiense y Comisaria de Protección de datos de Ontario Ann Cavoukian. Aquí se pueden analizar sus principios(recuperado el 3 de abril de 2017):
https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
La propia creadora del término "Privacy by design" lo analiza con perspectiva en (Cavoukian, 2013, 194), ahondando y afianzándose en su necesidad con el paso de los años, y estableciendo para la privacidad lo que denomina "design-thinking perspective" (Pág. 194) "Privacy by Design.
Igualmente podemos referenciar a Hustinx (2010) o a Duaso Calés (2016, 303) que orbitando sobre el concepto, nos relata que "la protección de la privacidad está literalmente incrustada en el diseño de toda tecnología y además está fundamentada en un enfoque centrado en el ususario…"

vinculante. Se requiere “contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros”.

Esa relación jurídica deberá contener los estipulados mínimos del artículo 28.3 en sus letras a) a la h), debiendo tratar los datos “únicamente siguiendo instrucciones documentadas del responsable”, con garantías de confidencialidad en las personas involucradas, con las medidas adecuadas y las condiciones necesarias para el mismo, asistiendo en el tratamiento y ayudando al responsable al cumplimiento de sus obligaciones. Y estando a su disposición en la posible futura supresión o devolución de datos, así como suministrando la información necesaria, sobre todo en posibles casos de infracción, con especial deber de alerta en estos casos.

Esa subcontratación entre encargados del tratamiento reúne condiciones similares a la clásica del derecho laboral, debiéndose imponer “este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado...” (artículo 28.4)

Cobran especial importancia, como medios probatorios de las garantías suficientes previstas en el artículo, los códigos de conducta y los mecanismos de certificación, aludiéndose a ellos en el Reglamento y avalándose así por el mismo. Preve asimismo las cláusulas tipo, previstas por la Comisión o las Autoridades de Control, con alusión también a la responsabilidad del encargado incumplidor.[823]

Se impone igualmente, en el artículo 30, la necesidad de llevar un Registro de actividades de tratamiento al responsable y, en su caso, su encargado, con los datos mínimos que se establecen en el precepto de la letra a) a la g) del punto 1 y de la a) a la d) del punto 2 respectivamente. Incluye identificación del responsable o responsables, los fines, las categorías de interesados y de datos tratados, las transferencias de datos personales a un tercer país o una organización internacional, y si fuera posible, los

[823] Puntos 5 a 10 del artículo 28 y artículo 29

plazos para la supresión de esas categorías y una descripción general de las medidas técnicas y organizativas de seguridad.

Esta obligación no opera para las PYMES, con salvedades. Así nos dice el punto 5 que "no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1[824], o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10."

En los Considerandos que van del 73 al 88 ya se perfilan las obligaciones y el cumplimiento de las determinaciones de la Norma por parte del responsable o el encargado del tratamiento, haciéndose especial hincapié a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento y las medidas de seguridad que tomen aquellos en su garantía, como puede ser la del "recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos" (C. 81), " mantener registros de las actividades de tratamiento bajo su responsabilidad" (C. 82) o la atención a las posibles actividades" de alto riesgo" y las posibles depuraciones de responsabilidades por esos perjuicios.[825]

Se destaca también la necesidad de comunicación "al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades",[826] incidiendo en la "protección tecnológica adecuada" y en "las medidas organizativas oportunas", así como las circunstancias acaecidas.[827]

[824] "… origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales"
[825] Considerandos 84 y 85
[826] Considerando 86
[827] Considerandos 87 y 88

5.1 La seguridad del tratamiento.

Así se van materializando en las siguientes secciones del Capítulo esas obligaciones sobre seguridad. La sección 2[828] se encarga de la seguridad del tratamiento, suponiendo un mandato al responsable y encargado para garantizar "un nivel de seguridad adecuado al riesgo", con especial atención a la seguridad de los datos, y teniendo igualmente la adhesión a códigos de conducta y mecanismos de certificación, carácter probatorio de esas garantías. Particular interés presenta la obligación del artículo 33 y del 34 de notificar y comunicar la violación de la seguridad de los datos personales a la Autoridad de control y al interesado sin dilación, siguiendo la estela de lo preceptuado en la Directiva.

En el caso de la notificación[829] a la autoridad se deberá contemplar, al menos, la naturaleza de la violación y sus posibles consecuencias, la información del delegado de protección de datos al que acudir, y las medidas adoptadas por el responsable para remediar la situación. Esas violaciones deberán documentarse por el responsable de tratamiento a efectos de su efectiva verificación por la autoridad de control respectiva.

La comunicación al interesado se producirá cuando la violación entrañe "un alto riesgo para los derechos y libertades de las personas físicas" y "describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales", y contendrá al menos la naturaleza y posibles consecuencias de la violación y la información del delegado de protección de datos al que acudir. Esta comunicación no se hace necesaria si "el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación", y particularmente si esos datos son ininteligibles o si se tomaron medidas ulteriores por el responsable que desactiven ese alto riesgo o cuando la comunicación "suponga un esfuerzo desproporcionado"[830]. Comunicación que, a su vez, pudiera ser exhortada por la autoridad de control, que también podrá decidir si se cumplen algunos de los condicionantes para no hacerlo. Medidas que llena el Reglamento, como vemos, de conceptos jurídicos indeterminados.

[828] Artículos 32 a 34 del Reglamento.
[829] Letras a) a d) del artículo 33
[830] Como ejemplo nos pone el precepto que aquellos estén cifrados

Se deben comentar aquí dos apuntes: en primer lugar el carácter de activación de ese derecho a ser comunicado de la violación que ponen en marcha los derechos y libertades y el alto riesgo para ellos; y en segundo lugar las dosis de excepción indeterminada que ofrece la segunda parte del precepto para su posible evitación (ya que dice que "no será necesaria" en esos condicionantes y no que no se aplicará, con lo que la comunicación, se puede interpretar que podría darse aún cumpliéndose las condiciones que no la hagan necesaria).

La Directiva, en la sección VII del Capítulo II, también se encargaba ya del marco técnico de confidencialidad y seguridad que debe seguir el tratamiento de datos[831]. Y en la sección IX del mismo Capítulo[832] del encuadre de referencia en el procedimiento de notificación, control y publicidad de esos tratamientos, también con la Autoridad de control nacional respectiva como referente indiscutido, y más sobre todo, como elemento institucional de filtro e interpretación primera de la protección de datos que les otorgaría el Capítulo III de la Directiva.[833]

En relación con la obligación en la seguridad del tratamiento que los Estados miembros deben establecer a los responsables, según el 17 de la Directiva, se viene a aclarar por el TJUE que va dirigida a los responsables estatales de tratamientos, (además de otras interpretaciones). Elemento que se viene a contemplar de manera más clara ya en el artículo 32 del Reglamento. Y ello, teniendo en cuenta la sentencia del Tribunal de Justicia (Sala Tercera) de 30 de mayo de 2013, Worten - Equipamentos para o Lar SA contra Autoridade para as Condições de Trabalho (ACT).Asunto C-342/12.[834]

En este proceso judicial se parte de las implicaciones de la protección de datos en el mundo laboral. Se produce tras una inspección de trabajo a un centro de la conocida cadena de electrodomésticos en Viseu (Portugal), que tras comprobaciones de ciertas

[831] Artículos 16 y 17 de la Directiva.
[832] Artículos 18, 19,20 y 21.
[833] Bajo el título "Recursos Judiciales, Responsabilidad Y Sanciones" y abarcando los artículos 22, 23 y 24.
[834] Petición de decisión prejudicial del Tribunal do Trabalho de Viseu (Portugal).

infracciones graves acarrea una multa al establecimiento por parte del organismo de Trabajo portugués (ACT) de 2.000 euros, que es recurrido por Worten ante el Juzgado de lo Social correspondiente que es el que interpone la cuestión al TJUE.

Las preguntas son: "1) ¿Debe interpretarse el artículo 2 de la Directiva [95/46] en el sentido de que el registro del tiempo de trabajo, es decir, la indicación de las horas en que cada trabajador inicia y finaliza la jornada, así como de las pausas o períodos no incluidos en ésta, queda comprendido en el concepto de datos personales?

2) En caso de respuesta afirmativa a la cuestión anterior, ¿está obligado el Estado portugués, en virtud del artículo 17, apartado 1, de la Directiva [95/46], a prever medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red?

3) Asimismo, en caso de respuesta afirmativa a la cuestión anterior, cuando el Estado miembro no adopte ninguna medida en cumplimiento del artículo 17, apartado 1, de la Directiva [95/46] y cuando la entidad empleadora, responsable del tratamiento de esos datos, adopte un sistema de acceso restringido a tales datos que no permita el acceso automático de la autoridad nacional competente para la supervisión de las condiciones de trabajo, ¿debe interpretarse el principio de primacía del Derecho de la Unión en el sentido de que el Estado miembro no puede sancionar a la entidad empleadora por dicho comportamiento?"

Para la primera pregunta el Tribunal despacha de manera indubitada la cuestión de forma afirmativa: nos encontramos ante datos personales según la Directiva.[835] Contesta seguidamente a las otras dos de forma conjunta. En primer término dando la completa razón al Gobierno portugués en sus alegaciones, y estableciendo no aplicable en este caso la interpretación del artículo 17.1 de la Directiva[836]. Precisamente porque la

[835] Párrafos 18 a 22.

[836] Párrafos 23 a 29. Llamando la atención que el TJUE establece la mala formulación en la premisa de la pregunta por parte del Tribunal portugués. Lo apunta en el par. 25: "...en contra de la premisa en que se basan las cuestiones segunda y tercera, el mencionado artículo 17, apartado 1, no impone a los Estados miembros, salvo cuando tienen la condición de responsables del tratamiento, la adopción de estas medidas técnicas y de organización, dado que la obligación de adoptarlas incumbe únicamente al

obligación en él contenida es para los casos en que el responsable del tratamiento sea precisamente un órgano estatal, no siendo el caso.[837]

Para continuar "ayudando" al Tribunal portugués en su obligación de interpretación legal, haciéndole "pedagogía" jurídica para la mejor consecución de su función.[838] Encauzándolo en su respuesta hacia los artículos 6 y 7 de la Directiva, sobre "fines determinados, explícitos y legítimos así como adecuados, pertinentes y no excesivos" en cuanto a su necesidad para el "cumplimiento de una misión de interés público o inherente al ejercicio del poder público". Invoca además que "la Directiva 2003/88 impone a los Estados miembros la obligación de adoptar las «medidas necesarias» para que, en función de las necesidades de protección de la seguridad y de la salud de los trabajadores..."[839]

Y termina estableciendo, siguiendo la lógica jurídica de la exposición de la sentencia, la interpretación de no oposición a la normativa nacional, en el caso del litigio principal de los artículos 6, apartado 1, letras b) y c), y 7, letras c) y e), de la Directiva.[840]

Destaca aquí, no solo la función interpretadora del Tribunal del Derecho Europeo, sino también su necesaria función de tutelaje con los organismos jurisdiccionales nacionales, y su voz autorizada en el engranaje del Derecho nacional así como su funcionamiento con, no ya solo la letra de la norma europea, sino también con su espíritu. E incluso

---

responsable del tratamiento, que en el presente caso es el empresario..."

[837] Párrafo 26: "...de la resolución de remisión no se desprende en absoluto que los datos de que se trata en el litigio principal hayan sido objeto de destrucción, accidental o ilícita, de pérdida accidental o de alteración, difusión o acceso no autorizados, ni de ningún otro tratamiento ilícito en el sentido del artículo 17, apartado 1, de la Directiva 95/46. Sin embargo, sí resulta de los datos obrantes en los autos aportados ante el Tribunal de Justicia que no se discute en el presente asunto que el Derecho nacional autoriza el acceso a estos datos de las autoridades nacionales competentes para la supervisión de las condiciones de trabajo."

[838] Párrafo 31: " En consecuencia, aun cuando, desde un punto de vista formal, el órgano jurisdiccional remitente ha limitado sus cuestiones a la interpretación del artículo 17, apartado 1, de la Directiva 95/46, tal circunstancia no obsta para que el Tribunal de Justicia le proporcione todos los elementos de interpretación del Derecho de la Unión que puedan serle útiles para enjuiciar el asunto de que conoce, con independencia de que dicho órgano jurisdiccional haya hecho o no referencia a ellos en el enunciado de sus cuestiones..." y Par. 32 "de los autos aportados ante el Tribunal de Justicia se desprende que el tribunal remitente desea esencialmente determinar si las disposiciones de la Directiva 95/46 deben interpretarse en el sentido de que se oponen a una normativa nacional, como la controvertida en el litigio principal, que impone al empleador la obligación de poner a disposición de la autoridad nacional competente para la supervisión de las condiciones de trabajo el registro del tiempo de trabajo, de forma que se permita su consulta inmediata."

[839] Párrafos 34 y 39.

[840] Párrafo 45.

dando pinceladas de inspiración interpretativa del propio y mero Derecho nacional que se le presenta.[841]

5.2 La evaluación de impacto.

La sección 3 (artículos 35 y 36 del Reglamento) se ocupa de la evaluación de impacto relativa a la protección de datos cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, "en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines", con asesoramiento del delegado de protección. El apartado 3 del artículo 35 marca cuando se requiere particularmente: serán en los casos de "a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público."[842]

Y nos aclara qué están dentro de la evaluación, la autoridad de control publicará una lista de los tipos de operaciones que la requieran y podrá hacer lo propio con las que no lo requieran.[843]

La evaluación requerirá, según el 35.7, "una descripción sistemática de las operaciones de tratamiento" y de sus fines, evaluación de su necesidad y proporcionalidad y de los riesgos para los derechos y libertades así como las medidas para afrontar esos riesgos.

[841] Siguiendo la vereda abierta por esta sentencia en su interpretación sustancial, y planteada por actores similares, citaremos el auto del Tribunal de Justicia (Sala Octava) de 19 de junio de 2014, en el caso Pharmacontinente - Saúde e Higiene SA y otros contra Autoridade Para As Condições do Trabalho (ACT). Asunto C-683/13. Y también en petición de decisión prejudicial por un tribunal de lo social portugués: Tribunal do Trabalho da Covilhã. Implicando la interpretación de los artículos 6 y 7, sobre los principios relativos a la calidad de los datos y a la legitimidad de los tratamientos y el artículo 17 sobre la seguridad del tratamiento.

[842] Ver referencia 811.

[843] Puntos 4 y 5 del artículo 35.

El cumplimiento de los códigos de conducta deberá tenerse en cuenta en la evaluación de impacto, y podría además no ser de aplicación cuando el tratamiento "tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica".[844]

La Directiva, en este sentido, ya establecía una sección donde se encarga de promover los códigos de conducta que contribuyan a la correcta aplicación de la misma. Aquí podríamos hacer una comparación con el paralelismo expresado por la FTC a través de su elaboración de *soft law* como guía de buenas prácticas a las empresas en Estados Unidos.[845]

Antes de la evaluación, el responsable debe realizar consulta previa al tratamiento a la autoridad de control en caso de que no se hayan tomado medidas para la mitigación de los riesgos. Autoridad que deberá "en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable", y que recibirá la información preceptiva del responsable; que serán las responsabilidades respectivas, los fines y medios del tratamiento, las medidas y garantías establecidas para proteger los derechos y libertades, datos de contacto del delegado de protección, la evaluación de impacto y cualquier otra información. Si bien se abre la puerta dispositiva al derecho nacional en el último apartado, que nos dice que "el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública" (artículo 36 del Reglamento).

[844] Puntos 8 y 10 del artículo 35
[845] Artículo 27 de la Directiva. Ver epígrafe sobre la FTC de este trabajo.

Debemos decir que estas previsiones proceden de una efectiva evaluación de la política legislativa europea, tal y como nos relatan los Considerandos del texto. Especial interés muestra así la plasmación de evaluación de políticas "en marcha" en el Derecho de la Unión, al indicarse que la obligación de notificar el tratamiento de datos personales a las autoridades de control, que imponía la Directiva del 95, no ha resultado eficiente y ha impuesto más cargas que aportado soluciones de garantía.[846] Es por ello que el Reglamento suprime esta obligación general, que se viene a sustituir por una previsión "ex ante" de una evaluación de impacto relativa a la protección de datos. Sobre todo para "las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional",[847] reconociendo así normativamente su enorme riesgo implícito. Estas evaluaciones se van desarrollando en sus requisitos en los siguientes Considerandos (y en el articulado analizado), destacándose el papel de los organismos de control en las mismas, que no quedan ni mucho menos desplazados en sus funciones.[848]

5.3 El delegado de protección de datos.[849]

La sección 4 fija su atención en otra novedosa figura, la del delegado de protección de datos. Son obligatorios en tratamientos llevados por autoridad u organismo público, exceptuándose al poder judicial en su función judicial, para aquellos que supongan "una observación habitual y sistemática de interesados a gran escala", o también sin esa habitualidad para la gran escala de "categorías especiales de datos personales, con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales".[850] Para casos distintos, su carácter y designación son potestativos, dejando abierta su preceptividad a la exigencia del Derecho de los Estados miembros. La figura podrá ser centralizada en el caso de grupos empresariales, o en caso de varias autoridades y

[846] Considerandos 89 y 90.
[847] Considerando 91.
[848] Considerandos 92 a 96.
[849] Tiene su origen en Alemania, en su ley nacional de 1977, y que fue también adoptada con éxito en Francia, Suecia, Luxemburgo o Países Bajos en base al resquicio del 18.2 de la Directiva 95/46/CE, tal y como nos ilustra Recio Gayo (2016).
[850] Artículo 37 del Reglamento y referencia 813.

organismos públicos en una única[851]. Su designación, con perfil de jurista, obedece a principios tecnocráticos de mérito y capacidad, y podrá ser personal asalariado de la entidad o contratado externo. Si bien, la garantía y respaldo en su actuación, funciones e independencia recae sobre el responsable o encargado del tratamiento.[852]

Esta previsión de mayor profesionalización en el ámbito de la protección de datos con la figura del experto "delegado de protección de datos" para asistir a los responsables o encargados del tratamiento, se presenta en el texto también en los Considerandos. Incidiéndose además en los "código de conducta" en las empresas y los mecanismos de certificación.[853]

Las funciones mínimas del delegado se contemplan en el artículo 39, siendo las propias de información y asesoramiento (también y en particular para la evaluación de impacto), supervisión "incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías", cooperación con la autoridad de control y punto de contacto con ella.

5.4 Códigos de conducta y mecanismos de certificación.

La sección 5 se encarga de los códigos de conducta y las certificaciones, que adquieren renovada importancia con el Reglamento, con el impulso dado a la autorregulación.[854]

Serán los Estados miembros, las autoridades de control, el Comité y la Comisión los encargados de la promoción de los códigos de conducta para la correcta aplicación del Reglamento y sus medidas entre los operadores involucrados, abriendo el paso a las asociaciones o entidades representativas de los responsables o encargados del tratamiento para su elaboración y desarrollo. También prevé la posible adhesión a

[851] Según el 37.5: "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones.
[852] Artículo 38.
[853] Artículos 97 a 100.
[854] Artículos 40 a 43.

códigos ya existentes con validez general, a entidades a las que se les aplica el Reglamento o a entidades a las que no se le aplique pero tenga la finalidad "de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales" (artículo 40 del Reglamento).[855]

Las autoridades control deben ser objeto de comunicación en la elaboración, modificación o ampliación de los códigos, debiendo prestar su conformidad a los mismos. En el caso de códigos que afecten a varios Estados miembros será competente el Comité, que presentará en caso de garantías adecuadas del código, dictamen a la Comisión que será la encargada de darle "validez general dentro de la Unión", y deberán ser objeto de publicación. El artículo 41 crea un nuevo órgano de supervisión de estos códigos, sin perjuicio de la autoridad de control, siempre que tenga un "nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin". Esa acreditación requerirá demostrar su independencia y pericia, su experiencia en supervisión de este tipo de idoneidades y en las gestión de las reclamaciones relativas a infracciones del código de que se trate y no tengan conflicto de intereses.

Serán la autoridad de control competente la encargada de la elaboración de criterios sobre esta acreditación y sus autorizaciones.

Este artículo se presenta poco claro y no dibuja de manera nítida los contornos de estos organismos de supervisión de los códigos, que, entendemos deberán ser objeto de algún tipo de normativa de desarrollo por parte del derecho de la Unión.

Igualmente serán los Estados miembros, las autoridades de control, el Comité y la Comisión los encargados de la promoción de los "mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos", de carácter voluntario y con procedimiento transparente. Con iguales previsiones para la adhesión que en el caso anterior de los códigos de conducta (también para las previsiones de

[855] Martínez Pastor (2014) se fija en las iniciativas de autorregulación en Europa, citando como inspiración los trabajos de la FTC americana, si bien destacando su perfil menos intenso en Europa. Destaca la "Online behavioural Advertising" de EASA/IAB (2011) entre las iniciativas privadas al igual que la respuesta del grupo de Trabajo del artículo 29 en su Dictamen 26/2011. En el capítulo "La publicidad comportamental "on line" y la protección de los datos personales".

transferencia internacional). Al igual que en lo anterior y con similar procedimiento, se puede declarar "el Sello Europeo de Protección de Datos". Siguiendo los mismos criterios que los analizados para los organismos de supervisión de códigos, se contemplan los organismos de certificación en el artículo 43. Si bien de regulación más completa ya que establece su acreditación por la autoridad de control por un período máximo de cinco años, renovables por igual periodo (punto 5 del artículo 43).[856]

[856] Veáse en este sentido el inspirador sello Europrise, que fundamenta el origen de esta regulación de la autorregulación. Recuperado el 25 de septiembre de 2018: https://www.european-privacy-seal.eu/EPS-en/Europrise-sello-europeo-de-privacidad

6. Las Autoridades de control independientes.[857]

El Capítulo VI del Reglamento (artículos 51 a 76) tiene por objeto a las autoridades de control, a las que se les refuerza indubitadamente y por fin, en su carácter de independientes. La sección primera (Artículos 51 a 54) se destina únicamente a dotar de este contorno de independencia.[858]

Los Estados miembros pueden establecer una o varias, pero deben configurar obligatoriamente estas entidades de control, que tendrán la autoridad de supervisión del Reglamento y la finalidad de "proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión." Con obligación de cooperación entre ellas y, en caso de Estados miembros con varias en su seno, solo una representará a las mismas en el Comité.

Su carácter independiente se formaliza de manera más desarrollada en el artículo 52, y comprenderá la propia en el desempeño de sus funciones y ejercicio de poderes, sin influencia externa ni instrucción ajena, con obligación de abstención en caso de incompatibilidad, con la disponibilidad suficiente de recursos humanos financieros y técnicos para su cometido, con personal propio de dependencia directa y con presupuesto independiente.[859]

---

[857] Un esbozo de la idea contenida en esta pregunta se presentó en una comunicación titulada "Las Autoridades de control en el Reglamento Europeo de Protección de Datos" en el "Congreso Internacional sobre el impacto del Reglamento Europeo de Protección de Datos: Análisis nacional y comparado." Celebrado en la Universidad Jaume I de Castellón de la Plana los días 17 y 18 de mayo de 2018.

[858] Troncoso Reigada (2016, 471 y ss.) aprecia que, a pesar del acercamiento general que supone el Reglamento al Derecho anglosajón, la figura de las autoridades y este capítulo del Reglamento son ejemplo del mantenimiento del modelo continental de protección de datos.

[859] Sobre su carácter compartimos la opinión de Duran Cardo (2016, 508): "Tienen una misión compleja, ya que, por un lado, brindan asesoramiento a los responsables del tratamiento, promueven el cumplimiento de la legislación y, por el otro, deben asegurase de que se cumple y deben perseguir a quienes la incumplen. De este modo, se vuelven juez y parte, lo que hace que tengan una papel muy difícil de desempeñar".
Igualmente García Costa (2014, 262 y ss.) realiza un completo estudio de las características orgánicas y de funcionamiento de las autoridades nacionales de control de los Estados miembros. Destacando que en general y con gran mayoría se les ha dotado a aquellas del carácter independiente del que establecía dispositivamente la Directiva. Estableciéndose el contraste en el modelo húngaro de autoridad, en la que se otorgaba por su Ley nacional de una entidad que reúne todas las garantías como modelo autónomo

Asimismo, también la Directiva presentaba especial interés en la generación de las autoridades independientes de control nacionales que vendrían a cumplir un papel indispensable en la protección de datos europea de los últimos 20 años (como bien acredita la labor de la AEPD) con poderes de investigación, de intervención y control y con plena capacidad procesal[860]. Con las necesarias atribuciones de coordinación entre ellas y que se plasman en el Grupo de protección consultivo con funciones de estudio, asesoramiento y emisión de dictámenes.[861]

En cuanto a sus miembros, el Reglamento (Artículos 53 y 54) deja abierta la facultad de nombramiento al poder Legislativo o al Ejecutivo, según disponga cada Estado miembro, o incluso a un organismo independiente dentro del aparato estatal. El nombramiento se debe basar en criterios de profesionalidad y capacidad, es decir, orientado a elegir entre expertos, mencionando concretamente al ámbito de los datos personales. Al igual que su sustitución que parece reducirse a casos de infracciones graves o dejar de cumplir las condiciones para el cargo, es decir, dejando a un lado la libre remoción con criterios políticos. Los criterios para el establecimiento de la autoridad de control, que debe crearse por Ley o disposición con ese rango, son: su propio establecimiento, las condiciones de idoneidad y cualificaciones necesarias de sus miembros, y las normas y procedimiento para su nombramiento y cese, la duración de su mandato (con un mínimo de 4 años) y su carácter renovable o no así como las obligaciones, prohibiciones e incompatibilidades de los mismos y del personal de la autoridad.

La sección segunda del Capítulo (artículos 55 a 59) entra a regular las competencias, funciones y poderes de las autoridades de control.

---

de independencia en su función de protección, con la actual deriva antidemocrática del país en materias de democracia institucional y de Estado de Derecho.
Independencia que, como nos apunta el autor, viene reforzada en el REPD, si bien fijando todavía este manual la atención en las primeras propuestas del mismo y no en su versión definitiva.

[860] Artículos 29, 29 y 30.

[861] Conocido como Grupo del artículo 29, de gran influencia consultiva, y al que aludimos en sus opiniones, como es propio, en este trabajo.

Las autoridades son competentes en base al poder que se les confieran a excepción del control de "las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial", según el artículo 55.3.

La autoridad de control competente será la que se encargue del control del "principal o del único establecimiento del responsable o del encargado del tratamiento", si bien todas podrán ser competentes para "tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro". Si bien deberán informar sin dilación a la autoridad principal que en el plazo de 3 semanas decidirá mostrarse o no conforme, siguiendo el artículo 60 (artículo 56.2).

Las funciones de las autoridades de control se establecen en el artículo 57. Son fundamentalmente las de control de aplicación del Reglamento y defensa, promoción y salvaguarda integral del derecho a la protección de datos en su ámbito y de manera coordinada y cooperante. Funciones que tendrán carácter gratuito para el interesado y para el delegado de protección de datos, si bien podrán implicar tasas "razonables" en caso de solicitudes infundadas o excesivas, sobre todo si tienen carácter repetitivo.[862]

Por tanto, dentro de sus poderes estarán los propios de un órgano de control, como son los de solicitud de información al responsable y/o encargado del tratamiento y acceso a la misma, los de auditoría, revisión de certificaciones en materia de protección de datos, notificación de infracciones y el acceso a establecimientos, equipos y medios de tratamiento del responsable y/o encargado del mismo (artículo 58.1).

Además disponen de los poderes correctivos de sanción y mandato al infractor responsable o encargado para que atienda a lo ordenado o deje de actuar en la manera lesiva e infractora sobre los datos personales y su efectiva protección. Junto con la

[862] Funciones para las que casi se queda corto el abecedario en el Artículo 57.1 y que van desde la general " a) controlar la aplicación del presente Reglamento y hacerlo aplicar; pasando por las de salvaguarda, fomento de la protección e investigación (ejemplo" d) promover la sensibilización de los responsables y encargados del tratamiento…" o f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación…)hasta la de aprobación de códigos de conducta o autorización de cláusulas tipo, quedando la sancionadora latente por el no reconocimiento en todos los Estados de la Unión de esta facultad a la Administración Pública.

imposición de limitaciones y prohibiciones, pueden ordenar la rectificación o supresión de datos personales en un tratamiento, retirar certificaciones, imponer multas administrativas u "ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional".[863]

Junto a los anteriores, disponen de importantes poderes consultivos y de autorización. Como son los de asesoramiento al responsable del tratamiento o el de emisión de dictámenes, autorización de tratamientos sobre "el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública", y aprobación de códigos de conducta, acreditación de organismos de certificación, expedición de certificaciones, adopción de cláusulas tipo, de cláusulas contractuales, acuerdos administrativos y normas corporativas.[864]

Se deja a los Estados miembros la dotación por ley a sus autoridades de control la capacidad jurisdiccional de entablar pleitos y de su ampliación de poderes. Con obligación de informar anualmente de sus actividades.[865]

6.1 Cooperación y coherencia entre autoridades de control.

El Reglamento dedica todo su Capítulo VII (artículos 60 a 76) a la salvaguarda de la cooperación y coherencia entre las autoridades de control, junto con la previsión del Comité Europeo de protección de datos, como órgano superior en este ámbito.

La cooperación clave será la que se dé entre las autoridades de control principal y las demás interesadas de las que se ocupa el artículo 60, una previsión de la coordinación del "día a día" en la protección de datos. La cooperación se establece como una auténtica obligación, y no como una previsión dispositiva de entendimiento. Se prevé el envío de la información sin dilación, y un procedimiento más o menos perfilado (con

[863] Artículo 58.2 letras a) a j).
[864] Artículo 58.3 letras a) a j) con remisiones a los artículos 36.5, 43, 42.5, 28.8, 46.2 a), 46.3 a) y b) y al 47.
[865] Artículo 58 apartados 5 y 6 y artículo 59.

plazos de 4 y 2 semanas incluidos) para gestionar las objeciones que puedan presentar las autoridades interesadas a la principal, con posibilidad de casos de urgencia. Igualmente el artículo 61 presenta la obligación de asistencia mutua entre autoridades, con previsión también de cierto procedimiento (un mes para contestarse por ejemplo) y establecimiento de supuestos en que se podrá negar la solicitud de asistencia.[866]

El artículo 62 ya se fija un paso más en la previsión colaborativa en lo que podríamos denominar "cooperaciones reforzadas" en la protección de datos entre autoridades de control. Bajo el nombre de operaciones conjuntas se establece la posibilidad de investigaciones y operaciones de ejecución conjuntas entre autoridades de distintos Estados miembros "si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento". Este supuesto da el derecho a participar a "una autoridad de control de cada uno de esos Estados miembros", que recibirán invitación de la autoridad principal competente. Asume igualmente la responsabilidad por los daños y perjuicios, que esa participación pueda suponer en la actuación en sus respectivos territorios.[867]

La sección 2ª del Capítulo se rubrica bajo el enunciado de "Coherencia", en la que además de previsión de mecanismos de coherencia, establece como principal elemento para ello al Comité en sus dictámenes y resolución de conflictos. Es decir, no se deja al arbitrio de futuros entendimientos acordados, sino que establece una fuerza jurídica vinculante en forma de previsión legal del Dictamen del Comité en los casos tasados en el artículo 64.

[866] Según el apartado 4 del 61: "La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:
a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o
b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud."

[867] Apartado 2 del 62. Entendemos que a la autoridad que sea competente en cada Estado miembro, no necesariamente la estatal, siempre en base a lo que diga el Derecho del Estado miembro, como apunta el 62.3

El Dictamen deberá emitirse según el 64.1 en caso de que las autoridades de control tomen decisión sobre medidas determinadas, que son “cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los criterios aplicables a la acreditación de un organismo con arreglo al artículo 41, apartado 3, o un organismo de certificación conforme al artículo 43, apartado 3;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.”

Es decir, en caso de estar previstos en listas de evaluación de impacto de protección de datos, asuntos de “proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros”, criterios de acreditación de amplio alcance, cláusulas tipo relativas a garantías para considerar adecuadas transferencias de datos y cláusulas tipo en general, así como normas corporativas vinculantes.

Por tanto, el artículo va recogiendo todas las previsiones previas de remisión en el Reglamento a la necesidad de este Dictamen del Comité, que se conceptúa al final como una garantía ejecutiva prevalente de coherencia. También se le podrán someter a dictamen al Comité asuntos de distinta índole por las autoridades de control que sean “de aplicación general o que surta efecto en más de un Estado miembro” (artículo 64.2).

A pesar de su obligatoriedad, el dictamen no resulta vinculante, si bien se le quiere dotar de la mayor influencia por el Reglamento dentro de ese límite formal. El apartado 7 del artículo 64 nos dice que la autoridad de control que planteó el asunto "tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión"[868]. Ese carácter que cabalga entre el de no vinculante en apariencia y vinculante, se sigue forzando en el siguiente apartado, ya que en caso de que la autoridad de control no prevea seguir el dictamen del Comité, el apartado 8 nos transporta al primer apartado del siguiente artículo del Reglamento, el 65, encargado de la resolución de conflictos, que tiene como fin "garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante". Con lo cual podremos considerar el dictamen no vinculante de manera formal y en primera instancia, para luego poder ser revisado por el mismo órgano que lo emitió, en este caso, en forma de resolución de conflicto, en cuyo caso el mismo Comité podrá revestirlo de vinculación jurídica. Esa resolución de conflictos no solo se da para esos casos sino, en general, para diferencias de interpretación y de decisión entre autoridades de control. De ahí el carácter prevalente del Comité entre autoridades y en materia de protección de datos en Europa, a nivel administrativo.

En caso de urgencia motivada se prevé en el artículo 66 un procedimiento que, en lógica, acorta los plazos de los generales contemplados. Y el 67 prevé la normalización por la Comisión de los modelos de intercambio de información entre autoridades.

Ya la sección 3ª se encarga al fin de la composición, estructura y funcionamiento del Comité, tantas veces con anterioridad citado en el Reglamento como un ente aparecido pero no especificado. La sección se encarga de darle forma de manera detallada. Su composición es la habitual de la Unión de los directores de una autoridad de control de un Estado miembro (no necesariamente el de la estatal), con participación de la Comisión y del SEPD. Tiene carácter independiente, (algo lógico, estando esta

[868] El apartado 7 del artículo no ofrece dudas: "La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité…"

configuración obligada para las autoridades de control en general), y sus funciones[869] son las de supervisión asesoramiento y control, con ese toque prevalente que ya hemos ido observando, así como emisión de directrices, dictámenes, recomendaciones, junto a la promoción de buenas prácticas, y evidentemente todas las particularmente preceptivas que se han ido recogiendo a lo largo del articulado del Reglamento. Obligación aparte incluida del informe anual sobre protección de datos a la Comisión, Consejo y Parlamento, según el artículo 71.

Su procedimiento de decisión viene marcada por la operativa mayoría simple y el de la adopción de su reglamento interno por la cualificada de dos tercios. Su presidencia es de 5 años y renovable una vez, elegida entre sus miembros y con funciones propias del puesto (convocatoria, notificación de decisiones y garantía de su funcionamiento). Se prevé además dos vicepresidencias. Igualmente para la secretaría del órgano en sus funciones propias de ese cargo ("apoyo analítico, administrativo y logístico"), si bien debemos mencionar que de este puesto se hace cargo la figura del SEPD, cuyo personal dedicado a esas funciones de secretaría del Comité "dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos", con objeto evidente de salvaguardar la independencia de una y otra institución. Igualmente se observa la reserva de confidencialidad (artículos 72 a 76).

6.2 Las autoridades de control en los Considerandos

Otro bloque importante de tratamiento legislativo en el Reglamento y de fuerte impulso dado, al igual que lo tratado para los flujos internacionales, es el encargado de las autoridades de control, también ya en los Considerandos que ofrecen mucha sustancia sobre el espíritu normativo de la reforma en este sentido, y blindando ya, como hemos visto, su condición de independencia.

[869] Funciones que se pormenorizan de las letras a) a y) del apartado 2 del artículo 70.

La Norma establece así más profusamente el desarrollo de estas figuras de control sobre la protección de datos en Europa como elemento esencial. Y dispone una mayor unicidad, con criterios de referencia para la actuación de la Autoridad correspondiente, abriéndose además la posibilidad de varias Autoridades en cada Estado miembro a nivel local y regional, si bien con la obligación de coordinación entre las mismas, como hemos analizado. Obligación de coordinación que debe darse también entre las diferentes Autoridades de los Estados miembros, entre ellas, y con la Comisión. Además de la dotación de recursos suficientes, debiéndose regular, en todo caso, con norma con rango de ley.

El Reglamento además, adopta el elemento jurisprudencial de interpretación para la aplicación de la competencia de la Autoridad de control, dejando claro así la correspondencia en función del establecimiento principal del tratamiento, si bien coordinadas con las demás afectadas, teniendo presente siempre el concepto y actuación de la "ventanilla única" en esas actuaciones.[870]

Ahora bien, en esa coordinación no se diluyen las potestades propias ni las actuaciones de cada Autoridad, como nos dice el Considerando 127: "cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal."

[870] Considerandos 117 a 138. Así el Considerando 124: "Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal..."

Debido ya principalmente al objetivo de unificación de garantías que supone el Reglamento, las autoridades de control se ven dotadas de unos poderes similares de actuación en el ejercicio de sus funciones[871]. Se crea, así, una suerte de red de autoridades de control para que las reclamaciones, aún recibiéndose en una de las que no sean competentes, siguiendo los criterios vistos del Reglamento, pueda trasladarse de manera efectiva y coordinada a la que resulte de aplicación. Con la posibilidad añadida de asistencia mutua entre ellas para auxiliarse en la resolución de los asuntos, así como las posibles "operaciones conjuntas" a llevar a cabo entre ellas. Estableciéndose como salvaguarda de esa actuación colaborativa a la que aspira la Norma, en el mecanismo de coherencia que supervise toda esa actividad cooperativa y que estará a cargo de un Comité dependiente de la Comisión y que se verá especialmente habilitado en su aplicación cuando sea urgente proteger los "derechos y libertades de los interesados" y sobre todo en aquellos casos con medidas destinadas a producir efectos jurídicos.[872]

El fomento último de esa aplicación de coherencia se observa con la creación del Comité, heredero del establecido en el artículo 29 de la Directiva, dotado de independencia, y con tintes de institución de control último europeo en protección de datos.[873]

A partir del Considerando 141 podemos observar ya un tratamiento legal destinado a lo que podríamos considerar el reforzamiento de las garantías de los interesados en la

[871] Así el Considerando 129. "...las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas..."

[872] Considerandos 130 a 138.

[873] Considerandos 139 y 140.
Dándosele especial relevancia también al SEPD en sus cometidos. Asi el C. 139: "...Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones".

protección efectiva de sus datos, con protagonismo de las autoridades de control en su ejercicio. Merece mención aparte lo apartados destinados a la previsión de infracciones y sus correspondientes sanciones en la materia.

Entre ellas vemos el "derecho a presentar una reclamación ante una autoridad de control única",[874] basado en la tutela judicial efectiva del artículo 47 de la CDFUE; el de habilitación de asociaciones y organismos de tipo colectivo en la defensa de su tutela; el "derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité" o a los tribunales nacionales sobre decisiones de las autoridades de control.[875]

O en relación con los encargados del tratamiento el derecho de "opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública..." Y la posibilidad de resarcimiento por parte del mismo de los daños y perjuicios, por actos contraviniendo el Reglamento.[876]

[874] Asi el Considerando 142: "El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos..."

[875] Considerando 143.

[876] Considerandos 145 y 146.

7. Previsiones sobre recursos, responsabilidad y sanción.

En el considerando 148 se empieza a hacer una previsión de la aplicación de sanciones a cualquier infracción del Reglamento (incluidas las administrativas), y a partir del considerando 149, se abre la posibilidad a los Estados miembros de establecer un sistema de previsión de esas sanciones en esta materia, siempre dentro del límite máximo y los criterios establecidos en el Reglamento (considerando 150).[877]

El capítulo octavo regula los recursos, las responsabilidades y las sanciones.

Se da derecho a presentar reclamación ante la autoridad de control a todo interesado, principalmente a la de su país de residencia, reconociéndose asimismo el derecho a la tutela judicial efectiva "contra una decisión jurídicamente vinculante de una autoridad de control", con plazo de tres meses tras el resultado de la reclamación. Se le reconoce también expresamente ese derecho a la tutela judicial efectiva "contra un responsable o encargado del tratamiento", dándose la opción alternativa al interesado entre el Tribunal del Estado de su residencia habitual o del establecimiento del tratamiento. Supuesto que no opera en caso de poderes públicos encargados del tratamiento (artículos 77, 78 y 79).

En el artículo 80 se abre la posibilidad de representación a efectos de reclamaciones de este derecho individual por parte del interesado en "una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales". Mientras el 81 recoge el clásico principio procesal de suspensión de los procedimientos hasta la sustanciación de casos pendientes sobre el mismo asunto, el artículo 82 se fija ya en la importante plasmación

[877] Observando el Considerando 151 la excepción de Dinamarca y Estonia que no contemplan ni permiten en su ordenamiento jurídico las sanciones administrativas.

de posibles responsabilidades y el derecho a indemnización de daños y perjuicios procedente y para el caso de que no se cumplan con las estipulaciones del Reglamento.

El artículo 83 (letras a) a k) de su apartado 2) fija las "condiciones generales para la imposición de multas administrativas", teniéndose en cuenta las habituales para la ponderación en el ámbito jurídico administrativo sancionador, como son la naturaleza del hecho, gravedad y duración, intencionalidad, medidas para reparar el daño, el grado de responsabilidad, la reincidencia etcétera, junto con alguna particular propia de la materia como la categoría de datos implicados.

Las sanciones (artículo 84) se prevén en forma de multas administrativas de un máximo de 10 millones de euros o del 2% de su cifra anual de negocios en caso de empresas para las infracciones de las obligaciones del responsable y del encargado, de los organismos de certificación y de las autoridades de control. O de un máximo de 20 millones de euros o del 4% de su cifra anual de negocios en caso de empresas para las infracciones que atañen a los principios básicos del tratamiento, los derechos de los interesados, las transferencias internacionales de datos, obligaciones establecidas por el Derecho de los Estados miembros sobre situaciones específicas o el incumplimiento de resoluciones de la autoridad de control. Las sanciones "serán efectivas, proporcionadas y disuasorias."[878]

En comparativa con el Reglamento, el artículo 24 de la Directiva es el encargado de las sanciones, y en relación con su considerando 8, se pueden destacar algunas críticas al objetivo primigenio de armonización de legislaciones pretendido en la Directiva en materia de sanciones. Así, destacaremos el trabajo de derecho comparado de Bru Cuadrada (2007, 90) con las normativas de transposición sobre sanciones en las legislaciones alemana francesa, española, italiana y sueca, concluyendo que "dicha pretendida armonización, destinada a atajar las diferencias existentes entre las legislaciones nacionales, no se ha logrado".

[878] Apartados 4, 5 y 6 del artículo 83 y Artículo 84.

8. Situaciones específicas de tratamientos y otras disposiciones.

Debemos apuntar las especificidades que se presentan en determinadas situaciones de tratamiento, que hacen al Reglamento prestar atención a unos elementos de especialidad jurídica de manera separada.

Así, en el Capítulo noveno se recogen situaciones específicas de tratamiento en el que se deja a los Estados miembros el amplio espectro de decisión por el que especificarán en leyes propias esos campos especiales en el tratamiento de datos.

En el artículo 85 se contempla el referido a la "libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria", para los que se abre el poder de excepción o limitación al régimen general de protección establecido en el Reglamento.

También se prevé la especialidad de los accesos a los datos contenidos en documentos en poder del sector público o de entidades privadas que ejecuten misiones en interés público para su conciliación con el principio de transparencia pública (artículo 86). Igual especialidad se prevé para el número o documento de identificación personal de identidad (artículo 87).[879]

Volvemos aquí a la sentencia Linqvist, en la que para contestar la sexta cuestión proveniente del poder judicial sueco, el tribunal dilucida si existe o no contradicción entre el consentimiento del interesado y la divulgación de sus datos con el principio general de libertad de expresión. Preve el Tribunal el notable flujo de datos que supone el mercado interior europeo y reconoce la necesaria flexibilidad en la interpretación de la Directiva, y la correcta apreciación nacional de ese equilibrio. Si bien ello no debe implicar la falta de tutela de la intimidad ni obviar las necesarias sanciones para su

[879] Alguna doctrina (Sánchez Bravo, 2014, 287-288) hace una crítica al mantenimiento de la especialidad de la prevalencia del derecho a la información sobre el de protección de datos con un "indeterminado concepto de datos periodísticos" que "además se deja a la determinación de cada uno de los Estados miembros" en el nuevo sistema de protección.

defensa, y clarifica que "las disposiciones de la Directiva 95/46 no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del CEDH." Aunque deja el juicio de equilibrio de libertades en manos de las jurisdicciones nacionales.[880]

Ya en el artículo 88 se observa una especialidad novedosa en su contemplación europea, como es el de la especificidad de los datos en el ámbito laboral. En todo caso, esas normas específicas contempladas en convenio colectivo o cualesquiera otros instrumentos válidos, "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo".

Otra especialidad se regula para el tratamiento de los datos con "fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos" en el artículo 89, con arreglo a las garantías adecuadas para los derechos y libertades de los interesados, y con particular respeto al "principio de minimización de los datos personales". Esta categoría de datos también, al igual que los sujetos a la libertad de información y expresión, tienen la posibilidad de que se contemplen excepciones al régimen general de protección en virtud de ley de los Estados miembros.

Además se recoge la especificidad que tienen los tratamientos de datos sobre los que recaiga la obligación de confidencialidad o de secreto, según el artículo 90 y su posibilidad de regulación específica estatal, al igual que sucede con los datos y tratamientos de los mismos de "iglesias, asociaciones o comunidades religiosas", contemplados en el artículo 91.

[880] Párrafos 80, 83, 84, 85 y 90 de la sentencia.

Se viene a reconocer, por tanto en el Reglamento, y desde el inicio en sus Considerandos, la especial protección para datos "particularmente sensibles en relación con los derechos y las libertades fundamentales", así como las categorías especiales de datos, como son los relacionados con la Salud. El tratamiento "de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública" según el considerando 54. Contemplándose así excepciones al consentimiento, precisamente basadas en esa especialidad.[881]

Así, algunos temas recurrentes en el ejercicio del derecho a la privacidad y su posible confrontación con otros derechos previstos, se viene a manifestar también en el Reglamento ya en sus Considerandos. Particularmente la previsión de los fines periodísticos o de expresión artística o las necesidades de la transparencia y el acceso a documentos públicos se siguen contemplando[882]. Así como los datos en el orden laboral o en el ámbito de la investigación o en el plano de la Salud. Igualmente para investigaciones históricas y estadísticas.[883]

8.1 Jurisprudencia sobre la confrontación entre la protección de datos y la libertad de expresión.

El Reglamento en su mantenimiento de esta diferenciada consideración de tratamiento especial viene influido por una extensa jurisprudencia, que, desde los Tribunales de Justicia de Luxemburgo y de Derechos Humanos de Estrasburgo, se lleva asentando sobre este conflicto jurídico. Elementos relacionados además con su precedente en el

[881] Considerandos 51 a 53 y 55 a 57.

[882] Así el Considerando 153 en la conciliación con "...las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria..." o el Considerando 154 que prevé que "...se tenga en cuenta el principio de acceso del público a los documentos oficiales..."

[883] Considerando 155: "El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral o el Considerando 156 sobre "El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado..." así como los Considerandos 157 a 159 y los Considerandos 160, 162 y 163.

artículo 9 de la Directiva 46/95/CE, y en los vigentes artículos 11 de la CDFUE y 10 del CEDH.

Así, el Tribunal de Justicia de la Unión, en el Asunto Satamedia, relacionado con la difusión de datos fiscales de más de un millón de personas obtenidos de manera legítima de la Administración tributaria de Finlandia, considera adecuada su utilización por las dos empresas (Markkinapörssi y Satamedia) en su actividad periodística y conforme a la legislación nacional, amparada en la expresión de ideas y opiniones. Extendiende la facultad de este tipo de actividad legítima no solo a empresas poseedoras de medios de comunicación, admitiendo igualmente el ánimo de lucro en las mismas.[884]

Por su parte, el TEDH realiza algunos pronunciamientos dignos de consideración en este sentido. Así, en la sentencia Axel Springer AG contra Alemania (nº 39954/08, 7 de febrero de 2012), el Tribunal de Estrasburgo considera vulnerado el artículo 10 del CEDH, en una prohibición que se impone a un diario propiedad de esta empresa sobre la publicación de problemas con la justicia de un actor famoso. En la sentencia se pondera la libertad de expresión con del derecho a la protección de datos y a la vida privada que debe cumplir con algunos parámetros: el interés general del asunto del artículo, que afecte a un personaje público y que la información fuera fiable. Los elementos venían cumpliéndose en la publicación por lo que el TEDH declaró desproporcionadas las medidas de protección de la vida privada del actor.

En otra sentencia del TEDH, Von Hannover contra Alemania (números 40660/08 y 60641/08, de 7 de febrero de 2012) se declara la inexistencia de violación del derecho al respeto de la vida privada del artículo 8 del CEDH.

La supuestamente afectada era la Princesa Carolina de Mónaco a la que no se facilitó una orden judicial que prohibiera una publicación de una fotografía de ella y de su marido, de vacaciones de invierno, y que incluía además información sobre la mala

[884] Sentencia TJUE, Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy, de 16 de diciembre de 2008, (Asunto C-73/07). Apartados 56, 61 y 62.

salud del Príncipe Rainiero. El Tribunal de Estrasburgo declaró la buena y equilibrada ponderación de los tribunales alemanes entre la libertad de expresión de las editoras y el respeto a la vida privada. Ese estado de salud del Príncipe se entendió como acontecimiento razonable de la sociedad contemporánea, que contribuía, en cierta medida, a un debate de interés general.[885]

Como elemento doctrinal interesante sobre el asunto destacaremos la opinión de Pauner Chulvi (2015, 391-392) que establece como innovación destacable del Reglamento, la supresión de la restricción "de que la prerrogativa sea aplicada «exclusivamente» a actividades periodísticas. No solo resultaba complejo dar con una definición exacta de lo que debía entenderse por periodismo sino que la exclusividad impedía que pudiesen beneficiarse de la excepción las actividades en las que concurría algún otro propósito además del de informar..."

Vemos así como la libertad de información se percibe como uno de los límites más certeros cuando se alega la intimidad y la protección de datos en ese necesario equilibrio que se mantiene hoy en la sociedad

[885] Apuntaremos el artículo de Mcdonald (2005).
Igualmente podremos citar otras sentencias en sentido diferente como la del TEDH, Biriuk contra Lituania, nº 23373/03, de 25 de noviembre de 2008, en la que no se entendió que la información de salud sobre la demandante (seropositiva) aportará nada al interés general.
Otro caso del TEDH, es el de Mosley contra el Reino Unido, nº 48009/08, de 10 de mayo de 2011.

9. La protección de datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial

Siguiendo la habitual especialidad de regulación que exige y viene presentando el tratamiento de datos en el ámbito de la infracción penal y su persecución (proveniente del antiguo tercer pilar), el paquete de protección de datos de 2016 separa igualmente su establecimiento normativo, si bien desgajando esa positivización normativa en forma distinta, a través de una Directiva y no de un Reglamento. Así, la norma principal de estudio, en este sentido, además de las relacionadas con este ámbito y analizadas en el anterior capítulo (Directivas PNR y sobre Ciberseguridad) será la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; que viene a dar forma a esa especialidad jurídica en la actualización jurídica llevada a cabo.

9.1. La Directiva 2016/680. Consideraciones previas.

La Directiva sigue una tramitación paralela a la del Reglamento General del que trae causa (compartiendo incluso informes como vimos en el del Comité de las Regiones). Algunos planteamientos consideraban deseable incluso una misma norma general que incluyera esta materia como capítulo diferenciado, o abogaban por dotar de carácter legal o reglamentario europeo a lo contenido en esta Directiva.[886]

[886] A modo de ejemplo referenciaremos a López Calvo (2017, 60) que nos dice que "Llama la atención, en primer lugar, su regulación como Directiva (…) no cabe sino plantearse la oportunidad perdida de unificar ambas regulaciones en el Reglamento a efectos sistemáticos (…) Duda que se acentúa al analizar la regulación de la Directiva, que reproduce múltiples previsiones del Reglamento (…) Los problemas que pueden derivar de la doble vía se acentúan (…) cuando se prevé (…) un plazo de obligatoria transposición

La Directiva se justifica, al igual que el Reglamento, directamente en el artículo 8 de la CDFUE y en el artículo 16 del TFUE. Dentro de la lógica del nuevo paquete de protección de datos, que marca una etapa distinta en su protección. Y la apelación a los derechos fundamentales y las libertades individuales de los ciudadanos como punto de partida esencial de la misma (Considerandos 1 y 2).

Al igual que en el Reglamento "la rápida evolución tecnológica y la globalización" plantean nuevos retos a afrontar con este nuevo paquete de protección[887]. Si bien la facilitación de la libre circulación de datos en el mercado interior es sustituida en la Directiva por la necesaria "entre las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales".[888]

Se presenta la curiosidad de la continuación de remisión a la Directiva 95/46/CE en lugar de al Reglamento General, como elemento aplicable al tratamiento de datos personales, fuera de la especialidad de las infracciones penales de la que se ocupa esta Directiva 2016/680. Entendemos que esta falta de remisión al Reglamento se debe a la aplicabilidad del momento de redacción, y que se deberá entender sustituida cuando sea aplicable el mismo.[889]

Se comparte asimismo con el Reglamento las características que debe reunir el tratamiento que debe ser "lícito, leal y transparente" y para los fines específicos perseguidos por él. Remitiéndose en el caso de la Directiva, y dentro de la lógica fundacional del nuevo paquete de protección, al "principio de tratamiento leal en materia de protección de datos" como concepto diferenciado y distinto "del derecho a un «juicio imparcial»", en virtud del artículo 47 de la CDFUE y del 6 del CEDH, que se citan directamente. Tratamiento que, en igual manera, debe contemplar "nivel adecuado de seguridad y confidencialidad", para fines "determinados, explícitos y legítimos"

por los Estados que finaliza el 6 de mayo de 2018 (…) que pueden generar problemas de congruencia."

[887] Considerando 3 de la Directiva y Considerando 6 del Reglamento.

[888] Considerando 4 de la Directiva.

[889] Considerando 5 de la Directiva. Tal y como apunta Tejerina Rodríguez (2016, 110).

compatibles con los perseguidos por la Directiva, siguiendo el principio de exactitud en los datos contenidos.[890]

La Directiva se fija más en el fondo que en la forma a la hora de referirse a la base jurídica del Derecho de un Estado miembro, no requiriéndose necesariamente forma de ley, sino que esa base jurídica para el tratamiento de las autoridades deba "ser clara y precisa y su aplicación previsible para quienes estén sujetos a la misma, tal y como exige la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos"[891]. Indica también cuándo se considera lícito el tratamiento a los efectos de la Directiva, que lo será cuando sea "necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente en virtud del Derecho de la Unión o de un Estado miembro con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública"[892]; no operando como fundamento jurídico, en este sentido, el consentimiento del interesado. Parece evidente en base a la naturaleza de este tipo de actuaciones. Ya que, como bien apunta la Directiva, "cuando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad", si bien si se observa la posibilidad de que las legislaciones nacionales prevean el consentimiento en cuestiones relacionadas. Se sigue, igualmente, atendiendo a la especialidad de los datos sensibles como los relacionados "con los derechos y las libertades fundamentales", el origen racial o la elaboración de perfiles.[893]

La notificación de las violaciones en los datos de los interesados, sin dilación indebida, la designación de una figura similar al Delegado de protección de datos en la organización de la autoridad o el velar por la corrección en las transferencias de datos a terceros países o a organizaciones internacionales, también presentes en la Directiva aún con diferenciaciones importantes, son otros hitos equiparables a las protecciones del

[890] Considerando 26 y Considerandos 28 a 30.
[891] Considerando 31.
[892] Considerando 35 y que además pone como ejemplo "para la realización de pruebas de ADN".
[893] Considerandos 36 a 38.

Reglamento que confirman el espíritu unificador y de avance del nuevo paquete de protección de datos.[894]

Se prevé también, como en el Reglamento, la posibilidad del mandato a asociación para ejercitar en su nombre reclamaciones y actuaciones judiciales, en caso de entender conculcados sus derechos en este ámbito. Al igual que las previsiones de sanciones por responsabilidad con perjuicios causados al interesado, por incumplimiento de la Directiva.[895]

9.2 Objeto de la Directiva 2016/680.

Dentro de las Disposiciones Generales del articulado de la Directiva (artículos 1 a 3) nos encontramos con el objeto y objetivos de su regulación, su ámbito de aplicación y las definiciones aplicables. La protección de datos de las personas físicas por las autoridades competentes encargadas de las actividades de represión penal de los Estados miembros, con obligación de protección de sus derechos y libertades y garantizar el intercambio de datos entre autoridades en la Unión para este fin. Podríamos decir que la norma tiene por un lado un objetivo de protección de derechos y por otro de armonización y colaboración en ese trabajo de seguridad europea. Las definiciones siguen la sistemática, también en su orden novedoso, de las establecidas en el Reglamento.[896]

Por tanto, la Directiva se encarga de la cooperación judicial en materia penal y de la cooperación policial dejando sin efecto la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Debemos apuntar además que la Directiva no solo se encarga, en este sentido, de las autoridades, sino también de "cualquier otro organismo o entidad en que el Derecho del

[894] Considerandos 61 a 65.
[895] Considerando 87, también constituidas con arreglo al Derecho del Estado miembro y para esos fines de protección de datos y Considerandos 88 y 89.
[896] Al igual que en el Reglamento se aplica "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales" (artículo 2.2).

Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas" (Considerando 11). En caso de actividades que lleven a cabo las fuerzas de seguridad, distintas de las conducentes a la "prevención, investigación, detección o enjuiciamiento de infracciones penales" (Considerando 12). al igual que "acceso del público a los documentos oficiales" de esas autoridades, se remite ya directamente al Reglamento (UE) 2016/679[897]. En similitud con el Reglamento, al quedar fuera del Derecho de la Unión, no se aplica la Directiva a las "las actividades relacionadas con la seguridad nacional". Igualmente solo se aplica "a las personas físicas" con carácter de "identificada o identificable" y la protección se entiende también que "debe ser tecnológicamente neutra"[898]. Los datos genéticos y de la salud también se presentan con carácter especial y diferenciado.[899]

Debemos apuntar, junto con Blasi Casagran (2015) el avance que ha supuesto la Directiva respecto a la Decisión Marco que viene a sustituir, si bien también compartimos algunas de sus críticas respecto a su alcance limitado y su falta de amparo general a la protección de datos en todo el espectro del espacio de libertad, seguridad y justicia europeo.

9.3 Principios de la Directiva 2016/680.

La Directiva establece asimismo unos principios que delatan su ánimo de norma general. Así, el capítulo II (artículos 4 a 11) se centra en los mismos, que siguen los consagrados en el Reglamento General (licitud, lealtad, pertinencia, exactitud, conservación, seguridad y adecuación a fines). Pudiendo establecerse para fines distintos para los que se recogieron "en la medida en que:

a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y

[897] Considerandos 14, 16 y 21
[898] Considerandos 17 y 18
[899] Considerandos 23 y 24. Con remisión a la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro." Los plazos de conservación de los datos se dejan a disposición de los Estados miembros en su fijación, así como la distinción de esos datos en base a distintas categorías de los interesados. Esa distinción ha de ser clara estableciendo la Directiva el siguiente marco de referencia para la misma:" a) personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal; b) personas condenadas por una infracción penal; c) víctimas de una infracción penal o personas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal, y d) terceras partes involucradas en una infracción penal como, por ejemplo, personas que puedan ser citadas a testificar..." Igualmente los Estados miembros, en la medida de lo posible, deberán distinguir los datos personales basados en hecho de los basados en apreciaciones personales, verificando la calidad de los mismos. Dando además a medida de licitud del tratamiento de esos datos en "en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente..."[900]

Se consagra, además, la necesidad de que la recogida de datos por las autoridades competentes no lo sea para fines distintos de los del objeto de la Directiva. Si su recogida lo fuera para otros fines (dentro del Derecho de la Unión) la Directiva nos remite directamente al Reglamento (UE) 2016/679. Pueden establecer además los Estados miembros "condiciones específicas aplicables al tratamiento" (artículo 9) que deberá notificar al interesado la autoridad competente responsable.

Se prevé igualmente el tratamiento de categorías especiales de datos que "que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física" solo en caso estrictamente necesario y en los supuestos únicos en que "a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos." Disponiendo también a los Estados miembros a la prohibición de tratamientos basados en perfiles, que pudiera ser salvada

[900] Artículo 4.2 y Artículos 6, 7 y 8

por “el Derecho de la Unión o del Estado miembro”, siempre que se establezcan medidas adecuadas de salvaguarda de los derechos y libertades de los interesados, prohibiéndose con carácter general aquellas elaboraciones de perfiles que den lugar a discriminación.[901]

9.4 Derechos de los interesados en la Directiva 2016/680.

El Capítulo tercero (artículos 12 a 18) se encarga de los Derechos de los interesados. Los derechos ARCO se recogen en la Directiva para las personas físicas sujetas a su regulación. Los Estados miembros se encargarán de asegurar, con medidas efectivas, que la información sobre el tratamiento de datos de esas personas llegue a ellas, que deberá incluir la identidad y los datos de contacto del responsable, y en sus caso del delegado de protección, los fines del tratamiento, el derecho a presentar una reclamación ante la autoridad de control así como la posibilidad de ejercicio de los derechos ARCO.

El derecho de acceso a la información podrá limitarse o exceptuarse por los Estados miembros a través de medidas legislativas siempre que constituyan “una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para: a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas.” [902]

El derecho de acceso y sus limitaciones se observan, así, expresamente. Los Estados miembros deberán reconocer este derecho con las estipulaciones mínimas de contenido que ya se observaban con carácter general en el Reglamento, si bien podrán restringirlo total o parcialmente, también a través “medida necesaria y proporcional en una sociedad

[901] Artículos 10 y 11
[902] Artículo 13.3

democrática", y "teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada", con el objeto de: "a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas." Con obligación de comunicar esa restricción por escrito y sin dilación al interesado.[903]

Igualmente, el derecho de rectificación o supresión de los datos objeto de tratamiento así como su limitación también vienen recogidas, en su acepción clásica, en la Directiva, para que los Estados miembros regulen la obligación del responsable del tratamiento de rectificar o completar los datos incorrectos o incompletos o de suprimirlos cuando incumplan los requerimientos de la Directiva. Esa supresión se podría sustituir por la limitación de su tratamiento cuando "a) el interesado ponga en duda la exactitud de los datos personales y no pueda determinarse la exactitud o inexactitud, o b) los datos personales hayan de conservarse a efectos probatorios..." Al igual que en lo visto para el acceso estos derechos se podrán denegar por los Estados miembros, siguiendo las mismas garantías y para los mismos supuestos[904]. Para estos casos, junto con los vistos, en el artículo 13.3 se añade la garantía adicional de que puedan ser ejercidos a través de las autoridades de control o comprobados por estas. Con la disposición que se deja a los Estados miembros conforme a sus derechos nacionales, para incluir estos derechos para datos que figuren "en una resolución judicial o en un registro o expediente tramitado en el curso de investigaciones y procesos penales".[905]

De igual forma que en el régimen general, por tanto, los interesados a los que se les aplica esta Directiva tendrá posibilidad de ejercitar los derechos "ARCO", con las especialidades propias de la condición que se regula en ella, y ello ya se viene apuntando en sus propios Considerandos. Junto con el general derecho de información, se podrá "tener derecho a acceder a los datos que se hayan recopilado en relación con ella y a poder ejercer este derecho con facilidad y a intervalos razonables, con el fin de

[903] Artículos 14 y 15.
[904] Artículo 16. No explicitándose aquí, como si ocurre en el Reglamento, el derecho al olvido.
[905] Artículos 17 y 18.

conocer y verificar la licitud del tratamiento", si bien podrá limitarse con medidas legislativas de los Estados miembros "en la medida en que dichas medidas sean necesarias y proporcionadas en una sociedad democrática y mientras sigan siéndolo, con el debido respeto a los derechos fundamentales y los intereses legítimos de la persona física afectada, con el fin de no entorpecer las indagaciones, investigaciones o procedimientos oficiales o judiciales, de no perjudicar la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, de proteger la seguridad pública o la seguridad nacional o de salvaguardar los derechos y las libertades de terceros". Restricciones de acceso que deberán "cumplir con lo dispuesto en la Carta y el CEDH, según los ha interpretado la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos, respectivamente, y, en particular, respetar el contenido esencial de los citados derechos y libertades" (Considerandos 39 a 46).

El derecho a la rectificación de datos personales inexactos también se contempla, y en general, no podrá entorpecer la investigación ni el proceso. Estos derechos podrán recibir atención en apelación si fueran denegados con posibilidad de acudir a las autoridades de control respectivas, con previsión de responsabilidad por la autoridad (responsable del tratamiento) competente, con previsión asimismo de adopción de medidas técnicas y organizativas necesarias y la llevanza obligatorio de registros y la obligación de cooperación con las autoridades de control entre otros, o siguiendo la novedad del Reglamento, la evaluación del impacto sobre la protección de datos en caso de alto riesgo para los derechos y las libertades de los interesados o la previsión del cifrado de datos (considerandos 48 a 60).

9.5 El responsable y el encargado del tratamiento en la Directiva 2016/680.

Siguiendo una estructura similar a la del Reglamento, el capítulo cuarto de la Directiva (artículos 9 a 34) se viene a encargar del responsable y del encargado del tratamiento, previendo también la figura del delegado de protección de datos.

La obligación general del responsable y del encargado en su extensión deberá disponerse por los Estados miembros, debiendo asegurase que cumplen con las medidas

técnicas y organizativas apropiadas con los criterios de la Directiva, incidiéndose también aquí en la privacidad por diseño y por defecto, junto a la previsión de la figura del corresponsable. La regulación del encargado contempla requerimientos similares en la Directiva a los establecidos en el Reglamento.[906]

Como obligación importante de la Directiva destacaremos la de establecimiento y llevanza de un registro "de todas las categorías de actividades de tratamiento de datos personales efectuadas" para el responsable y el encargado del tratamiento, junto con la aportación de la obligación de un registro de operaciones "de, al menos, las operaciones de tratamiento en sistemas de tratamiento automatizados siguientes: recogida, alteración, consulta, comunicación incluidas las transferencias, combinación o supresión", que se utilizarán "únicamente a efectos de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales y en el ámbito de los procesos penales".[907] De igual forma los delegados de protección deberán ser observados en las disposiciones legislativas de los Estados miembros como obligatorios para las autoridades responsables del tratamiento.

La evaluación de impacto sobre protección de datos, la consulta previa a la autoridad de control en esos casos, y en otros con alto riesgo para los derechos y libertades de los interesados así como la colaboración con esta, también serán elementos a disponer por los Estados miembros en sus normas de desarrollo de la Directiva. Igualmente la seguridad del tratamiento, las notificaciones en las brechas de esa seguridad (violaciones de la misma) a los interesados y a las autoridades de control serán elementos a introducir en las normas nacionales de desarrollo (artículos 26 a 34).

[906] Ver página 463 de este trabajo y y artículos 20 y 21 de la Directiva.
Se observa en el articulado una consecuencia de redacción que hace muy similares los estipulados de la dos normas, con la salvedad obvia de remisión a los Estados miembros en su regulación. Podríamos observar, en una apuesta de futuro que, debido al lógico desarrollo más pormenorizado del Reglamento, las normativas de transposición nacionales vayan a seguir estrechamente los dictados de aquel, cuya fuerza y espíritu irradia a todo el paquete de protección de datos.

[907] Artículo 24, que coincide en los requerimientos y contenido del registro con los preceptuados en el artículo 30 del Reglamento.

9.6 Autoridades de control independientes en la Directiva 2016/680.

Las autoridades de control independientes vienen recogidas en el capítulo sexto (artículos 41 a 49), que sigue igualmente la referencia del Reglamento, por las cuales en su virtud se crean. Su carácter independiente, su estructura, composición y funcionamiento y sus poderes reproducen casi en su literalidad lo estipulado en el Reglamento[908], si bien con la necesaria actuación interpuesta de los Estados miembros para la aprobación de sus estipulaciones por ley.

También se ocupan las primeras disposiciones de la Directiva (Considerandos) de las autoridades de control, remitiéndose en su regulación al Reglamento, pero destacando su importancia en la protección de los derechos contenidos en la Directiva y en la aplicación de la misma (salvando de su actuación al ejercicio de la función jurisdiccional por exigencia lógicas de la independencia judicial). Con previsión igualmente del derecho a la reclamación ante una única autoridad de control. E incluso el general recurso judicial efectivo ante sus las decisiones de estas (Considerandos 74 a 86).

El Capítulo VII (artículos 52 a 57) sigue la obligación de las autoridades de control a cooperar, debiendo así estipular los Estados miembros la asistencia mutua, junto con la mención al Comité Europeo de Protección de Datos, creado por el Reglamento.

Asimismo el Capítulo VIII plasma la previsión del derecho a reclamación y recursos en el ámbito de la Directiva, que no presenta tampoco novedades con respecto al Reglamento. Así en similitud al Reglamento contempla el derecho a reclamación ante la autoridad de control, la alusión genérica al derecho a la tutela judicial efectiva contra las decisiones de la misma, la posible representación en sus derechos en órganos colectivos (como asociaciones de protección de datos), el derecho a indemnización y las sanciones por incumplimiento de las disposiciones de la Directiva. Todo ello a través del desarrollo normativo de los Estados miembros.

[908] Así lo estipula expresamente el artículo 41.3: "Los Estados miembros podrán disponer que una autoridad de control creada en virtud del Reglamento (UE) 2016/679 pueda ser la autoridad de control mencionada en la presente Directiva..."

De igual manera, se remite a la asistencia del Comité del artículo 93 del Reglamento a la Comisión, en la adopción de los actos de ejecución[909], y se prevén las disposiciones finales en los capítulos nueve y diez. En ellas encontramos la derogación de la Decisión Marco 2008/977/JAI del Consejo con efecto a partir del 6 de mayo de 2018, los informes de evaluación y revisión de la Comisión sobre la Directiva "a más tardar el 6 de mayo de 2022 y posteriormente cada cuatro años", junto a la revisión de otros actos jurídicos de la Unión relacionados con el objeto de la Directiva antes del 6 de mayo de 2019 para acercarlos a la misma. Y la obligación de transposición "a más tardar el 6 de mayo de 2018", si bien se deja a los Estados miembros podrán "excepcionalmente y cuando suponga un esfuerzo desproporcionado, los sistemas de tratamiento automatizado establecidos con anterioridad al 6 de mayo de 2016 sean conformes con el artículo 25, apartado 1, antes del 6 de mayo de 2023." Siendo los destinatarios de la Directiva todos los Estados miembros (artículos 59 a 65).

Como buena Directiva, ya los Considerandos se encargan de la previsión de actuación de la Comisión en los actos de ejecución, dejando claro que el objetivo de la misma (la protección de los derechos y libertades fundamentales) y su mejor consecución se conseguirán mejor en el ámbito europeo, la Comisión tiene espacio de actuación.[910]

El resto de Considerandos se van ocupando de cuestiones de encaje de la Directiva en el Derecho de la Unión y su incidencia en otras normas. Así establece el plazo de dos años para su incorporación por los Estados miembros (Considerando 96), deroga la la Decisión Marco 2008/977/JAI (Considerando 98), se encarga de la posición del Reino Unido[911] y de Irlanda respecto del espacio de libertad, seguridad y justicia, junto con las especialidades de Dinamarca (Considerandos 99 y 100), del acervo Schengen y esta Directiva para Islandia, Noruega, Suiza y Liechtenstein (Considerandos 101 a 103) y el debido respeto a los derechos fundamentales de la CDFUE (104), entre otros.

[909] Artículo 58, único del capítulo X.

[910] Lo expresa así en su Considerando 93: "Dado que los objetivos de la presente Directiva, a saber, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales y garantizar el libre intercambio de datos personales por parte de las autoridades competentes en la Unión, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a la dimensión o los efectos de la acción, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos."

[911] Sobre la que deberá volverse a encargar esta vez ya la Comisión en negociación tras la triste salida británica.

PARTE IV. LAS RELACIONES SOBRE PRIVACIDAD ENTRE LA UNIÓN EUROPEA Y ESTADOS UNIDOS.

Debemos tener presente que, como vimos, ya tanto el artículo 25 de la Directiva 95/46/CE como el Convenio 108, prevén como elementos importantes en la privacidad los flujos internacionales de datos[912], hasta el punto de la aprobación en el último caso del Protocolo adicional al Convenio 108 en el año 2001. Así como, igualmente, se le presta atención a los mismos en todo el capítulo V del Reglamento General de Protección de Datos, y en igual número de Capítulo, el quinto, en el caso de la Directiva 2016/680 sobre la esa protección en el ámbito de las infracciones penales. En este sentido, la relación entre la UE y EE.UU para garantizar la efectividad y legalidad de ese flujo entre los dos bloques más importantes de ese mercado global, resulta de especial interés y marca ese tenso e importantísimo punto de unión jurídica que acerca los dos regímenes jurídicos estudiados en este trabajo.[913]

Pasaremos primero a analizar la actual regulación de las transferencias de datos en el derecho europeo, para que nos sirva de punto de partida esencial en esa relación transatlántica que inspira el contenido de este trabajo. Para luego, centrar nuestra ayención en las normas que afectan a esa relación (los acuerdos Estados Unidos – U.E.) y la jurisprudencia que se ha encargado de delimitar su fuerza y contenido.

[912] Debemos apuntar que la UE incluía a Islandia, Liechtenstein y Noruega en el mercado interior, a efectos de no considerarlos dentro de estos flujos y, por tanto, fuera de esa necesidad de adecuación.

[913] Son importantes las opiniones del Grupo del artículo 29 (2003) (2005) al respecto sobre transferencias de datos personales a terceros países en aplicación de los artículos 25 y 26 de la Directiva y sobre la interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE.

1. Transferencias de datos personales a terceros países u organizaciones internacionales.

El Capítulo V del Reglamento[914] se ocupa de las transferencias de datos personales a terceros países u organizaciones internacionales. Siendo un elemento de desarrollo importante en el Reglamento.

El principio general de estas transferencias se contempla en el artículo 44, y se puede resumir en que el responsable y el encargado del tratamiento (allá donde se ubiquen) deben cumplir el Reglamento en lo establecido en el capítulo.

Es la Comisión la que decide si el "tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional" dan garantías de un nivel de protección adecuado[915]. Evaluación que hará sobre la base de los siguientes elementos (artículo 45):

"a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

[914] Artículos 44 a 50.

[915] Se puede consultar aquí la lista actualizada de idoneidad en la protección aprobada por instrumentos de la Comisión y debidamente publicados (recuperado el 30 de agosto de 2018): https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
Dentro de esa lista no están los Estados Unidos como marco normativo adecuado en su marco general, (sí está en los acuerdos puntuales como fue el Safe Harbour o es el Privacy Shield) porque conocedor de las reticencias europeas a la adecuación general sobre la Privacidad americana, basadas sobre todo en su dispersa y sectorial legislación, nunca Estados Unidos ha solicitado esa adecuación de su marco general a la Comisión, ya sabiendo cuál sería la respuesta de la Unión. En este sentido Wolf (2014).

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales."[916]

Es decir, realizará un análisis de funcionamiento efectivo de un Estado democrático de Derecho u organización que ofrezca plenas garantías de respeto al mismo en su funcionamiento, y que observen el derecho a la protección de datos y lo protejan efectivamente en los mimbres de lo estipulado por el Reglamento (garantías jurídico democráticas y medidas de seguridad, sometimiento a autoridades de control y compromisos con el orden internacional de protección).

Esta regulación es de especial interés para este trabajo, y que ya se mostraba de tal manera en el capítulo IV de la Directiva de 1995,[917] que actuaba de soporte legal a los acuerdos de validación ejecutiva de la privacidad de las empresas estadounidenses operando en Europa, y que tienen su mejor exponente en el fallido Acuerdo de Puerto Seguro entre la Unión Europea y los Estados Unidos, firmado a raíz de lo contenido en el mismo.[918]

[916] Es interesante la opinión del Comité de las Regiones (2002, Punto 16) sobre la propuesta que considera que "la iniciativa sobre un marco jurídico para la protección de la esfera privada en la economía de las tecnologías de la información, presentada simultáneamente por el gobierno de los Estados Unidos de América, brinda la oportunidad de combinar las iniciativas reformadoras con vistas al establecimiento de criterios de protección comunes en ámbitos fundamentales de la circulación de datos, y no solo implantar así unas normas efectivas en materia de protección de datos sino también evitar que existan unas condiciones de competencia desiguales…"

[917] Con el Título "Transferencia de datos personales a países terceros" ocupando a los artículos 25 y 26.

[918] Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto

La Comisión, tras la evaluación, tomará la decisión[919] mediante un acto de ejecución, que especificará su ámbito de aplicación y la autoridad de control actuante, y contendrá la obligación de un mecanismo "de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional"[920]. Deberá, además, publicarse una lista sobre esos países y entidades.[921]

En caso de que no haya este tipo de decisión por la Comisión, el artículo 46 nos dice cómo actuar, siendo posibles esas transferencias en ausencia de la comprobación de la Comisión si el responsable o encargado "hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas". Esas garantías se aportarán, sin necesidad de autorización de la autoridad de control en una serie de supuestos que indica el Reglamento, que tienen en común dotar de gran importancia, en este sentido, al *soft law* y a los acuerdos o pactos adoptados.[922]

---

seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Como bien apunta Heredero Higueras (1997, 186-188): "El problema del movimiento internacional de datos ofrece una fisonomía específica en el contexto de la Directiva". El Convenio 108 se basa en el concepto de "protección equivalente" mientras que el 25 de la Directiva se basa en el de "nivel de protección adecuado", que es un concepto que como dice Higueras "cabe admitir que es más débil".

El concepto "se configura como una norma en blanco que deberá "rellenar la Comisión".

Con las dificultades y resultados que podremos comprobar en el acuerdo Safe Harbour y ahora con el Privacy Shield.

[919] Entendemos que en las formas propias atribuidas por el TUE/TFUE a ella, principalmente la Decisión.

[920] Artículo 45.3. Es decir, revelaciones como la de Snowden o la de Wikileaks podrían ser decisivas en esas renovaciones.

[921] La incidencia de estas informaciones y acontecimientos se refleja en puntos exclusivos del artículo 45, que ya establece la revisión continua en base a los mismos. Así el artículo 45.4: "La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE." Y el punto 5 del 45: "Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo." Incluso previendo situaciones de urgencia (45.8) en el DOUE y en la web de la Comisión.

[922] Según el artículo 46.2 letras a) a f)) si están amparados:

– En un instrumento jurídicamente vinculante y exigible o
– Por normas corporativas vinculantes o por cláusulas tipo de protección de datos adoptadas por

Si existe autorización de la autoridad de control además se amplian los supuestos a clausulas de tipo más general.[923]

El artículo parece salvar solo la forma en la acreditación de las garantías adecuadas para una transferencia internacional, en caso de ausencia del acto ejecutivo de la Comisión, si bien entendemos que el contenido sustancial y de fondo para su validez lo siguen marcando los criterios del artículo 45.

Se regulan normas corporativas vinculantes (artículo 47) que aprueba la autoridad de control siempre que "sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial, confieran expresamente a los interesados derechos exigible y cumplan con una serie de elementos indispensables.[924]

Las sentencias o decisiones administrativas dadas en país tercero, es decir, fuera del Derecho de la Unión, solo serán reconocidas o ejecutables en base a tratado o acuerdo internacional y además el Reglamento prevé excepciones[925]a la regla general del artículo 46, en situaciones específicas:

– Con consentimiento explícito del interesado.

---

la Comisión o adoptadas por una autoridad de control y aprobadas por la Comisión, siguiendo el 93.2 del Reglamento o

– Por "un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas."

– Por "un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas".

[923] Según el artículo 46.2 letras a) y b) se amplían a:

– "Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

– Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados".

[924] Como son la información de contacto del grupo empresarial, las transferencias de datos, su carácter jurídicamente vinculante, la aplicación de los principios generales en materia de protección de datos, los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, la aceptación por parte del responsable o del encargado del tratamiento de la responsabilidad por cualquier violación de las normas corporativas vinculantes, la forma de facilitación a los interesados de esa información sobre normas corporativas vinculantes, las funciones de todo delegado de protección de datos y los procedimientos de reclamación, los mecanismos establecidos para el cumplimiento de estas normas, mecanismos de la comunicación de sus modificaciones, de cooperación e información con la autoridad de control y por último la formación en protección de datos. (Artículo 47. 2 letras a) a n)).

[925] Excepciones que se venían a recoger en forma similar en el artículo 26 de la Directiva y que será interpretado por la sentencia Schrems que veremos en la última parte de este trabajo.

– Cuando sea necesaria la transferencia para la celebración o ejecución de un contrato, entre el interesado y el responsable "para la ejecución de medidas precontractuales adoptadas a solicitud del interesado" o entre el responsable y otra persona física o jurídica "en interés del interesado". Tanto esta como la del consentimiento anterior no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

– Sea necesaria por razones importantes de interés público, para el ejercicio de reclamaciones o cuando "para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento".

– Se realice desde registros públicos abiertos al público "con arreglo al Derecho de la Unión o de los Estados miembros" si bien "no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro".

Podría seguirse incluso una última excepción fuera de las anteriores y llevarse a cabo la transferencia internacional "si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales" (artículo 49.1 *in fine*).

Conforme al artículo 50, y "en relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control" tomarán medidas apropiadas de coordinación, asistencia mutua, promoción de asociación de partes interesadas y de buenas prácticas en general.

La Directiva ya se ocupaba de lleno de este problema, aunque no con la profusión del Reglamento. Dejaremos apuntada alguna idea, pareciéndonos útil la que nos aporta Guerrero Picó (2005, 307-308), siguiendo el dictado del artículo 25 de la Directiva de 1995 en "el peligro de fomentar siquiera indirectamente la existencia de paraísos de

datos lleva a que las transferencias internacionales de datos personales sólo puedan efectuarse cuando se garantice un nivel de protección adecuado".

Nivel de protección adecuado, que será la idea clave para la licitud de estas transferencias desde la Directiva de 1995, no solo con Estados Unidos, sino con cualquier otro territorio fuera del de la Unión, y que, de entrada deberá ser apreciado como un espacio de disfrute en materia de protección de datos, al menos equivalente al que podemos percibir en nuestro estándar europeo.

1.1. Las transferencias internacionales de datos en los Considerandos del Reglamento.

Debemos resaltar como importante elemento motivador del cambio legislativo este de los flujos transfronterizos de datos personales, que cobra lógica y paralela importancia en la redacción de la Norma, tratando la misma de mantener el difícil equilibrio sobre el papel de las necesidades del comercio global y el respeto a los derechos y libertades.[926]

En los Considerandos ya se manifiesta esta inquietud jurídica, que sigue a vueltas con el concepto de "nivel de protección de datos adecuado" delegado en la Comisión, que reconociendo y en consonancia con los "valores de la Unión", deberá "tener en cuenta de qué manera respeta un determinado tercer país el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal" (Considerandos 101 a 116).

La Comisión, como sabemos, deberá tener en cuenta además, el grado de implicación internacional de ese tercer país en sistemas multilaterales o regionales de protección de datos, y revisar y supervisar periódicamente esa aplicación, con posibilidad de reversión en su apreciación de esa adecuación de la protección por el tercer país firmante. Si bien a falta de esa adecuación se traslada al responsable o el encargado del tratamiento la

[926] En el Considerando 101 nos dice que esos flujos "son necesarios para la expansión del comercio y la cooperación internacionales" si bien "esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión".

obligación de tomar "medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado",[927] en lo que parece una externalización a gran escala de un asunto vital para la autoridad pública europea hacia los responsables del tratamiento, que suelen ser, en estos casos de flujos internacionales, y en su gran mayoría, operadores privados. Más si cabe, cuando el propio Considerando 108 hace mención concreta y con tintes facilitadores (memorando de entendimiento) a los poderes públicos de los terceros países.[928] Dándose la sensación de que cobran especial relevancia los acuerdos internacionales del sector privado y sus cláusulas y normas de conducta para la correcta aplicación de lo contenido en el Reglamento para esos flujos internacionales de datos. Se aduce, en cambio, para la excepción del consentimiento para esos flujos "razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley".[929] Si bien se toma conciencia en el espíritu normativo del riesgo que supone en el día a día global estos flujos poniéndose el respeto al Reglamento y a los derechos y libertades como preeminentes en su ejecución y observancia, fomentando la cooperación para ello de las autoridades de control.[930]

[927] Considerando 108. Garantías adecuadas que "pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control"

[928] "...Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados..."

[929] Considerandos 109, 110 y 111.

[930] Así el Considerando 115 nos dice que "Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros (…) La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países..."

Y el Considerando 116: "Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales..."

1.2 La sentencia Lindqvist y la transferencia de datos a terceros países.

Será la quinta cuestión de la cuestión prejudicial de esta importante resolución judicial la que se encargue de abordar este elemento, y que ya entra en un terreno de gran dificultad interpretativa, con la interesante cuestión de dilucidar si la publicación de esos datos en Internet constituye una "transferencia a un país tercero de datos" en el sentido del artículo 25 de la Directiva. Tras una serie de consideraciones, entre las que puede destacar el escaso desarrollo de Internet, al momento de aprobarse la Directiva, interpreta el espíritu de esa "transferencia" como elemento concreto y especial ya que "cada vez que se publican datos personales en una página web, dicha transferencia será forzosamente una transferencia a todos los países terceros en los que existen los medios técnicos necesarios para acceder a Internet. El régimen especial que prevé el capítulo IV de la citada Directiva se convertiría entonces necesariamente, por lo que se refiere a las operaciones en Internet, en un régimen de aplicación general"[931]. Y establece la inoperabilidad de un pronunciamiento jurídico contrario: "... en efecto, en cuanto la Comisión detectara, con arreglo al artículo 25, apartado 4, de la Directiva 95/46, que un solo país tercero no garantiza un nivel de protección adecuado, los Estados miembros estarían obligados a impedir cualquier difusión de los datos personales en Internet.", terminando la cuestión en que "procede responder a la quinta cuestión que no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25."[932]

1.3 Transferencias de datos personales en el ámbito de la infracción penal.

Es la Directiva 2016/680, como hemos estudiado, la que se encarga de esta especialidad penal en la protección de datos europea. También en los supuestos de las transferencias internacionales de datos en ese ámbito.

Así, su Capítulo quinto (artículos 35 a 40, que sigue igualmente la estructura normativa marcada en el Reglamento General), contempla el mandato a los Estados miembros a

[931] Párrafos 67,68 y 69.
[932] Párrafo 71.

seguir en los flujos y transferencias internacionales de datos a un tercer país o a una organización internacional, incluidas las ulteriores a las mismas, que no requerirán autorización específica cuando estén basadas en una decisión de adecuación de garantía adoptada previamente por la Comisión. En ausencia de este acto de la Comisión, los Estados miembros podrán ejercitar ese papel de aval garantista en esta protección en la transferencia cuando "a) se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante, o b) el responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales....",[933] o para situaciones específicas en ausencia también de este último supuesto de toma de decisión estatal.[934]

Además, esa idoneidad de transferencia se puede dar para casos concretísimos, descendiendo a nivel de interesado si así lo prevé el Derecho de la Unión o del Estado miembro para las autoridades competentes en la investigación y persecución penal, según el artículo 39.[935]

[933] Artículo 36, donde se reproducen los elementos del artículo 45 del Reglamento que la Comisión tendrá en cuenta para esa declaración de idoneidad. Y artículo 37.

[934] Artículo 38, que prevé acto concreto de decisión de los Estados miembros "únicamente cuando la transferencia sea necesaria: a) para proteger los intereses vitales del interesado o de otra persona; b) para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales; c) para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país; d) en casos individuales a efectos del artículo 1, apartado 1, o e) en un caso individual para el establecimiento, el ejercicio o la defensa de acciones legales...", que sigue la lógica y estructura si bien no el contenido del artículo 49 del Reglamento.

[935] Que nos dice que: "únicamente si se cumplen las demás disposiciones de la presente Directiva y se satisfacen todas las condiciones siguientes: a) la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente de la transferencia según dispone el Derecho de la Unión o del Estado miembro a los fines expuestos en el artículo 1, apartado 1; b) la autoridad competente de la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado en cuestión son superiores al interés público que precise de la transferencia de que se trate; c) la autoridad competente de la transferencia considere que la transferencia a una autoridad competente del tercer país a los fines que contempla el artículo 1, apartado 1, resulta ineficaz o inadecuada, sobre todo porque no pueda efectuarse dentro de plazo; d) se informe sin dilación indebida a la autoridad competente del tercer país a los fines que contempla el artículo 1, apartado 1, a menos que ello sea ineficaz o inadecuado; e) la autoridad competente de la transferencia informe al destinatario de la finalidad o finalidades específicas por las que los datos personales vayan a tratarse por esta última solamente cuando dicho tratamiento sea necesario."

En lo relativo a las transferencias internacionales también los Considerandos (66 a 73) se explayan más en su detalle, quizá por la importancia que a la situación de amenaza de terrorismo global se viene justamente prestando. Así, se prevé la posibilidad de actuación de la Comisión para declarar un "nivel adecuado de protección de datos" de otros países y el "Estado de Derecho, el acceso a la justicia y las normas y principios internacionales en materia de derechos humanos, y su Derecho tanto general como sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el Derecho penal y el orden público", del país para tomar su decisión (Considerandos 66 y 67).

Como solvente aportación doctrinal sobre la Directiva 2016/680, y particularmente orientada a su regulación de las transferencias internacionales de datos en su ámbito, citaremos a Sánchez Domingo (2017), que, desde la óptica penal, observa un avance importante regulatorio con la Directiva (y sobre todo, tras el Tratado de Lisboa), si bien aboga por una posible mayor intervención de las autoridades de control en la sustanciación y aclaración de este derecho en esos flujos internacionales de datos.

2. El fallido (pero duradero) "Safe Harbour" o Acuerdo de Puerto Seguro.

El Acuerdo de Puerto Seguro[936] ha regido durante todo el siglo XXI la relación de adecuación en las transferencias de datos de Europa a Estados Unidos, como estándar autorizado de protección de los mismos, con el visto bueno de la Comisión. Y ello hasta el año 2015, en el que la sentencia Schrems vendrá a dar un vuelco a esa certificación de garantía, para los datos de los ciudadanos europeos. Por tanto, ha sido un acuerdo fallido porque esta histórica sentencia ha venido a paralizar su validez y declararlo nulo, y duradero porque la "falta de adecuación" de esta declaración ha venido dando por bueno el flujo de datos entre la UE y Estados Unidos durante más de 15 años.

Basado como vimos en el artículo 25.6 de la Directiva, y en su habilitación por la Comisión para esta declaración de idoneidad sobre la protección equivalente de datos por parte de otros países y organizaciones internacionales, se traslada la garantía de esa idoneidad de protección a la vigilancia (si bien basada principalmente en principios) de la FTC, plasmado ello en la sección 5 de su Ley reguladora.

El Acuerdo se basa en siete principios generales de protección publicados por la FTC en fecha 21 de julio de 2000. Estos principios han sido el marco de protección sobre los que se ha garantizado en el tiempo de aplicación del Acuerdo, la protección de los datos de los europeos transferidos a Estados Unidos. Así, el principio de notificación (o información) será aquel por el que las entidades deberán informar a los particulares de los fines con los que cuales recogen y utilizan información sobre ellos. El principio de opción (o de opt-out) que sirve para excluir su información de divulgación o posteriores tratamientos. Igualmente se contemplan el principio de transferencia ulterior a terceros (implicando los de notificación y opción), así como el de seguridad. En quinto lugar está el de integridad de los datos, coincidente con los principios clásicos de finalidad y

[936] Aprobado en la Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

de uso proporcional. Asi como el clásico principio de acceso, incluyendo el derecho a corregir, modificar o suprimir.

Por último debemos señalar el principio de aplicación, incluyendo una vía de recurso independiente, asequible e inmediatamente disponible, un procedimiento de seguimiento y la obligación de subsanación por las entidades de los problemas derivados del incumplimiento de los principios (Anexo I del Convenio).

En ese marco se adquiere por las "FAQ's" (preguntas frecuentes) de la FTC en orientación de aplicación de esos Principios un rango jurídico que calificaremos como impropio, debido a la capacidad interpretativa inusitada de lo que, en forma, serían meras indicaciones de ayuda de la FTC, en verdaderos elementos de implementación de los principios que venían a regular los datos europeos transferidos a EE.UU. A ellas (FAQ's) se remite directamente el artículo 1 del Acuerdo (contenidas en el Anexo II).[937]

Hemos de decir que el Acuerdo es principalmente una declaración de remisión, y que no aporta una regulación novedosa y consensuada entre las dos orillas jurídicas del Atlántico, sino un visto bueno más o menos general de la Comisión a las garantías ofrecidas por la legislación americana, principalmente en la labor y regulación de la FTC (y en menor medida de la FCC) en la protección de la privacidad; y para que sea extensible a los ciudadanos europeos (que recordemos no tienen que moverse de casa para verse afectados por vía tecnológica). Además del carácter voluntario sobre la adhesión que regía para las empresas norteamericanas para este Acuerdo.

Ese posicionamiento garantista se ha visto por parte de la doctrina jurídica americana de manera encontrada. Algunas posiciones observan que esa aproximación europea es adecuada y optan por la consecución de un sistema integral de protección también en Estados Unidos (Reidenberg, 2001), mientras que otras la observa desde un punto de vista más escéptico, sobre todo en la desventaja que pudiera suponer para el posicionamiento europeo ante la Sociedad de la Información (Swire & Litan, 1999).

[937] Algunos autores lo cuestionaban abiertamente, los principios y su adecuación. Poullet (2000)

Particularmente interesante nos parece la posición de Robert Gellman (1999) desde esa óptica americana que considera, en contra de lo que pudiera parecer, que la aparición de la Directiva europea ha creado eficiencias beneficiosas para el negocio estadounidense, creando soluciones para el resto del mundo (y ello apuntamos también a través de los mecanismos de adecuación), al dotar de una solución jurídica exportable en esa armonización en un entorno jurídico multinivel.

Una vez pasado un tiempo se ha ido haciendo un seguimiento por parte de la Comisión sobre la ejecución y cumplimiento del Acuerdo. También la FTC ha ofrecido datos de las acciones que ha emprendido en base al acuerdo (Comisión, 2004).

En ese documento de 2004 ya la Comisión apuntaba[938]: "falta de transparencia o información defectuosa (...) falta de definición con respecto al concepto de tercero y, en algunos casos, no había un compromiso de ese tercero (...) en relación con el Acceso, la información que se ofrecía al respecto por parte de las empresas era muy vaga e imprecisa (...) La información sobre las actividades y finalidades era escasa..."

Además de contestaciones por parte de la FTC (2013)[939], en un toma y daca institucional (que viene a explosionar a partir del verano de 2013 en el que Edward Snowden relata al mundo a través de medios de comunicación serios la vigilancia masiva que Estados Unidos está llevando a cabo) defendiendo su labor de vigilante y aportando historial de trabajo al respecto. E igualmente en la comunicación al Parlamento Europeo por parte de la Comisión (2013)[940], todo ello a partir de las revelaciones de Snowden, que, podremos decir, es el primer detonador del Acuerdo, ya que pone en plena agenda política el riesgo sobre la privacidad a escala mundial, señalando a Estados Unidos como principal foco de riesgo.

Advierte así la Comisión (2013, 19) (antes de sus recomendaciones) al Parlamento de que: "Las empresas de la red, como Google, Facebook, Microsoft, Apple o Yahoo, tienen centenares de millones de clientes en Europa y transfieren datos personales para

[938] Coincidiendo con el análisis de Álvarez Caro y Recio Gayo (2015, 21-22)
[939] (Recuperado el 25 de septiembre de 2018): https://www.ftc.gov/public-statements/2013/11/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission
[940] (Recuperado el 25 de septiembre de 2018): http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290847_/com_com%282013%290847_es.pdf

su tratamiento en Estados Unidos a una escala inconcebible en el año 2000, cuando se creó el marco de puerto seguro.

Las deficiencias en lo que respecta a la transparencia y la aplicación del marco hacen que persistan problemas concretos que deben solucionarse:

a) la transparencia de las políticas de protección de la vida privada de los miembros de puerto seguro;

b) la aplicación efectiva de los principios de protección de la vida privada por parte de las entidades en Estados Unidos; y

c) el carácter efectivo de la aplicación.

Por otra parte, el acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de puerto seguro suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país."[941]

[941] Otro elemento importante relacionado y que nos ofrece similares inquietudes por parte de la Comisión es la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre cómo restablecer la confianza en los flujos de datos entre la UE y EE.UU. (2013)

3. La sentencia Schrems.[942]

Este pronunciamiento judicial supone la definitiva defunción jurídica del Acuerdo de Puerto Seguro, que ya venía estando en entredicho tras las evaluaciones del Acuerdo reseñadas y los planteamientos ofrecidos por la información de vigilancia masiva.

La petición de decisión prejudicial planteada por la *High Court* de Irlanda viene a preguntar por la interpretación de los artículos 7, 8 25, 28 y 47 de la Directiva 95/46/CE. Reclamación de interpretación de particular relevancia para estos supuestos de transferencia y flujos de datos de los que nos ocupamos aquí, y que van desde la Unión Europea a Estados Unidos. Sentencia, por tanto, de gran calado en la determinación de la protección de datos en la era de la globalización, y particularmente para la relación entre Estados Unidos y la Unión Europea en su defensa. Implica, así, no solo la interpretación de la Directiva, sino también la aplicación de la CDFUE, y que se da entre el demandante austriaco Sr. Schrems y el "Data Protection Commissioner" irlandés ante la negativa de este último de tramitar su reclamación ante Facebook Ireland Ltd.

El caso incide directamente en la actividad de las autoridades de control pero, sobre todo, en la transferencia de datos a país tercero y a sus principios de validez. Replantea además una de las principales decisiones ejecutivas en este campo, como era el Acuerdo de Puerto Seguro con Estados Unidos en relación con la transferencia de datos entre aquel país y Europa (los dos principales bloques nacionales y mercados de tratamiento de datos en el mundo).[943]

---

[942] Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015. Maximillian Schrems contra Data Protection Commissioner. Asunto C-362/14.
Y la historia continúa ya que la sentencia del Tribunal de Justicia (Gran Sala) de5 de junio de 2018, Sentencia en el asunto C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig-Holstein GmbH, también interpuesta en procedimiento prejudicial, en este caso por tribunal alemán, y con Facebook como protagonista, sigue la estela de la sentencia Schrems y su interpretación del artículo 28 de la Directiva y establece que la autoridad de protección de los datos del estado miembro en el que el correspondiente administrador de Facebook esté domiciliado tiene capacidad de actuación tanto contra ese administrador como contra la filial de Facebook en ese etado establecida.

[943] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida

El usuario de Facebook (a través de su filial en Europa *Facebook Ireland Ltd.*), nacional austriaco y ciudadano europeo Schrems, residente en Austria, ve tratados sus datos en Estados Unidos, donde se ubica el responsable de su tratamiento. El 25 de junio de 2013, Schrems presenta reclamación al Comisario irlandés de protección de datos prohibiendo a *Facebook Ireland Ltd.* transferir sus datos personales a Estados Unidos, alegando la falta de protección equivalente a la protección de la que goza como europeo, y relacionándolas directamente (y en directa colación), con las revelaciones del ex analista de la NSA Edward Snowden. El órgano de protección de datos de Irlanda la desestima por pretensión infundada. Decisión que Schrems recurre ante la *High Court* irlandesa, aceptando este Tribunal que las informaciones reveladas por Snowden daban crédito a la comisión de "importantes excesos" por la agencia de inteligencia americana y por otros organismos federales estadounidenses; si bien reconoce las limitaciones del Derecho irlandés en el asunto, reclamando la intervención interpretativa del Tribunal de Luxemburgo.

Siendo particularmente conciso y certero en sus dos cuestiones: "1) En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520?"

En primer lugar "sobre las facultades de las autoridades nacionales de control, a las que se refiere el artículo 28 de la Directiva 95/46", empieza respondiendo el Tribunal con alusión a la reiterada Jurisprudencia que considera a la Directiva y a su funcionamiento conforme a los Derechos Fundamentales y a la Carta de la Unión sobre los mismos[944]. E

privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

[944] Párrafos 38 a 42 de la sentencia

incide en la importante labor que los organismos de protección de datos deben desempeñar en la defensa y garantía de esos derechos, particularmente en el de protección de la intimidad y la privacidad. Destaca que "la operación consistente en hacer transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46"; y recordando con claridad sus funciones (y de paso particularmente al Comisario irlandés de protección de datos): "las autoridades nacionales de control, conforme al artículo 8, apartado 3, de la Carta y al artículo 28 de la Directiva 95/46, están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales, toda autoridad nacional de control está investida, por tanto, de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por la Directiva 95/46."[945]

A partir de ahí va pasando la sentencia a analizar el importante cometido de la Comisión encomendado en el artículo 25.6 de la Directiva, para establecer en decisiones ejecutivas la conveniencia sobre si terceros países u organizaciones internacionales disponen de un nivel de protección adecuado, con la consiguiente capacidad de transferencia segura de esos datos de ciudadanos europeos. Si bien este tipo de decisiones no deben entenderse como "carta blanca" avalada por la Comisión para la transferencia de esos datos ni deben ser obstáculo para la labor de investigación y protección de las autoridades nacionales de protección de datos, según el TJUE.[946]

Por tanto ese tipo de decisiones de la Comisión, recuerda el Tribunal, aún más en su perspectiva de gran incidencia sobre los derechos fundamentales, no pueden escapar a la independiente revisión de esas autoridades. Recuerda el Tribunal directamente el espíritu propio de la Unión fundada en el Derecho, y particularmente en los valores y derechos fundamentales, a escala, como se ha venido llamando, multinivel, e integral. Y

[945] Párrafos 43 a 47 de la sentencia.

[946] Párrafos 48 a 51 de la sentencia. Expresándolo certeramnete el párrafo 53 "...una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos".

lo expresa en la manera de construcción del Derecho y de la Unión tan propia del Tribunal: "Hay que recordar en ese sentido la reiterada jurisprudencia del Tribunal de Justicia según la cual la Unión es una Unión de Derecho en la que todos los actos de sus instituciones están sujetos al control de su conformidad, en particular, con los Tratados, con los principios generales del Derecho y con los derechos fundamentales (…) Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25, apartado 6, de la Directiva 95/46 no pueden quedar excluidas de ese control."[947]

Para pasar ya más adelante el Tribunal a la propia declaración de validez de la Decisión de la Comisión que viene fundamentando el asunto. Revisa por tanto el TJUE la Decisión a la luz de la CDFUE, y no de la Directiva propiamente, dando un peso específico significativo a los derechos fundamentales y su defensa en la protección y garantía de los datos personales en Europa. El enlace, por tanto, es ya directo e indiscutido, con independencia del mercado común o de las necesidades de éste en su relación con otros países; y en este caso, con países tan poderosamente mercantiles en lo tecnológico como EE.UU. (sin hablar ya de la fuerza que Facebook tiene en ese mundo del comercio digital).[948]

Admite el Tribunal que el concepto de protección "adecuado" no es semejante a que exista una protección idéntica, pudiendo ser los medios para la protección de datos de esos países "diferentes" a los establecidos en la Unión. Y destaca la obligación de la Comisión de estar pendiente de manera permanente sobre la idoneidad de esa adecuación de protección. Y alude además a la necesidad estricta de esa supervisión por parte de la Comisión.[949] Para pasar por último a analizar, técnica y jurídicamente, el articulado controvertido de la Decisión 2000/520/CE al caso que se presenta.[950]

[947] Párrafos 57 y 60 de la sentencia.
[948] Párrafo 67 y siguientes de la sentencia.
[949] En su párrafo 75 "al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas…" Y en su párrafo 76: "…dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido."
[950] Párrafos 79 a 106.

Y tras todo ello, entra ya a cuestionar directamente la idoneidad del Acuerdo a la luz de la protección europea ya que " la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas".[951]

El principio de "Puerto Seguro", se basa en el sistema de autocertificación por el tercer país. Sistema cuya fiabilidad se cuestiona, como se encarga el Tribunal de recordar en la linea del espíritu que recorre toda la sentencia: "en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales" haciendo esta Decisión "posibles así injerencias, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos." Injerencias que en el acuerdo no se encuentran ni siquiera contempladas para su posible prevención y evitación.[952]

Igualmente debemos destacar que la propia Comisión, en comunicaciones posteriores, parece cuestionar el nivel de protección contenido en el propio Acuerdo. Se cuestiona directamente por la sentencia que esa transferencia de datos que posibilita la Decisión de la Comisión, se base en exigencias mínimas de protección, y se circunscriba en su injerencia de penetración en los datos personales y en la vida privada de los europeos, a lo estrictamente necesario. Lo expresa así: "no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a

[951] Párrafo 86.
[952] Párrafos 87 a 89.

fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización".[953]

Y además, argumenta el Tribunal que "se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta"[954] Palabras del Tribunal que pone en entredicho la idoneidad misma del sistema ejecutivo de garantías planteado por la Comisión sobre la base de sus decisiones de adecuación en estas transferencias internacionales de datos.

De igual forma se analiza el artículo 3 de la Decisión, que priva a las autoridades nacionales de las posibilidades de control que les vienen siendo propias en virtud de la Directiva. Algo para lo cual la Comisión no tiene competencia de decisión ni regulación en base al mandato del 25 de la Directiva.

Por todo ello la sentencia declara inválidos tanto el artículo 1 como el 3 de la Decisión, que a su vez provocan la invalidez de la Decisión de la Comisión en su conjunto. Dejando así por tanto inválido y sin efecto el Acuerdo de Puerto Seguro con Estados Unidos, y cuestionada la legitimidad, legalidad y eficacia de la adecuación de las transferencias de datos a aquel país en virtud de la misma. En una sentencia de alcance histórico en el acervo de la Unión.[955]

Comprobamos así el carácter de contrapeso de la sentencia en el equilibrio de la privacidad y la seguridad, que consigue ajustar un poco la balanza hacia el derecho fundamental que nos ocupa, tal y como se hace eco Puero y Sferrazza Taibi (2018).

[953] Párrafo 93.
[954] Párrafo 94.
[955] Párrafos 95 a 106.
En este sentido ver Declaración del Grupo del Artículo 29 sobre las consecuencias de la sentencia de (2016), en los que establece 4 garantías esenciales para el tratamiento de datos por los servicios de inteligencia: "A. Processing should be based on clear, precise and accessible rules (...)B.Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual. C. An independent oversight mechanism should exist (…) D. Effective remedies need to be available to the individual..."

4. El Acuerdo "Privacy Shield" o Escudo de Privacidad.

El Acuerdo de Escudo de Privacidad[956], ha venido a ser, tras las arduas negociaciones entre la Comisión y el gobierno de Estados Unidos, la norma transaccional que viene a sustituir al acuerdo de Puerto Seguro en el mismo objeto de regulación de adecuación de protección de los datos en ese continuo devenir de transferencia entre los dos bloques mundiales.

Un buen resumen y enfoque de la transición del Puerto Seguro al Escudo de Privacidad, de sus causas y consecuencias, y análisis certero de lo que viene a suponer el *Privacy Shield* (con óptica americana) nos lo ofrecen Weiss & Archick (2016). Una de sus principales conclusiones es que el "Privacy Shield" presenta mejoras importantes respecto al "Safe Harbour": unos compromisos fortalecidos con mayores obligaciones para las empresas americanas, un mayor poder y autoridad para la FTC en su cumplimiento, preceptos y salvaguardas más claras y obligaciones añadidas de transparencia y una efectiva protección para los ciudadanos de la UE con varias posibilidades en su garantía de protección, con capacidad por ejemplo, de reclamación individual a las compañías responsables del tratamiento (2016, 10).

Debemos aludir además al documento de investigación del Parlamento Europeo sobre la puesta en marcha del *Privacy Shield* (Monteleone y Puccio, 2017). El documento, que es un elemento de análisis sobre los Acuerdos y la transición entre los mismos incide también, junto al del Congreso americano y al igual que los del SEPD y del Grupo de trabajo del artículo 29, en el avance que supone el Escudo de Privacidad respecto al Puerto Seguro pero refleja también críticas y preocupaciones al igual que elementos de posible mejora.[957]

[956] Se ha dispuesto una guía y una página web sobre el mismo (Recuperados el 30 de agosto de 2018):http://ec.europa.eu/justice/data-protectorio/files/eu-us_privacy_shield_guide_es.pdf http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

[957] De igual manera, como análisis de esa transición del Puerto Seguro al Escudo de Privacidad podremos citar a Ortega Giménez (2017). De igual manera citaremos a Chicharro Lázaro (2017) y su alusión a la necesidad de una asociación estratégica digital entre las dos posturas europea y americana con respeto a los derechos fundamentales. A nivel más general Prislan (2016) se pregunta si existe una grieta digital entre EE.UU y la U.E., llegando a la respuesta de la necesaria reconciliación de posturas.

El instrumento jurídico que lo adopta y en el que se contiene toda la información relevante al mismo es la Decisión de ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.

Esta norma ejecutiva declara, así, adecuada la protección que brinda Estados Unidos a la privacidad de los europeos en las relaciones de estos con las empresas de ese territorio, y por el que se aprueba el acuerdo del "Escudo de Privacidad" con aquel país.

Es evidente que los vínculos comerciales entre Estados Unidos y la Unión y los flujos de datos que ellos conllevan siguen siendo un elemento de primera necesidad para los dos bloques regionales occidentales. Así, el Acuerdo se impone como una necesidad (y más en la dependencia tecnológica que vivimos) tras la invalidez judicial del de Puerto Seguro. Es por ello que nos encontramos ante un instrumento jurídico mucho más desarrollado y pormenorizado, que ha ido cubriendo los defectos, al menos más sobresalientes, del anterior acuerdo, presentando mayores garantías de protección a nivel general. Si bien siguiendo el principio de la autocertificación por parte de las empresas americanas como elemento principal de actuación en esa protección.

4.1 Objeto y Principios.

El objeto del Acuerdo está previsto para los datos que van desde la vieja Europa a territorio norteamericano (si bien porque el amparo de la regulación europea en sentido de flujo contrario está mejor asegurado), es decir, para "aquellos que hayan sido transferidos desde la Unión a entidades establecidas en los Estados Unidos que figuren en la denominada «lista del Escudo de la privacidad»". Ya que se estima necesario para el correcto seguimiento del Acuerdo que: "...las partes interesadas, entre ellas las personas a las que se refieren los datos, los exportadores de datos y las autoridades de protección de datos («APD») deben poder identificar a las entidades que suscriban los principios. A tal efecto, el Departamento de Comercio (o su representante) se ha comprometido a mantener y poner a disposición del público una lista de las entidades que han autocertificado su adhesión...". Destacándose la importante responsabilidad de

ejecución y supervisión e la FTC en este ámbito (artículo 1.3 de la Decisión y punto 31 de la Decisión).[958]

Si las empresas se adhieren a este sistema de autocertificación de privacidad deberán entonces cumplir con los principios establecidos de manera obligatoria en el Acuerdo, que son los principios establecidos al efecto por la FTC norteamericana. Estos son:

– Principio de notificación, que establece la obligación de informar a los interesados por las entidades sobre elementos fundamentales del tratamiento.

– Principio de opción en el caso de que se de un nuevo fin compatible con el originario, los interesados se pueden oponer al tratamiento.

– Principio de responsabilidad de la transferencia ulterior, para que no se eluda la protección con posterioridad.

– Principio de seguridad.

– Principio de integridad de los datos y de limitación de la finalidad, por el que los datos personales, además de ser fiables exactos, completos y actuales, deberán limitarse a la finalidad del tratamiento.

– Principio de acceso.

– Principio de recurso, aplicación y responsabilidad, como mecanismos de garantía de la eficacia de lo estipulado en el acuerdo. Implicando una vía de recurso independiente e inmediatamente disponible, procedimientos de seguimiento y comprobación y obligación de subsanación de los incumplimientos.

Como principios complementarios a estos principios generales, la FTC nos presenta los siguientes:

[958] La lista de las empresas aheridas al "escudo de privacidad" se pueden consultar en la página sobre el Acuerdo habilitada por la FTC (Departamento de Comercio) estadounidense (Recuperada el 12 de septiembre de 2018):
https://www.privacyshield.gov/list

– Para los datos sensibles no es necesario el consentimiento explícito y positivo.

– Las excepciones propias por razón de la Libertad de Prensa.

– La falta de responsabilidad subsidiaria para los proveedores y operadores intermedios no responsables del tratamiento.

– La excepción de los principios para la "diligencia debida" y secreto en los casos de auditoría de esas empresas, durante la realización de la misma.

– El compromiso de colaboración con las autoridades de protección de datos de la UE.

– El principio de autocertificación.

– El principio de verificación.

– El desarrollo del principio de acceso.

– La especialidad de los datos en recursos humanos.

– La obligatoriedad del contrato para transferencias ulteriores.

– El desarrollo de la resolución de conflictos y aplicación.

– El del momento del ejercicio del derecho de exclusión (opción).

– El principio de información sobre viajes.

– El principio sobre productos médicos y farmacéuticos.

– El principio de información de registros públicos e información accesible al público.

– El principio de las solicitudes de acceso de las autoridades públicas.

El Anexo I de la Decisión contiene el modelo de arbitraje a utilizar en las reclamaciones por las empresas norteamericanas en base a este acuerdo para "ofrecer un mecanismo rápido, independiente y equitativo, opcional para los ciudadanos, para la resolución de

las infracciones denunciadas de los principios no resueltas por uno de los mecanismos del Escudo de la privacidad".

4.2 Posicionamientos institucionales.

El acuerdo *Privacy Shield*, precisamente por la causa y el carácter de su aparción y necesidad de aprobación, tras la sentencia Schrems y el replanteamiento profundo que el TJUE ha provocado sobre el asunto, ha hecho que las instituciones europeas y sus órganos relacionados con la protección del derecho manifiesten con interés su posición sobre el nuevo acuerdo.

Así podemos aludir a la Opinión del Supervisor Europeo de Protección de Datos (2016) sobre el Acuerdo.[959] El SEPD reconoce el valor de un marco jurídico sostenible para las transmisiones de datos con fines comerciales entre los dos bloques en un mundo hiperconectado, manteniendo una actitud positiva ante lo que supone este paso del Escudo de Privacidad, sobre todo en cuanto a transparencia se refiere. Si bien también indica algo que venimos observando a lo largo de este trabajo y es que la excepción de la seguridad se ha convertido en la regla.

El SEPD nos presenta un balance positivo respecto a los principios y a la participación de las instituciones estadounidenses en la comparativa entre el Escudo de Privacidad y el Puerto Seguro, si bien considera los avances insuficientes. No se persigue, citando la sentencia Schrems, una protección idéntica, si bien sí que se requiere una equivalencia esencial. Lo que requiere abarcar la totalidad de los elementos clave del marco vigente en la UE en materia de protección de datos, abogando por una solución "sólida e integral", lo que significa introducir mejoras para proteger el respeto a largo plazo de los derechos y libertades fundamentales de los europeos, "y sustituir el escudo protector de la intimidad por un marco jurídico más estable y robusto que impulse las relaciones transatlánticas".

[959] Y su resumen en español (recuperado el 30 de agosto de 2018): https://edps.europa.eu/sites/edp/files/publication/16-07-15_privacy_shield_adequacy_decision_es.pdf

También es de interés la Opinión del Grupo del artículo 29 (2016)[960] en la que el grupo de expertos reconoce igualmente las mejoras respecto al Puerto Seguro que supone esta Decisión de adecuación. Si bien también observa aspectos de mejora, al igual que en la opinión del SEPD.

Tras la reivindicación que el grupo de trabajo hace de las autoridades de protección en un mundo que, desde el año 2000 del Acuerdo de Puerto Seguro, ha avanzado enormemente en la recopilación y uso de datos, observa además la necesidad de que esa adecuación se equipare en mayor medida con los principios de la UE y las previsiones del Reglamento. El Grupo manifiesta su crítica concreta en algunos elementos importantes como la no previsión del principio de conservación de datos o el marco de protección insuficiente para las transferencias ulteriores a otros países u organizaciones internacionales. También critica la complejidad de los mecanismos de recursos y de garantías. Si bien también reconoce el gran paso respecto al Puerto Seguro en lo relativo al acceso en temas relacionados con la seguridad nacional y el "Law Enforcement". Aunque, apunta, no se excluye la posibilidad de vigilancia masiva e indiscriminada con el Acuerdo. El grupo ve con buenos ojos el mecanismos del "redress" (de reparación) y del Defensor del Pueblo para los derechos de los ciudadanos de la UE, si bien recela de la suficiente independencia de la figura.

Por último, y muy relacionado con las reacciones al Acuerdo, debemos nombrar la Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos.[961] En el que el Parlamento es consciente de la importancia económica del flujo transatlántico de datos, junto con la necesidad de protección que requieren esos datos, animando a la Comisión a la buena consecución y vigilancia de una y otra, respectivamente.[962]

[960] Recuperado el 30 de agosto de 2018: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

[961] Recuperado el 30 de agosto de 2018: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//ES

[962] Para mayor análisis la página del Servicio de Investigación del Parlamento Europeo hay un completísimo análisis con sus respectivos enlaces, sobre las reacciones a la sentencia Schrems (recuperado el 30 de agosto de 2018): https://epthinktank.eu/2016/04/18/reactions-to-the-eu-us-privacy-shield-the-successor-to-the-safe-harbour-agreement/

En este sentido algunos autores (Cole & Fabbrini, 2016) proclaman un acuerdo más integral y definitivo, reclamando su incorporación de protección en un acuerdo transatlántico amplio, o el posicionamiento crítico de otros autores (Deighton, 2016) y de algunas ONG's como Privacy International.[963]

4.3 Contenido de los Principios.

Es el Anexo II del Acuerdo el que se encarga de la definición y contenido de los principios expuestos. Empieza el anexo estableciendo que: "Los Estados Unidos utilizan un enfoque sectorial que se basa en una mezcla de legislación, regulación y autorregulación. Dadas estas diferencias y para dotar a las entidades de los Estados Unidos de un mecanismo fiable para las transferencias de datos personales a los Estados Unidos procedentes de la Unión Europea y, a la vez, garantizar que los interesados de la UE continúen beneficiándose de protección y garantías eficaces, tal como exige la legislación europea con respecto al tratamiento de sus datos personales cuando son transferidos a países no pertenecientes a la UE, el Departamento de Comercio publica estos principios del Escudo de la privacidad". Si bien las conocidas razones de seguridad, además de posibles excepciones legales comunitarias o nacionales matizan también aquí el posible alcance de la adhesión: "La adhesión a estos principios puede verse limitada por: a) exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que origine conflictos de obligaciones o prevea autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios está limitado en la medida necesaria para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; o c) por excepción o

---

El Tribunal de Estrasburgo también se ha interesado por las implicaciones de la sentencia Schrems, en relación con el caso de su jurisdicción, asunto Zakharov v. Russia. (recuperado el 12 de septiembre de 2018): https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/

[963] Recuperado el 12 de septiembre de 2018: https://privacyinternational.org/node/832

dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables...” (Puntos 1 y 5 de la Síntesis).

Debemos decir que es en este Anexo donde se va desgranando la sustancia jurídica que, bajo el enunciado de principios (bien generales o los complementarios relacionados), va perfilando toda la regulación del Acuerdo a la que los interesados pueden atenerse.

Una vez adheridas las entidades se ven obligadas por el contenido del Acuerdo y de los principios en él desarrollados. Pasaremos ahora a ahondar un poco más en los mismos, los cuáles, si bien siguen el espíritu del Reglamento General de Protección de Datos, están lejos de ofrecer una protección equivalente a la del mismo.

El principio de notificación implica la información por parte de la entidad a los particulares sobre su participación en el Escudo de Privacidad y su compromiso con sus principios para los datos procedentes de la UE, los tipos de datos personales recopilados, los fines, los posibles terceros a los que se les pueda suministrar los datos, derechos u opciones que les asisten, y el organismo para tramitar y resolver sus reclamaciones, con independencia de que sea: “1) el panel designado por las APD, 2) un organismo de resolución alternativa de conflictos radicado en la UE, o 3) un organismo de resolución alternativa de conflictos radicado en los Estados Unidos”. Además de informar sobre las competencias y funciones de la FTC y de la posibilidad de arbitraje vinculante.

El Principio de opción se sustancia en la posibilidad de elegir excluir el tratamiento por los particulares “si su información personal: i) puede divulgarse a un tercero, o ii) puede utilizarse para un propósito sustancialmente distinto del objetivo inicial para el que fue recogida o autorizada posteriormente por el particular”. Si bien este principio puede dejarse sin efecto, “cuando la divulgación se realice a un tercero que actúe como agente para realizar las tareas en nombre de la entidad y siguiendo sus indicaciones”. Siendo necesaria la suscripción de contrato entre los mismos.

Respecto a su ejercicio, y en aquellos con fines de marketing directo, se podrá ejercitar en cualquier momento, si bien con los límites de tiempo razonables que establezca la entidad.

Para cumplir con la responsabilidad de la transferencia ulterior “solo se podrán transferir datos: i) con fines limitados y específicos, ii) en virtud de un contrato (o de un acuerdo similar dentro de un grupo de empresas (29)), y iii) únicamente si dicho contrato ofrece el mismo nivel de protección...” (Punto 28 de la Decisión).

La seguridad y el principio de integridad de los datos limitados a su finalidad, se entienden desde la óptica del buen manejo integral del tratamiento, con medidas razonables y apropiadas para su cumplimiento y para la información relevante a efectos del tratamiento, sin una conservación excesiva de los mismos.

El principio de acceso implica “corregir, modificar o suprimir dicha información si resultase inexacta, o haya sido tratada infringiendo los principios”, al igual que “podrá restringirse en circunstancias excepcionales en las que puedan violarse los derechos legítimos de terceros o cuando la carga de trabajo o el gasto de proporcionar el acceso sean desproporcionados en relación con los riesgos para la privacidad”. También se realiza mención especial a la protección en el acceso de la información comercial confidencial. Deben, así, las entidades contestar en un plazo razonable y de una manera también razonable y fácilmente comprensible.

Nos llama la atención la consideración en su consentimiento, como hemos visto, de no ser explícito ni positivo para los datos sensibles, referidos principalmente a datos sanitarios, de intereses vitales del interesado, de origen político, filosófico o religioso o sobre obligaciones laborales. Y ello parece ser una concesión a las entidades americanas para facilitarles la tarea de su recopilación de datos.

Debemos por último criticar, junto con Blasi Casagran (2017), que, a pesar de las mejoras respecto al anterior Acuerdo, estos principios que rigen no representan protecciones equivalentes a las contenidas en las normas europeas.

4.4 Mecanismos para atender las reclamaciones.

El derecho a recurso implica, en lógica jurídica, el derecho a su procedimiento y a corregir y resarcir los problemas surgidos por el incumplimiento. Sobre el mecanismo de recurso y tramitación y ejecución de reclamaciones, se encarga de su desarrollo el punto 2.3 de la Decisión, que establece de manera más pormenorizada como se podrá ejercitar este derecho clave del acuerdo.

Las entidades tienen la "posibilidad de comprometerse voluntariamente a cooperar con las autoridades de protección de datos de la UE." Salvo si son entidades de recursos humanos para las que la colaboración es obligatoria. Siendo otras opciones "la resolución alternativa de litigios (RAL) independiente o programas de privacidad desarrollados por el sector privado que incorporen los principios en sus normas". Deja, por tanto, abierta la posibilidad de reclamación, lo que podemos intuir como un problema para la seguridad jurídica en la ejecución. Sobre todo teniendo en cuenta que se prevé, para el caso de reclamaciones no resueltas, el recurso al arbitraje. Si bien se percibe también algún esfuerzo de concreción como el del establecimiento del plazo de 45 días para que la entidad responda, una vez recibida la reclamación por las autoridades, o la posibilidad de "reclamar directamente a un organismo independiente de solución de conflictos (en los Estados Unidos o en la Unión) (…) o a una autoridad nacional de protección de datos". Autoridades que darán además "asesoramiento a través de un panel informal". Junto con la regulada implicación de la FTC y del Departamento de Comercio y con previsión expresa de sus poderes de investigación en base a la sección 5 de la FTC Act, para su correcta aplicación. Por último, y haciendo la labor de elemento de superior revisión administrativa, tenemos la posibilidad de "solicitar un procedimiento de arbitraje vinculante al «panel del Escudo de la privacidad»", y que estará "integrado por un grupo mínimo de veinte árbitros designados por el Departamento de Comercio y la Comisión en función de su independencia, su integridad y su experiencia en el Derecho estadounidense en materia de privacidad y el Derecho de la Unión en materia de protección de datos". Se encuentra facultado, así, para compensar de manera no monetaria la subsanación de los

incumplimientos del acuerdo. Para solicitar daños y perjuicios se nos remite al Derecho estadounidense y su vía judicial.[964]

El desarrollo de los modelos de arbitraje, los requisitos para los mismos y su carácter vinculante se establece en el Anexo 2 de la Decisión para el caso de las reclamaciones no resueltas. La figura encargada de sus resoluciones es el Panel de arbitraje que se compondrá sobre una lista compuesta por la FTC y la Comisión de, como mínimo, 20 árbitros independientes, para un período de 3 años renovables por igual periodo. Igualmente tienen las dos instituciones el encargo de adoptar los procedimientos arbitrales ante este Panel (letras F y G del Anexo 2).

Como elemento adicional de protección se contempla la posibilidad de poner fin a las transferencias de datos por parte de una Autoridad: "cuando una APD, tras recibir una reclamación de un interesado de la UE, considere que la transferencia de datos personales a una entidad en los Estados Unidos se realiza violando la legislación de la UE sobre protección de datos, incluso cuando el exportador de datos de la UE tenga razones para creer que la entidad no se ajusta a los principios, también podrá ejercer sus competencias respecto del exportador de datos y, si es necesario, ordenar la suspensión de la transferencia" (punto 60).[965]

4.5 La especial alusión al acceso a los datos transferidos en base al "Privacy Shield" por parte de los poderes públicos estadounidenses.

Es evidente que el recelo provocado tras el conocimiento de las revelaciones de Snowden subyace en todo el Acuerdo, y en las previsiones de la Decisión. Así ésta dedica una capítulo especial a advertir qué ocurre con esos datos una vez transferidos a Estados Unidos, y la manifestación "de portarse bien" por parte de los órganos de

[964] Puntos 38 a 63.

[965] Apuntar por último la guía sobre el escudo de privacidad que ha preparado la Comisión para orientar a los usuarios sobre su uso y derechos. Aquí en su traducción por parte de la AEPD (Recuperado el 1 de diciembre de 2017): https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Guia_acerca_del_Escudo_de_Privacidad.pdf

inteligencia y del "law enforcement" de Estados Unidos (Anexo VI), aportando además carta firmada del secretario de Estado John Kerry (Anexo III) que aboga por "crear un nuevo mecanismo de supervisión de las injerencias con fines de seguridad nacional". Ese nuevo mecanismo será un "Defensor del Pueblo en el ámbito del Escudo de la privacidad, que será independiente de los servicios de inteligencia". Además de aportar carta del Departamento de Justicia (Anexo VII) con las "limitaciones y salvaguardias aplicables al acceso a los datos y a su utilización por parte de los poderes públicos a efectos de aplicación de la ley y otros fines de interés público" (punto 65).[966]

En los siguientes puntos (68 a 90) la Decisión se encarga de ir relatando las limitaciones para los poderes públicos de la seguridad nacional estadounidense sobre esos datos europeos transferidos. Con especial atención a la tutela judicial efectiva en su defensa, capacidad de supervisión (a través del *Privacy and Civil Liberties Oversight Board* o Consejo de Supervisión de la Privacidad y de las Libertades Civiles y de los Tribunales FISC de la FISA), y la previsión de recursos individuales (que hace una relación de las leyes estadounidenses que incluyen casi todas las estudiadas en este trabajo)[967] (puntos 91 a 135).

En este capítulo Tercero de la Decisión, por tanto, se va haciendo un recorrido de análisis exhaustivo sobre las limitaciones que el Derecho estadounidense presenta para el acceso por motivos de seguridad nacional, que van desde la Orden presidencial de Obama "PPD-28" adoptada el 17 de enero de 2014, con declaraciones de garantía a la

[966] Igualmente se presentan Cartas de diversos responsables de instituciones como implicaciones relacionados en la privacidad estadounidense dirigidas a los Comisarios y responsables equivalentes de la Unión y que relatan las garantías, proyectos y medidas relacionadas con la protección de la privacidad en cada uno de sus campos de actuación. Así tenemos: En el ANEXO I la Carta de la Secretaria de Comercio estadounidense, Penny Pritzker de 7 de julio de 2016, la Comisaria Jourová (de Justicia, Consumidores e Igualdad de Género). En el Anexo I Carta del Subsecretario de Comercio Internacional en funciones, Ken Hyatt a la misma Comisaria. E igual destinataria tiene la Carta de la Presidenta de la Comisión Federal de Comercio, Edith Ramirez de 7 de julio de 2016 en el ANEXO IV, así como la Carta del Secretario de Transporte estadounidense, Anthony Foxx de 19 de febrero de 2016 en el ANEXO V. El Apéndice A nos ofrece una síntesis de la labor y funciones de la FTC. Además en los ANEXOS VI y VII se presentan comunicaciones intergubernamentales entre instituciones estadounidenses sobre privacidad en asuntos de inteligencia y seguridad y que son de interés para el acuerdo; como son respectivamente la Carta del Asesor General, Robert Litt de la Oficina del Director de Inteligencia Nacional de 22 de febrero de 2016 , al igual que la Carta del Asistente del Fiscal General y Consejero de Asuntos Internacionales, Bruce Swartz, del Departamento de Justicia de 19 de febrero de 2016 dirigidas ambas a Justin S. Antonipillai Consejero del Departamento de Comercio de los Estados Unidos, y a Ted Dean Subsecretario de Administración del Comercio Internacional.

[967] Ver páginas de este trabajo sobre la FISA.

privacidad para la protección de datos (con alusiones al principio de legalidad o a la dignidad y respeto de los derechos también de los no estadounidenses), hasta las estipulaciones de la FISA y de la USA Freedom Act[968], con la prohibición de la recopilación indiscriminada de documentos.

Se observa aquí más una declaración de voluntad para que el Derecho no se sobrepase a la vía de los hechos, en cuanto al espionaje masivo se refiere, que una salvaguardia jurídica de protección equivalente para los europeos de la propia de los ciudadanos americanos. Si bien el espíritu de cooperación del poder estadounidense es evidente y además se reserva la Comisión la facultad de revisión periódica del acuerdo (tal y como prevé el Reglamento) para comprobar la efectividad del mismo.

Y termina con ánimo conclusivo: "Por todo lo anterior, la Comisión concluye que en los Estados Unidos existen normas destinadas a garantizar que las posibles injerencias cometidas a efectos de seguridad nacional en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión a los Estados Unidos en el marco del Escudo de la privacidad UE-EE.UU. se limiten a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido" (punto 88).

Y da así la Comisión por cumplida con las estipulaciones de la sentencia Schrems: "en la evaluación de la Comisión, esto es conforme con la norma establecida por el Tribunal de Justicia en la sentencia Schrems, según la cual una legislación que implique una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe imponer unas «exigencias mínimas» y «no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización». Tampoco habrá una recopilación y almacenamiento de datos ilimitados de todas las personas sin ninguna limitación, ni acceso ilimitado" (punto 90).

[968] Aprobada en 2015, tras la marea irresistible de las revelaciones del verano de 2013.

En los recursos individuales se presta especial atención a los habilitados por la FISA y la FOIA para su posible ejercicio por los ciudadanos europeos a su amparo. Además de la novedad de la figura del Defensor del Pueblo que "garantiza la supervisión independiente y la reparación individual", que cuenta con el compromiso de colaboración garantizado por el Gobierno americano. Y con especial referencia a su independencia respecto a los servicios de inteligencia de los Estados Unidos (puntos 113, 114 y 118).[969]

Al igual que lo previsto para la seguridad nacional la Decisión contempla previsión para los accesos a efectos de aplicación de la ley y de otros fines de interés público, siendo aquí ya competente el Departamento de Justicia norteamericano. Referenciando en primer lugar la Cuarta Enmienda de la Constitución americana, que, si bien no se extiende a ciudadanos extranjeros, podrán éstos beneficiarse "de manera indirecta de su protección, dado que los datos personales obran en poder de empresas estadounidenses con el efecto de que las fuerzas y cuerpos de seguridad deben contar con autorización judicial o, al menos, respetar el requisito de razonabilidad". Ocurre igual con los requerimientos administrativos con fines de interés público. Y alude aquí también, en especial, a la legislación de la FOIA y de la ECPA, junto con la referencia a las *Wiretap Act*, a la *Computer Fraud and Abuse Act*, la *Right to Financial Privacy Act* y a la *Fair Credit Reporting Act*. Todas ellas de las que se puede beneficiar el ciudadano europeo en la protección de sus datos (puntos 125 a 135), y estudiadas en este trabajo.

[969] En el Anexo A se desarrolla la figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad, que en realidad parte de la previsión de la orden PPD-28 en su artículo 4 letra d) que exige que el Secretario de Estado designe un "Senior Coordinator for International Information Technology Diplomacy" (coordinador superior) para las dudas de gobiernos extranjeros respecto a las actividades de inteligencia. Este coordinador (coordinadora siendo a partir de enero de 2015 la Subsecretaria C. Novelli) será el que actúe como Defensor del Pueblo sobre Privacidad. El Anexo, que es, al fin y al cabo, un memorando de entendimiento, encauza el procedimiento a través de las autoridades de protección europeas sin que los particulares se puedan dirigir a esta figura directamente. Y serán a las autoridades a las que se le hayan presentado la solicitud a las que prestará respuesta de sus investigaciones. Si bien estas respuestas y labor parecen tener, ya en su previsión, un alcance limitado ya que según letra e) del punto 4 del Anexo: "...ofrecerá una respuesta al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE en cuestión, confirmando: i) que la reclamación ha sido debidamente investigada; y ii) la observancia de las leyes, estatutos, órdenes ejecutivas, directivas presidenciales y políticas de los organismos estadounidenses, siempre y cuando se hayan respetado las limitaciones y las protecciones descritas en la carta de la ODNI o, en caso de incumplimiento, cuando este incumplimiento haya sido subsanado. El Defensor del Pueblo en el ámbito del Escudo de la privacidad no confirmará ni negará si el individuo ha sido objeto de vigilancia ni tampoco confirmará la reparación concreta aplicada ..."

4.6 La posible suspensión.

La Comisión se reserva la posibilidad de suspender (total o parcialmente) el Acuerdo para el caso de que observe y compruebe, en general, incumplimientos de los principios en él estipulados. Previa notificación a la FTC para que actúe, y en caso de que no se tomen las medidas pertinentes por los órganos estadounidenses.

Se impone a la Comisión su actuación en unos casos determinados: "En particular, la Comisión incoará el procedimiento de suspensión o derogación en las siguientes circunstancias:

a) cuando haya indicios de que las autoridades estadounidenses no se atienen a las declaraciones y compromisos recogidos en los documentos adjuntos a la presente Decisión, en particular por lo que respecta a las condiciones y limitaciones del acceso por parte de los poderes públicos de los Estados Unidos a los datos personales transferidos en el marco del Escudo de la privacidad a efectos de aplicación de la ley, seguridad nacional y otros fines de interés público;

b) si no se atienden eficazmente las reclamaciones presentadas por los interesados de la UE; en este sentido, la Comisión tendrá en cuenta todas las circunstancias que influyan en la posibilidad de que los interesados de la UE hagan valer sus derechos, incluido, en particular, el compromiso voluntario contraído por las empresas estadounidenses autocertificadas de cooperar con las APD y acatar sus recomendaciones, o

c) en caso de que el Defensor del Pueblo en el ámbito del Escudo de la privacidad no responda de forma oportuna y adecuada a las peticiones de los interesados de la UE." O bien también cuando exista falta de colaboración por los órganos estadounidenses, incluido el Defensor del Pueblo de la Privacidad (puntos 151 y 152[970]

[970] Como nos dice el punto 152 en el caso de que "...no facilitasen la información o las aclaraciones precisas para evaluar el cumplimiento de los principios"

5. El Acuerdo sobre el flujo de datos en el ámbito del *Law Enforcement*: el *Umbrella Agreement.*[971]

Podemos decir que estamos ante el *alter ego* del *Privacy Shield*, si bien en materia de persecución de las infracciones penales, en base al Acuerdo con Estados Unidos sustanciado en la Decisión de mayo de 2016, y que se instrumentaliza jurídicamente como Tratado internacional el 2 de diciembre del mismo año. Al igual que en el *Privacy Shield* sobre la previsión del 25.6 de la Directiva 95/45/CE, el *Umbrella Agreement* se remite al artículo 37.1, letra a), de la Directiva (UE) 2016/680 que prevé, con las garantías apropiadas, las transferencias de datos por los Estados miembros.[972]

5.1 Objeto y Contenido.

El Acuerdo (que se compone de un Preámbulo y 29 artículos), regula estos flujos de datos a efectos de persecución criminal entre las dos potencias de las orillas del Atlántico, comprometidos a "garantizar un alto nivel de protección de los datos personales intercambiados en el contexto de la prevención, investigación, detección y

[971] Tratado Internacional aprobado por Decisión (UE) 2016/2220 del Consejo de 2 de diciembre de 2016 relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, sobre el Acuerdo con Estados Unidos adoptado en la Decisión (UE) 2016/920 del Consejo, de 20 de mayo de 2016, sobre la firma, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales.

[972] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión 2008/977/JAI.

Y apuntando la especialidad prevista en el Protocolo nº 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia así como en el Protocolo nº 22 sobre la posición de Dinamarca, ambos anejos al TUE y al TFUE. Lo que implica tal y como se contempla en el artículo 27 del Acuerdo que: "...sólo se aplicará a Dinamarca, el Reino Unido o Irlanda si la Comisión Europea notifica por escrito a los Estados Unidos que Dinamarca, el Reino Unido o Irlanda han decidido que se les aplique."

enjuiciamiento de infracciones penales, incluido el terrorismo". Estableciendo este acuerdo "el marco para la protección de los datos personales cuando se transfieren entre los Estados Unidos, por una parte, y la Unión Europea y sus Estados miembros, por otra." (Preámbulo y artículo 1.2). Y ello lo hace por un plazo indeterminado.

Las definiciones del artículo 2 son las propias de la normativa, circunscribiendo la autoridad a "los cuerpos y fuerzas de seguridad y los órganos jurisdiccionales nacionales" de Estados Unidos y de la Unión y de los Estados miembros responsables en la investigación de delitos. Y siendo su ámbito de aplicación los datos transferidos entre autoridades a estos efectos, es decir limitados a los "fines específicos autorizados por la base jurídica de la transferencia". Viniendo el Acuerdo a complementar, y no a sustituir, las respectivas legislaciones de protección de datos aplicables en cada territorio (artículos 3 a 6).

Sí requerirá consentimiento previo de la autoridad competente que envió inicialmente los datos en caso de transferencia ulterior a otra autoridad u organismo internacional no previsto en el Acuerdo. En caso de consentimiento podrá establecer esa autoridad originaria una serie de condiciones específicas para el mismo. Contemplándose asimismo los principios de calidad e integridad de los datos y el principio de seguridad de los mismos (incluyendo el de comunicación de una brecha en esa seguridad). Al igual que la obligación de llevanza de registros en este ámbito (artículos 7 a 11).

El principio de conservación de datos no más de lo estrictamente necesario, el principio de rendición de cuentas, al igual que la previsión de categorías especiales de datos, también se contemplan (artículos 12 a 14).

Igualmente no se podrán tomar decisiones adversas "significativas" sobre la base de "tratamiento automatizado de datos personales sin intervención humana" (perfiles) si bien ello se puede autorizar por el Derecho nacional. Debemos decir que teniendo en cuenta los sistemas de vigilancia automatizada de los Estados Unidos, aquí se está a la expensa total de las previsiones en este sentido por el Derecho estadounidense.[973]

[973] Tal y como advierte Garriga Domínguez (2014, 35) sobre los problemas y vicisitudes diarias que provocan riesgo en la protección de los datos personales, cuando nos señala que "existen auténticos programas rastreadores o espía utilizados por los Estados para la lucha antiterrorista o la delincuencia grave y que, en muchos casos no respetan las normas sobre derechos humanos."Citando como ejemplo el programa "Carnivore" del FBI o el programa "Ecgelon", de factura norteamericana.

Los derechos de acceso y de rectificación se contemplan específicamente y en artículos separados. Operando el marco jurídico aplicable en el Estado donde se ejerciten. El derecho de acceso tiene las restricciones propias ya analizadas en otros apartados de este trabajo (derechos y libertades de los demás, seguridad pública y nacional,..) presentando especial interés por la materia las restricciones para: " proteger información sensible a efectos policiales y judiciales; evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos u oficiales; evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales;" (artículos 16 y 17).

El Acuerdo presenta también la posibilidad de recursos tanto administrativos como judiciales, siguiendo los respectivos marcos y legislaciones nacionales aplicables. Además de un principio de transparencia informativo del objeto, finalidad y leyes aplicables al tratamiento de datos.

Se prevén autoridades de supervisión para lo estipulado, y la cooperación entre ellas, siendo en Europa las autoridades de protección de datos de la Unión y las de los Estados miembros. Estando en Estados Unidos la concreción más extendida y difusa ya que se realizará esa tarea: "...de forma acumulativa a través de más de una autoridad, entre las cuales, inspectores generales, responsables en materia de protección de la privacidad, departamentos de rendición de cuentas de la Administración, consejos de supervisión de la vida privada y de las libertades civiles, y otros organismos ejecutivos y legislativos pertinentes de control en relación con las libertades civiles y la protección de la privacidad" (artículo 21.3).

Los siguientes artículos (23 a 25) se van encargando de las relaciones de cooperación entre la Unión Europea y los Estados Unidos en la aplicación del Acuerdo, implicando revisiones conjuntas, notificaciones sobre modificaciones y aprobaciones de normas que puedan afectar, y consultas relacionadas en general. También se prevé que "las Partes podrá suspenderlo en su totalidad o en parte mediante notificación escrita a la otra Parte por vía diplomática" (artículo 26.1).

6. La Redress Act de 2015.

Consecuencia de todo lo relatado anteriormente, se produce, en octubre de 2015 su aprobación en la Cámara de Representantes para después sufrir la enmienda del Senado. Para ser definitivamente aprobada y firmada como ley por el presidente Obama el 24 de febrero de 2016.

La Ley es importante por la repercusión significativa que supone tras el revés judicial de la sentencia Schrems al Acuerdo de Puerto Seguro, como hemos visto, y la determinación en el Acuerdo de Escudo de Privacidad de la tutela judicial efectiva a los ciudadanos europeos (que hemos analizado anteriormente). De hecho su aprobación ha sido un requisito fundamental para la consecución del Acuerdo *Privacy Shield*.

Así se deviene necesaria la modificación legal estadounidense para dar cabida a lo que supone la principal novedad de esta Ley: la garantía de ciertos derechos a ciudadanos no estadounidenses, entre los que se incluyen el derecho a presentar demanda por violaciones de su Privacidad en aquellas transferencias de datos para fines comerciales a ciudadanos de países con los que esas relaciones estén permitidas, y no se impida materialmente con ello los intereses de la seguridad nacional de Estados Unidos.[974]

Junto a este importante derecho la *Redress Act* amplía a los ciudadanos no estadounidenses algunos de los derechos contemplados en la *Privacy Act* de 1974, destacándose el derecho de acceso y de rectificación sobre la información en materia penal que estén compartiendo con la agencias federales estadounidenses las autoridades del país del que sea nacional el ciudadano titular de los datos.[975]

[974] Letras B y C del punto 1 de la letra d) de la Ley. Aquí como nos ilustra Blasi Casagran (2017, 215) "la compensación judicial para los ciudadanos europeos sigue siendo limitada en cuanto a su alcance. La Ley de Recurso Judicial de los EE.UU solo permite compensar a los ciudadanos europeos cuando las vulneraciones de protección de datos se produce por la transferencia de datos desde una autoridad europea o compañía privada a una de las autoridades estadounidenses que cubre la ley con fines de prevención, investigación, detección o persecución de delitos. Sin embargo, todos aquellos datos obtenidos o recogidos por otros medios, o para autoridades fuera del alcance de la ley, quedan fuera del alcance de protección."

[975] Véase en este sentido la declaración de la Comisaria Jouravá celebrando la firma de la ley americana

7. Consideraciones.

Como estudio relevante sobre estos Acuerdos, y también bajo el patrocinio del Parlamento Europeo, aludiremos al trabajo de las autoras Monteleone & Puccio (2017), que ponen el énfasis en la asunción del derecho a la garantía judicial efectiva (*Redress*) para los ciudadanos europeos en el sistema jurídico estadounidense en relación con su privacidad, y a raíz de la sentencia Schrems, con la remisión a los derechos de la "Privacy Act" de 1974. Siendo ello un prerrequisito para la firma del Acuerdo por parte de las instituciones europeas. Nos ilustran también sobre el período transicional entre el fin de vigencia del régimen jurídico del Safe Harbour y la entrada en vigor del Privacy Shield, en el que el gran volumen de intercambio de datos por motivos comerciales se vendrá a regir en su adecuación, siguiendo la recomendación del G29, por normas corporativas vinculantes o por cláusulas contractuales generales de las que vimos podía aprobar la Comisión.[976]

Igualmente sobre los Acuerdos, y que nos sirve en la comparativa del *Law Enforcement* y en la comparación general de sistemas jurídicos, citaremos el estudio de la Dirección General de Políticas Internas de la Comisión para el Comité LIBE del Parlamento Europeo.[977]

El estudio se refiere a los elementos de protección penal en el ámbito de la ejecución legal que es el ámbito donde la UE y los EE.UU. están embarcados en el entendimiento, a través de los acuerdos suscritos entre ambos. Y ello debido a que la privacidad interior de los dos bloque regionales mundiales en otras materias (consumidores o protección de datos en general) no ofrecen una perspectiva de acuerdo más allá del fallido acuerdo TTIP, que ha caído en un destacado olvido en los últimos meses, pareciendo haber desaparecido de la agenda de las dos potencias políticas.

---

como un logro histórico para restablecer la confianza transatlántica en el flujo de datos (recuperado el 12 de septiembre de 2018): http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm

[976] En este sentido Grupo del Artículo 29 (2015) sobre la sentencia Schrems.

[977] A cargo de Boehm (2015): "A comparison between US and EU data protection legislation for law enforcement purposes".

Nos ilustra el estudio de Boehm (2015, 7), que la mayoría de estándares europeos de protección no se encuentran en la ley estadounidense. Sobre todo en lo referido a la compartición de datos, en este ámbito, sin que la aprobación de la "Freedom Act" estadounidense vaya a cambiar este panorama legal.[978]

El Puerto Seguro, siguiendo con Boehm (2015, 35-36), parecía contener en apariencia todos los principios y estándares de protección que podría exigir el derecho europeo, si bien una visión más pormenorizada dejaba entrever sus debilidades como instrumento de garantía para la protección de datos, ya que cualquier elemento de derecho estadounidense (Ley, Jurisprudencia, órdenes ejecutivas o requerimientos del Law *Enforcement*) podrían dejar sin efecto los mecanismos de autocertificación previstos en el Acuerdo. Prima así cualquier manifestación del derecho de Estados Unidos sobre el Acuerdo con la UE. Otro ejemplo significativo es que la regla general europea de que la transferencia de datos está prohibida a falta de consentimiento, era establecida al revés en el Acuerdo de Puerto Seguro. La opción del "opt out" estaba totalmente limitada en el Safe Harbour a prácticamente dos casos: uso para otros fines o traspaso a un tercero. Además los derechos ARCO, aún previstos, no están concretados en el Safe Harbour. Además de que las opciones de intervención de las autoridades independientes no se contemplan, llevando a una general alusión al proceso civil norteamericano o al mecanismo alternativo de resolución dentro de los mimbres limitados de la FTC.[979]

Destaca en la comparación, ya de manera concreta, que la más importante divergencia entre los dos sistemas se encuentra en la protección constitucional de los datos personales. Mientras son tratados en su protección como derechos fundamentales en la UE, en Estados Unidos no se aplica ese contexto ni hay esa protección equivalente.[980]

---

[978] Así, nos dice el autor: "*Whereas in EU law every transfer of data to other agencies interferes with fundamental rights and requires specific justification, data sharing in the US between law enforcement authorities and the intelligence community seems to be the rule rather than the exception*."
El estudio sigue en parte el trabajo elaborado igualmente para el Comité LIBE: "The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens" (Bignami, 2015).

[979] Anexo 1 y Anexo 2 punto 11 del Safe Harbour(para la parte de violación de la sección 5 de la FTC Act)

[980] Completando el studio con la ilustración de ese sistema de protección multinivel europeo, no asimilable en Estados Unidos: *"...The EU's understanding of these rights have been shaped since the 1970s by comprehensive case law of the ECtHR and was been further developed in recent years through important EU instruments such as the Directive 95/46/EC, the TFEU and the Charter of Fundamental Rights, as well as the EU courts' case law. The US, with its restrictions to the protection of the Fourth Amendment, through the Third Party Doctrine, and the exclusion of non-US persons from both the Fourth Amendment and the Privacy Act protection, follow a very different approach, which is contrary to the*

Otra distinción crucial para el estudio es la de los diferentes objetivos en la protección, tal y como ya hemos apuntado: una protección general de datos en Europa para los ciudadanos y una protección específica en función de cada materia y ley en Estados Unidos. No dando por sentado legalmente una capacidad de acción de protección como derecho individual automáticamente. (Boehm, 2015, 68)

También importante es la distinción sobre la protección de las personas en base a si son o no ciudadanos americanos. Sobre todo en todo lo relativo a la seguridad nacional, marcadamente diferenciado en la FISA y en la USA Patriot Act.[981]

Según el estudio parece que el *Umbrella Agreement* viene a obtener de los Estados Unidos unas garantías judiciales (como hemos apuntado anteriormente) para los ciudadanos europeos si bien no equiparada a la de los propios americanos en este ámbito.[982]

La garantía más llamativa, como hemos visto, es ese derecho al "redress", a la corrección y reparación judicial y administrativa, si bien no en pie de igualdad a la establecida para los ciudadanos estadounidenses en la *Privacy Act*. Excluyéndose además a las autoridades encargadas de la defensa nacional (que en base a lo visto son sobre la que recae el peso de la vigilancia masiva y que más pueden horadar los derechos fundamentales de los europeos sobre privacidad).[983]

Otro elemento a tener en cuenta es que las sucesivas transmisiones de datos, que requieren consentimiento a nivel europeo, no se tratan de manera clara en el Acuerdo, con la mera mención de "accountability" en el artículo 14 y que deja abierta dudas, ya que es algo muy habitual el tránsito interadministrativo de datos en Estados Unidos sin ulteriores garantías acompañantes (Boehm, 2015, 73).

EU's perspective of privacy and data protection as comprehensive fundamental rights." (Boehm, 2015, 67)

[981] "*A majority of the EU data protection standards cannot be found in US law. A comparison is therefore not possible. Rules limiting inter-agency data exchange, exchange with other third parties, complete independent oversight and effective judicial review possibilities for non-US persons simply do not exist at all or are at best very limited...*" . (Boehm, 2015, 69)

[982] (Boehm, 2015, 71): "*perhaps the most important point, concerns the concession for the US to provide judicial redress procedures for EU citizens within the US. However, the agreement is far from being able to guarantee equal judicial redress rights to EU and US citizens..."*

[983] Los tres supuestos de las letras a) a c) del art. 19 del Acuerdo

Por último, debemos apuntar que, a pesar de reconocer la mejora para los derechos de los ciudadanos europeos que han supuesto tanto el *Privacy Shield* como el *Umbrella Agreement* en sus tranferencias transatlánticas de datos, junto con Blasi Casagran (2017, 215), que ambos instrumentos "siguen permitiendo la recogida masiva de datos de ciudadanos europeos". Coincimos así en que ello "es especialmente decepcionante teniendo en cuenta que el TJUE concluyó que la vigilancia masiva por parte de los EE.UU vulneraba el derecho fundamental de protección de datos y privacidad de la UE".

CONCLUSIONES COMPARATIVAS

1. Nos encontramos ante unos de los derechos, el derecho a la privacidad, de regulación más necesaria y controvertida conforme al signo del tiempo actual en la sociedad que habitamos. Nuestras vidas se empiezan a medir en el siglo XXI, y de manera novedosa en la Historia, por los datos que volcamos en la red global de internet y, particularmente, en sus redes sociales. Nuestros datos son medidos, determinados y clasificados, como si de productos en mayor o menor fase de elaboración o perfilación se tratasen, para ir poniéndose a disposición del mercado globalizado a un ritmo vertiginoso. Ese elemento de disposición de los datos actual tiene además la singularidad, única en este ámbito mercantil, de que, en la gran mayoría de las ocasiones, se ofrecen por su titular de manera voluntaria; una dación de manera gratuita de aspectos de su personalidad, estados de ánimo, preferencias personales de todo tipo, que van desde las gastronómicas a las ideológicas, y, en general, posicionamientos vitales generales y particulares sobre todo ámbito.

2. Todo ello sería la vertiente de mercado de la situación que pretende regular el derecho a la protección de datos. En su otra vertiente, está la actuación que sobre esos datos se pueda realizar desde los poderes públicos. En general, se trata de una actuación necesaria para el funcionamiento del Estado y, sobre todo, para la prestación de los servicios públicos esenciales que éste tiene encomendado. Su regulación ha sido, por definición, respetuosa con esos datos, cuyo derecho, además, se veía obligado a proteger, en general, a través de autoridades de control. También esa regulación ha solido ser vanguardia que abría el camino jurídico para una mayor protección general (sirva de ejemplo en este sentido la *Privacy Act* americana o el Reglamento europeo de 2001 sobre esta protección en las instituciones europeas). Ahora bien, quizá, y sobre todo también atendiendo al sentido de los tiempos en este siglo XXI, su reverso tenebroso lo encontramos en las excepciones y limitaciones al derecho a la privacidad, originadas y motivadas por razones de seguridad. Observamos en ellas el gran agujero negro para la protección de datos, por la que se vendrá a justificar la vigilancia general

de la ciudadanía. Y ello, en el peor de los casos, no amparado legalmente, difuminado en una exigencia contra una permanente e inconcreta amenaza terrorista. Esta situación, se da en los dos sistemas jurídicos de protección referidos en este trabajo, si bien de manera más flagrante e inspiracional en el sistema americano.

3. Es además, el derecho a la protección de datos un derecho asociado al mayor índice de desarrollo de cada país, por esa misma vinculación del mismo a la capacidad de consumo, sobre todo traducida mediante el acceso a internet y a la capacidad de formar perfiles de consumidores por un lado, o al mayor y más eficiente poder estatal de los países de mayor nivel de desarrollo en los que se produce la actividad por otro; precisamente también por la sofisticación de los poderes de vigilancia de que disponen esos Estados más desarrollados. Es, por tanto, un derecho cuya protección comienza en los países y regiones del mundo con mayor nivel socioconómico, y se va extendiendo a las demás naciones de manera paulatina. Ello lo podemos comprobar en el grado de implicación e influencia de la OCDE en su protección, cuyas directrices empiezan a hacerse efectivas ya a partir de 1980. En este sentido la ONU, también se muestra consciente de la necesidad de esa implantación de la protección, a nivel mundial, y por ello ha empleado recursos en el estudio de su implementación progresiva en los países interesados. En este sentido el modelo de la Unión Europea, basado en la concepción de la privacidad como derecho fundamental, parece la óptica de futuro más deseable.

4. Así, llegamos a la distinción de la protección de datos como derecho fundamental y su falta de unanimidad jurídica global sobre esa percepción, sobre todo, por la falta de apuesta clara por parte de Estados Unidos en esa consideración clasificatoria como parte de los derechos humanos. Debemos aclarar que estamos ante un derecho, que por su propia naturaleza solo debe contemplarse en entornos democráticos (siendo su observación como derecho fundamental quimérica, y su vulneración estatal estandarizada ante las ventajas de la vigilancia totalitaria, en los países sin esa estructura de democracia liberal garantista).

Esa puede ser quizá la diferencia más significativa entre los sistemas americano y europeo de protección, si bien no es una diferenciación cristalina y sin matices, ya que

Estados Unidos tiene, como apuntabamos, elementos de constitucionalización importantes sobre este derecho, que, paradójicamente, se ve más difuso en ese carácter en las relaciones comerciales de los consumidores, que en las prerrogativas estatales de vigilancia (al menos sobre el papel legal y en cuanto a la consideración de derecho fundamental de esa protección.)

En Europa, y sobre todo tras la evolución del derecho en su positivación, su inclusión en el catálogo de protección como derecho fundamental se ha despejado totalmente, si bien ese camino también se vió influenciado inicialmente por posiciones timoratas al respecto, mercado mediante, y de consideraciones no tan claras sobre ese carácter fundamental. De ahí que hablemos, a la luz de lo estudiado, de una distinción no tan clara y meridiana entre los sistemas como en principio cabría suponer.

5. Debemos destacar igualmente la condición de derecho reactivo que caracteriza al derecho a la privacidad, y la manera en que este derecho va a la zaga, tanto en su origen como en su desarrollo de contenido, de las realidades que van surgiendo. Esta característica parece ser común en la mayoría de los derechos reconocidos, si bien en algunos, su conformación parte de impulsos políticos o situaciones sociales previsibles. En el derecho a la protección de datos esa faceta y sensación de perseguir a una realidad acuciante, y rápidamente contingente por parte de un derecho lento y vacilante, se nos muestra, quizá, sin parangón (con el permiso del derecho medioambiental). Y ello no solo en dependencia de una realidad tangible, sino que, en muchos momentos sin disponer siquiera del conocimiento certero de los hechos que puedan provocar una actuación jurídica en consonancia. Como ejemplo de ello debemos volver a las declaraciones de Edward Snowden, que no solo nos han mostrado una realidad desconocida para el gran público (y por ende para el legislador), sino que voltea buena parte de la principal legislación sobre privacidad en Europa, y en menor medida en Estados Unidos. Y ello, previa reacción jurisprudencial en los dos sistemas jurídicos (en Estados Unidos principalmente), y con incidencia directa en los acuerdos de relación entre los dos bloques sobre su protección (siendo la denuncia originadora de la sentencia Schrems motivada de manera directa por esas revelaciones), y los nuevos sistemas de entendimiento. Aparte de todas las reacciones políticas e institucionales surgidas a raíz de esa nueva ampliación de la información sobre el estado de la realidad.

6. En cuanto a las características de la privacidad americana y su protección, las mismas vienen a sustanciarse de manera desgajada por razón de la materia.

Por un lado, desde el propio campo jurídico de actuación. Ya que hay aproximaciones a la misma desde las principales disciplinas del derecho público y privado, sin que legalmente o jurisprudencialmente se haya consolidado una visión unívoca de uso estipulado para esa protección. Así, hay posibilidades de utilización del derecho civil y mercantil, o del propio del derecho público, principalmente a través del especial derecho de los consumidores para ejercitar este derecho (con la encomiable labor de la FTC en este campo).

Y ello se da y se nos ofrece, de origen, debido a una falta de determinación clara del concepto amplio de privacidad. Éste parece así abarcar partes del derecho al honor, del derecho general a la intimidad personal y al de la propia imagen (todos ellos ubicados en su ejercicio de protección en la opción más privatista de esta visión), y el grueso del que conocemos más concretamente como derecho a la protección de datos, que además se va diseminando por las normas federales estadounidenses en función de la materia. Y tampoco hay una determinación legal clara del modelo de protección que se puede poner en práctica de manera uniforme, ni siquiera dentro de la misma materia, que se atomiza en base a determinadas lineas de actuación jurídica. Ejemplo claro de ello es la subespecialidad de la privacidad del consumidor, ya lo sea como consumidor general (faceta en la que gozará de la protección más homogénea de la privacidad americana), ya lo sea como consumidor de productos financieros (abriéndosele al usuario todo un nuevo mundo regulatorio diferenciado).

7. Por otro lado no encontramos en Estados Unidos, de igual manera, una linea jurisprudencial clara a la hora del tratamiento e interpretación de este derecho y su protección, posiblemente partiendo también de ese pecado original del inabarcable término de privacidad.

Así, la aproximación constitucional del Tribunal Supremo oscila entre la alegación de la Primera y la Cuarta Enmienda a la Constitución y de su posibilidad o no de aplicación.

Los pronunciamientos suelen, además, atender principalmente a las circunstancias del caso, más que a una linea consecuente previa de interpretación dentro del mismo órgano judicial. Elemento de oscilación que se confirma acusadamente en los casos de enjuiciamientos donde entra en juego el factor seguridad y su ponderación con la privacidad.

8. En Europa encontramos, en cambio, un derecho reconocido y reconocible en la protección de datos. Un derecho fundamental cuyo carácter se antoja abanderado en el entorno digital global, tintado así de un tono azul oscuro estrellado en dorado, que ondea como seña de identidad, y referente en el foro internacional en cuanto a privacidad se refiere.

Compartimos que estamos con el Reglamento General europeo (heredero de su importante precedente en forma de Directiva) ante el instrumento jurídico de mayor protección del derecho a la privacidad a escala global. Y ello tanto por la homogeneidad de protección que presenta, como por la cantidad de ciudadanos beneficiarios a los que ampara, con ánimo de igualdad. Asimismo se presenta la regulación del derecho europeo como referente jurídico a escala mundial, no solo en cuanto a su recomendación desde las instituciones internacionales, con la ONU a la cabeza, sino como guía de uso en la que reflejarse para los distintos países que se proponen establecer una aprobación general legal en esta materia.

9. La alabanza que merece ese esfuerzo vanguardista europeo de protección, requiere igualmente una contrarréplica en algunos de sus componentes, que hacen flaquear la integridad de esa protección. Ese talón de Aquiles del conjunto regulatorio en Europa puede mostrarse en una tendencia a la heterogeneidad normativa en ámbitos especiales, como el de la privacidad en el clásico espacio de libertad seguridad y justicia, o la falta del mismo nivel de exigencia para el tratamiento de datos amparados por el escudo de privacidad; que, en la práctica, traslada buena parte de la tutela de derechos sobre nuestros datos migrantes, a una regulación americana, que, como hemos visto, no presenta unos niveles garantistas equivalentes al tratamiento “intramuros” europeo de

esos datos. Y ello, teniendo en cuenta que el flujo transatlántico de esos datos hace vulnerable la garantía de protección plasmada sobre el papel de las normas europeas.

10. Por tanto, el derecho a la privacidad estadounidense y el derecho a la protección de datos europeo, ya difieren desde su propia determinación terminológica.

Paul Bernal (2014) se fija en el problema relacional entre las perspectivas de la UE y de Estados Unidos, respecto a la necesidad de regulación o de mayor liberalidad en beneficio de las grandes tecnológicas (principalmente estadounidenses), sobre la base del reconocimiento de este nuevo derecho o de esta nueva modalidad de ejercicio del derecho de supresión y cancelación, que se ha llamado "derecho al olvido". El artículo es citado porque es paradigma del asunto trascendente del contenido del derecho a la privacidad y a la protección de datos en su protección por parte de las dos culturas jurídicas que se ocupan de su defensa y equilibrio, y que son el asunto principal de este trabajo. El derecho a ser olvidado, que viene a contemplarse en el Reglamento General de la UE pone ante el espejo las contradicciones (si bien también la sustancialidad de algunos elementos de unión) entre Europa y Estados Unidos en la protección de la privacidad del individuo, y su encaje en la sociedad en general, y en la tecnológica en particular.

No sabremos si llegar tan lejos como el autor en afirmar la falta de auténtico propósito de protección en EE.UU hacia los derechos económicos, sociales y culturales, en base a su tradición jurídico política; mientras que, sí que entendemos con él, de forma más nítida, su reconocimiento y el equilibrio entre derechos como una marca propiamente europea. Igualmente ello se traduce en la regulación, abordando Europa la protección de una manera más normativa, más legal mientras Estados Unidos prefiere una opción más cercana a la autorregulación, más de *laissez faire* (Bernal, 2014, 70-71).

De ello hemos venido dándonos cuenta a medida que nos ocupábamos del estudio y elaboración de este trabajo, que viene a reunir algunas conclusiones que comparten la característica de comparativa y de contorno de los principales elementos apreciativos en el régimen jurídico de los dos sistemas de protección de la privacidad y protección de datos en Estados Unidos y en Europa.

11. Una primera característica, ya apuntada en su consideración global, en la diferenciación de los sistemas americano y europeo es ese punto de partida diferenciado. La protección de datos es conceptuada como derecho fundamental en Europa, así está definida y asentada en el viejo continente, y no así en Estados Unidos donde esa conceptuación del derecho no se encuentra ni mucho menos despejada, como aludiamos. La asimilación liberal de las aproximaciones de protección estadounidense es una pauta jurídica, en sí de mayor fuerza, que el asentamiento del derecho como derecho fundamental; que solo se observa por alguna vía de equiparación jurisprudencial en encajes indirectos en algunas enmiendas constitucionales, o por cierta influencia del derecho internacional (incluido, y con la mayor fuerza precisamente, el proveniente de Europa).

12. Hemos visto, por tanto, que el recorrido jurídico del derecho a la protección de datos en la Unión Europea está estrechamente ligado al posicionamiento inicial del defensa de la protección de los derechos fundamentales como tarea asimilada en ese camino por el Derecho Europeo. Sin esa toma de actuación sobre los mismos, y sobre los que se basa en gran medida, la progresiva constitucionalización de la Unión, (primero pasando de valores a principios y de ellos a derechos, y luego cristalizando esos derechos en una Carta asimilada al derecho originario con fuerza ejecutiva), no podemos entender la magnitud de la protección de datos como ejemplo perfecto de ese camino. Todo ello hasta ser consolidado en su protección en forma de Reglamento General, y ya no solo por su carácter necesario para el mercado común, sino como elemento de garantía de libertad e igualdad del ciudadano europeo en el conjunto de su territorio. Lo que implica una protección más allá, cuando su ciudadanía virtual viaje con él, ya sea en persona o a través de las redes y comunicaciones electrónicas, también en su defensa mínima y estándar en servidores remotos de localizaciones distintas a las europeas (principalmente como hemos visto en Estados Unidos).

13. Para la consecución de ese recorrido en Europa debemos destacar también la labor configuradora de la jurisprudencia de la estrucutura multinivel europea, principalmente del TJUE, si bien también con la valiosa influencia del TEDH. Así el TJUE, casí desde

sus inicios, ha trabajado incansable en la consideración de la atención de los derechos fundamentales como parte integrante e inevitable de sus pronunciamientos, y ello coincide y se demuestra particularmente relevante, con el derecho a la protección de datos en sí mismo. Así, la sentencia Stauder, que abre esas consideraciones, según unánime doctrina, se puede considerar un primigenio asunto sobre la privacidad del señor alemán y su "vergonzante" cupo de reducción navideña para comprar mantequilla. Y todo para que, tras los avances de la técnica informática en los 70, recorrer el último tercio del siglo XX y las casi dos primeras décadas del XXI, en una evolución paralela del derecho europeo, pueda llegar la protección de datos a conformarse como parte sustancial de la ciudadanía europea. Derecho que parece estandarte visible de lo que pueden significar los derechos de los europeos, tras la labor constructora judicial del Tribunal de Luxemburgo (con inestimable aportación del TEDH) y su protección en igualdad, incluso orientado de manera similar a un ámbito global (y jurídicamente portable).

14. Estados Unidos, en comparativa y como apuntábamos, viene a caracterizarse por un régimen de protección difuso, heterogéneo y disperso en su recolección de protección. En aquel se puede encontrar esta regulación de privacidad en multiplicidad de normas, y no de manera sistemática, ya que, según su ámbito de regulación, parecen verse obligadas a contener un apartado diferenciado dedicado a la protección de la privacidad. Ello multiplica así sus alusiones, provocando una falta de homogeneidad protectora, con la consiguiente pérdida de seguridad jurídica y de garantía de normalización de un derecho variablemente exigible según la materia en la que entre en juego. En Europa, en cambio, la estructura jurídico normativa de protección es a la inversa más bien: dotada de una estructura que se ve reforzada en su integridad y coherencia con la aprobación del Reglamento General de Protección de Datos de 2016. Es decir, se dota de una Ley general sobre protección de datos (antes en forma de Directiva homogeneizadora), y solo en algunos ámbitos jurídicos que gozan de especialidad se produce una derivación de esa Ley General (principalmente relacionados con los asuntos de seguridad y persecución criminal). Si bien ahí sigue siendo coherente con la dotación constitucional europea de los Tratados, ya antes también definidos en Pilares.

15. Vemos, por tanto también, dos vertientes bien definidas a la hora de abarcar la regulación de la protección de datos en la que coinciden ambos sistemas. Una, la general, que se corresponde con la regulación del derecho en su ámbito cotidiano. Y la otra la especialidad motivada por razones de seguridad, que abarca el espectro de la persecución criminal, de las necesidades del orden público y de los requerimientos de los asuntos de inteligencia.

Esta distinción es clara en la regulación europea, y es una especialidad separada que no solo afecta al derecho de protección de datos, y que viene heredada del clásico espacio de libertad, seguridad y justicia, bastión último de la soberanía nacional; que los Estados miembros tienden a preservar (si bien ese celo también tiene una tendencia europeizadora, como podemos comprobar en la renovada necesidad de una defensa común o de la policía de fronteras, tan actual y necesaria a la vista de los acontecimientos sociales, económicos y políticos de los últimos años).

Esa pulsión de especialidad jurídica en Estados Unidos se revela no más clara, pero sí más acusada, con mayor peso, y con más incidencia en el derecho a la privacidad individual. Ello, que obedece a las razones de la obsesión por la seguridad de un país que, se siente especial y permanentemente tensionado por una amenaza de terrorismo (a veces muy real y otras muchas infundada), se ve reflejado en un derecho a la privacidad fuertemente condicionado por esa situación. En Estados Unidos el difícil equilibrio entre seguridad y privacidad, muestra una balanza jurídica descompensada en favor de la primera, que viene motivada, entendemos, por una decidida apuesta política, variante en intensidad pero indiscutida, marcada por esa obsesión relacionada con las posibles amenazas a la seguridad.

Ahora bien, debemos observar que el sistema de *check and balances* americano compensa esa predisposición a la seguridad, sobre todo en el ámbito judicial. Sistema, que se ve complementado por una pátina de liberalismo político, todavía extendido (aunque no reluciente) en el espíritu político y social del país, que hace que un derecho como el de privacidad, que parte de los derechos personalísimos asociados a la intimidad, (y así, a la defensa de la libertad individual, y de la dignidad de la persona), se vea especialmente abrazado de igual manera por la gran mayoría política (en ambos bandos) del país. Estos elementos, asociados a la sólida construcción jurídico-política de

la nación estadounidense, parecen, así, equilibrar el, ya de por sí, fragmentado y atribulado, derecho de la privacidad americano.

16. Se observa, asimismo, una tendencia de influencia recíproca entre las dos orillas del Atlántico, que parecen van dejando un poso jurídico de intercambio en las mareas, ya vengan del Levante o del Poniente del Océano. Así se observa una apuesta decidida por buena parte de la Doctrina estadounidense en asimilar la homogeneización normativa de la protección en una Ley única o al menos en una Autoridad de protección fuerte y con prestigio conformador de la protección, siguiendo los parámetros europeos. Por otro lado, no podemos obviar la gran influencia de la autorregulación, de inspiración norteamericana, en las regulaciones de protección de datos del derecho europeo, empezando por su gran presencia en el Reglamento General recientemente aprobado, que conforma una de sus principales novedades.

17. Así, la propia Unión Europea, en su rumbo hacia la defensa integral de la protección de datos, ha navegado en esa línea de mayor homogeneización que parece querer recorrer ahora EE.UU. en su protección de la privacidad, precisamente influenciado también por esa travesía europea culminada con éxito. Desde la necesaria armonización planteada y conseguida por la Directiva de 1995, se va andando el camino hacia la necesaria homogeneización que representa el Reglamento General. Y ello ya no solo por un interés de la unidad del mercado interior, que es un motivador común de la Directiva y del Reglamento, sino por la consideración debida a la protección de datos como derecho fundamental; que se entiende no puede ser tratado de manera divergente, aun dentro de los límites armonizados, en las diversas partes del territorio europeo.

Estados Unidos parece sentirse proclive, al menos institucionalmente, a esa homogeneización normativa, si bien, en la relaciones con la Unión va dejando también su sello de identificación. Sello principalmente estampado por las necesidades de sus grandes empresas, que, en este sentido, parecen los faros que más influyen en la aprobación normativa y perfilación del confuso modelo de protección americano.

18. Lo que se asimila claramente es la percepción común sobre la importancia del problema y de la necesidad de establecer una regulación de cooperación común de protección de la privacidad en general, y de los flujos internacionales de datos en particular, que dote de seguridad jurídica a las personas de los dos bloques concernidos en esta era tecnológica de la globalización. Los esfuerzos políticos para transformar esa defensa jurídica para los flujos de datos son claros, al menos, lo eran hasta finales del año 2016, momento en el que se ha puesto en tela de juicio por parte del nuevo presidente norteamericano la firma de los acuerdos de protección en este sentido, con ánimo de una supuesta mayor seguridad para su país. Al cierre de este trabajo la pluma amenazante del presidente Trump sobrevolaba sobre la intención de aprobación de una orden ejecutiva presidencial, que ponga las bases para la destrucción (de un plumazo redundante) de los tímidos avances que el presidente Obama consiguió para la privacidad en el año 2015, motivados tras las revelaciones de Snowden. Luego quizá este punto de unión también pudiera ser considerado, en un infausto futuro, otro punto de divergencia entre Estados Unidos y Europa, en su régimen de protección y en su interpretación jurídica sobre cómo abordar uno de los más importantes derechos individuales de nuestro tiempo: el derecho a la privacidad o el derecho a la protección de datos, según la orilla atlántica desde donde partan o hacia donde lleguen esos elementos vitales informativos de la personalidad de los ciudadanos estadounidenses y europeos.

19. Ahora bien, el sistema de protección de datos europeo, entendemos, no debe verse mermado en su fuerza garantista, por las exigencias de un mercado global de datos, cuyo beneficiario de más calado es el conjunto norteamericano de empresas (principalmente tecnológicas), en tanto esas exigencias se pretendan conseguir con la erosión del estándar europeo de protección de datos como derecho fundamental.

Podriamos realizar así un paralelismo, en lo concerniente al fallido acuerdo de Puerto Seguro, y al mejorado (aunque también contestado) Escudo de Privacidad, con las reticiencias que vinieron a suponer el planteamiento de los grandes acuerdos comerciales entre las dos orillas atlánticas: el Acuerdo transatlántico sobre Comercio e Inversión (TTIP), cuyas negociaciones se encuentran pausadas y en un perfil bajo, tras la considerable contestación que su posible firma provocó; y el Acuerdo Económico y

Comercial Global (AECG), más conocido por sus siglas en inglés CETA (*Comprehensive Economic and Trade Agreement*), cuya firma también ha recibido críticas, quizá menos justificadas, teniendo en cuenta los estándares del mercado canadiense, más cercano al europeo. Ejemplos claros de confrontación de los dos sistemas jurídicos y de la manera en que el público al que van dirigidos percibe su legitimidad, garantía de derechos y la defensa de los mismos.

20. De igual manera se nos sugiere, aún salvando las distancias de los casos y los bienes jurídicos a proteger en los mismos, la viculación comparativa en clave garantista de estos acuerdos sobre privacidad en su flujo transatlántico, con el caso tratado en la sentencia Soering. Sentencia del TEDH de 7 de julio de 1989, Soering contra Reino Unido en base al artículo 3 del CEDH, relativo a la prohibición de sometimiento a tortura y a penas o tratos inhumanos o degradantes.

La posibilidad de esas torturas y tratos humanos y degradantes como efecto extraterritorial de la extradición de un ciudadano alemán, condenado por asesinato en el estado de Virginia (EE.UU.), fue considerada por el TEDH como altamente probable y contraria, así, al CEDH. En este caso un razonamiento de seguridad y de ejecución penal no prevaleció ante la defensa de un derecho fundamental previsto en el Convenio, también para los enjuiciados y sentenciados penalmente. Ese elemento de garantía se produce también en cuanto a la posible vulneración del derecho a la privacidad de los ciudadanos europeos, si bien la niebla provocada por el miedo al terrorismo parece no dejar tan expedita esa visión de garantía jurídica para la evitación de la vigilancia masiva que vulnera el derecho a la protección de datos.

21. Estamos, por tanto, convencidos, tras el estudio realizado en este trabajo y a pesar de aspectos mejorables, que la protección de datos encuentra su acomodo de mayor protección en el territorio de la Unión Europea. Al fin y al cabo es un derecho fundamental reconocido como tal sin ambages, elemento de reconocimiento que no se comparte en otras partes del mundo, como Estados Unidos. Es, además, un derecho evolucionado en la Unión desde sus inicios hacia ese posicionamiento, salvando las distinciones normativas propias de las soberanías de los Estados miembros, para acabar

siendo un derecho general con garantía común europea. Ello, además, se ve certificado por sus propios motores de desarrollo, que incluyen la mejor tradición nacional, para, con el mercado interior común mediante y como magnífico cauce, verse tamizado y deslindado por la gran labor de los Tribunales, con especial incidencia del TJUE y del TEDH. Esa doble labor se ve también reconocida en los instrumentos de influencia, primero del Consejo de Europa y su protocolo 108, y luego en la constitucionalización efectiva del derecho en la CDFUE y en el Tratado de Lisboa.

Ese cenit de garantía puede también ser comprobado en la alta influencia que el modelo europeo de protección presenta en los estudios legislativos para la aprobación de nuevos sistemas de privacidad en el plano internacional.

22. Nos encontramos en tiempos convulsos, tiempos con falta de certezas. Tras la mayor crisis económica que ha experimentado el sistema económico en su conformación actual, atendemos, algo impasibles, a una deriva lenta pero continuada que conduce a nuevos viejos repliegues en Europa, y con mayor novedad, en Estados Unidos. Es la vuelta a un nacionalismo exacerbado, por definición excluyente, y potenciador del miedo, generalmente indefinido, y alimentado a su vez por él. En buena parte de los países europeos, surgen movimientos que van abrazando esa reacción contraliberal. Esas corrientes políticas culpan de los males sociales a la inmigración, a la Unión Europea o a la democracia misma que les permite ejercitar su derecho electoral pasivo y su libertad de expresión. En Budapest se realizan marchas nocturnas con antorchas mientras se lanzan consignas antieuropeas y en Roma, miembros del gobierno, llaman “carne humana” a migrantes que se encuentran a punto de ahogarse en el Mediterráneo. En los países nórdicos proliferan los partidos “auténticos” en su apelativo a un inventado ADN nacional, y en Polonia se nos presenta la identidad del país por sus actuales gobernantes, a través del catolicismo como única confesión verdadera compatible con la nación. Hasta en Francia se explota a Juana de Arco como orígen heroico de la visión lepenista del lugar que acuñó la Revolución y la Declaración de los derechos del hombre y del ciudadano. Incluso en Alemania, tras décadas de educación en valores contra la nazificación que enloqueció al país, provocó su división y arrastró a Europa y a medio mundo al mayor desastre originado por el ser humano, se

presenta una “alternativa” pirómana al sistema surgido, precisamente, de aquellas cenizas.

En Estados Unidos, tras el primer presidente negro de su Historia, el péndulo político parece perder su eje, y coloca al mando de la Casa Blanca, bajo el lema de *America first*, a una persona que se vanagloria en querer dinamitar los propios fundamentos de la democracia que le ha permitido auparse en el poder, y desdeña el orden y derecho internacional establecido, sin aparente conocimiento de sus consecuencias. Un presidente americano que se entrevista con el sucesor del totalitarismo coreano, mientras se empeña en anunciar un muro con su vecina democracia del sur, y critica y desplanta al primer ministro de su democracia vecina del norte. De igual manera desprecia los acuerdos comerciales mundiales, y anuncia aranceles y vuelta al proteccionismo, en su formato de nacionalismo exacerbado económico, para que ya sean el acero o la aceituna negra más competitivos no accedan con cierta igualdad al mercado estadounidense. Y ello obviando una de las lecciones básicas keynesianas de las razones de distorsión económica como causa del desastre de la II Guerra Mundial. Y mientras, marca una equidistancia incendiaria entre los agresores racistas sureños, que ondean esvásticas y banderas confederadas, y los manifestantes contrarios que defienden la igualdad racial en la ciudad de Charlottesville.

23. Todo lo anterior nos sirve de contexto, de pulsión de la sociedad global en la que, en Europa, se ha consolidado el derecho a la protección de datos como derecho fundamental. Y ello con una motivación clara: defender ese producto jurídico de la privacidad europea como paradigma claro de protección jurídica que este “artefacto político no identificado” que es la Unión Europea puede generar. Nos sirve, así, este derecho consolidado, con la evolución configuradora propia del derecho europeo, como prueba certera de lo que supone la propia U.E. en su objetivo y fin último. Cual es, a través del respeto de los derechos humanos y de las libertades fundamentales, fortalecer el funcionamiento democrático y conseguir una más estrecha unión de los ciudadanos, que pueden disponer con él de un estándar de protección de sus datos personales incomparable.

De igual manera esa influencia trasciende a Estados Unidos, que, se ve así influenciado en esa marea protectora proveniente de Europa, y rubrica el acuerdo implícito de esa

percepción con el Escudo de Privacidad y su aprobación normativa y modificación legal al efecto. Sin olvidar el papel relevante de Estados Unidos en la génesis del concepto mismo de privacidad plasmado por Warren & Brandeis, así como la importancia de la iniciativa individual de un ciudadano de aquel país, tan necesario como Snowden, en todo este proceso de culminación protectora de la privacidad.

24. Por ello, y para terminar, queremos reivindicar así el significado del derecho a la privacidad y a la protección de datos en este contexto global, como medida esperanzadora de la democracia global o postnacional (o al menos regional europea); que no podrá desplegar todos sus potenciales efectos, sin la asunción de su respeto por parte del sistema americano, que alberga las mayores empresas de manejo de esos datos y las más fuertes centrales públicas de vigilancia y seguridad. Tal y como hemos visto, es posible, con un trabajo gradual, influenciado por las mejores tradiciones nacionales y por los organismos internacionales, y perfilado por las instituciones europeas y su democracia, alumbrar un derecho culminado en un efecto general e igual para una ciudadanía de perfil transnacional. Y ello, en estos tiempos convulsos, extraños y necesitados de discursos y certezas reales.

BIBLIOGRAFÍA

AUTORES CITADOS

Albers, M. (2014). Realizing the Complexity of Data Protection. En Gutwirth S., Leenes R., De Hert P. (Eds.). Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. (pp. 213-235) Dordrecht: Springer.

Allen, A. L. (2001). Minor Distractions: Children, Privacy and E-Commerce. *Houston Law Review.* 38, 751-776.

— (1999). Coercing Privacy. *William & Mary Law School Law Review,* 40 723-757.

— (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa: Rowman & Littlefield

Alvárez Caro, M. (2016). El derecho a la supresión o al olvido. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.). Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 241-256). Madrid: Editorial Reus.

Álvarez Caro, M. y Recio Gayo, M. (2015). Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU. y la UE. *Papeles de Derecho Europeo e Integración Regional número 25.* Madrid: Instituto de Derecho Europeo e Integración Regional (IDEIR).

Amsterdam A.G. (1974). Perspectives on the Fourth Amendment. *Minnesota Law Review*. 58, 349-477.

Arenas Ramiro, M. (2015). Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades. En Rallo Lombarte, A. y García Mahamut, R. (Eds.) Hacia un nuevo derecho europeo de protección de datos (pp. 311-381). Valencia: Tirant lo Blanch.

— (2014). Hacia un futuro derecho al olvido de ámbito europeo. En Valero Torrijos (Ed.). La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica (pp. 325-380). Pamplona: Aranzadi.
— (2014). Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (Google vs. AEPD). *Teoría y Realidad Constitucional de la UNED*, 4, 537-558.
— (2008). La protección de datos personales en los países de la Unión Europea. *Revista Jurídica de Castilla y León.* 16, 113-168.

Arendt, H. (2009). *La Condición Humana*. Buenos Aires: Paidos.

Azpitarte Sánchez, M. (2005). Del derecho constitucional común europeo a la Constitución Europea. ¿Cambio de paradigma en la legitimidad de la Unión? *Teoría y Realidad Constitucional de la UNED*, 16, 343-373.

Azurmendi, A. (2015). Por un «derecho al olvido» para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia europeo del caso Google Spain y su recepción por la sentencia de la Audiencia Nacional española de 29 de diciembre de 2014. *Revista de Derecho Político de la UNED.* 92, 273-310.

Bagley A.W. (2001). Don't be evil: the Fourth Amendment in the age of Google, National Security, and Digital Papers and Effects. *Albany Law Journal of Science and Technology*. 21, 153-191.

Bailey D. (2004). *The Open Society Paradox: Why the 21st Century Calls for More Openness-Not Less*. Washington D.C.: Potomac Books Inc.

Balaguer Callejón (2007). La constitución europea tras el Consejo Europeo de Bruselas y el tratado de Lisboa. *Revista de derecho constitucional europeo*, 8, 11-42.

Ball, H. (2004). *The U.S.A. Patriot Act of 2001: Balancing Civil Liberties and National Security: A Reference Handbook.* Santa Barbara: Abc-Clio.

Bar Cendón, A. (2009). El Tratado de Lisboa y la reforma constitucional de la Unión Europea". *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol.* 60/61, 183-220

Banks, C.P. (2004). Protecting (or Destroying) Freedom through Law: The USA Patriot Act's Constitutional Implications. En Cohen D. B. & Wells J.W. (Eds.). American National Security and Civil Liberties in an Era of Terrorism. New York: Palgrave MacMillan.(pp. 29-70).

Bellanova, R. (2018). *Connecting the Dots? PNR and Air Passenger Surveillance in Europe*. (Artículo de blog jurídico). Recuperado de: https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centrebordercriminologies/blog/2018/05/connecting-dots

Bellia, P. (2004). Surveillance Law through Cyberlaw's Lens. *George Washington Law Review*. 72, 1375-1458.

Bernal, P. (2014). The EU, the US and Right to be Forgotten. En Gutwirth S., Leenes R., De Hert P. (Eds.). Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. (pp. 61-77) Dordrecht: Springer.

Bils, J. (2013). Fighting Unfair Credit Reports: A Proposal to Give Consumers More Power to Enforce the Fair Credit Reporting Act. *UCLA Law Review Discourse*. 61, 226-242.

Bindi, E. (2016) Test de proporcionalidad en el "age of balancing". *Revista de Derecho Político de la UNED*, 96, 291-330.

Blasi Casagran, C. (2017). Nuevo régimen jurídico para la transferencia de datos entre la UE y los Estados Unidos ¿Es compatible con la normativa europea de protección de datos? *Revista General de Derecho Europeo*, 42, 193-217.

— (2016). El Reglamento Europeo de EUROPOL: un nuevo marco jurídico para el

intercambio de datos policiales en la UE. *Revista General de Derecho Europeo*, 40, 202-221.

— (2015). Límites del derecho europeo de protección de datos en el control de fronteras de la UE. *Revista CIDOB d'Afers Internacionals*, 111, 127-151.

Bloustein, E. J. (1978). Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory. *Georgia Law Review,* 12(3), 429-454

— (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York Law Review,* 39, 962-1007.

Blume, P. (2010). Data protection and privacy - basic concepts in a changing world. *Scandinavian studies in law*, 56, 151-164.

Boehm, F. (2015). A comparison between US and EU data protection legislation for law enforcement purposes. Brussels: European Parliament.

Borrell, J., Carnero C. y López Garrido, D. (2003). *Construyendo la Constitución Europea. Crónica Política de la Convención*. Madrid: Real Instituto Elcano de Estudios Internacionales y Estratégicos.

Bosch, A. (2010). *Historia de Estados Unidos*. Barcelona: Crítica.

Brin, D. (1998). *The transparent society*. New York: Basic Books

Bru Cuadrada, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de los Estudios de Derecho y Ciencia Política de la UOC*. 5, 78-92.

Byford K.S. (1998). Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment. *Rutgers Computer & Technology Law Journal*, 24,1-74.

Campuzano Tomé, H. (2000). *Vida Privada y Datos personales: Su Protección Jurídica frente a la sociedad de la Información*. Madrid: Tecnos.

Canales Gil, A. (2007). El derecho fundamental a la protección de datos de carácter personal. *Revista Jurídica de Castilla y León*. 12, 13-56.

Carmona Contreras, A. (2016). El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales. *Revista Española de Derecho Constitucional*, 107, 13-40.

Cate, F.H. (2001). *Privacy in Perspective.* Washington D.C.: The AEI Press.

— (2000). Principles of Internet Privacy. *Connecticut Law Review,* 32, 877-896.

Cavoukian, A. (2013). Privacy by Design: Leadership, Methods, and Results. En Gutwirth S., Leenes R., De Hert P. & Poullet, Y. (Eds.). European Data Protection: Coming of Age (pp. 175 a 202). Dordrecht: Springer.

Chicharro Lázaro, A. (2017). El nuevo acuerdo entre la Unión Europea y Estados Unidos para la transferencia de datos personales compartidos en redes sociales. En Herrero Gutiérrez, F.J. y Mateos Martín, C. (Coords.). Del verbo al bit (pp. 1037-1066). La Laguna: Sociedad Latina de Comunicación Social.

Clarke, R. (1994). Dataveillance by Governments: The Technique of Computer Matching. *Information Technology & People* 7,2, 46-85

Cohen, J. E. (2000). Examined lives: Informational Privacy and the subject as object. *Stanford Law Review,* 52, 1373-1438.

Cole, D. & Fabbrini, F. (2016). Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders. *International Journal of Constitutional Law*, 4 (1), 220-237.

Copeland, R.A. (2004). War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America. *Texas Tech Law Review.* 35, 1-31.

Coudhry, S. (2014). Commentary to article 7: Right to respect for Private and Family life (Family Life Aspects). En Peers S., Harvey, T., Kenner, J. & Ward, A. (Eds.). The EU Charter of Fundamental Rights. A Commentary. Oxford and Portland: Hart Publishing.

De Miguel Asensio, P.A. (2017). Competencia y derecho aplicable en el Reglamento General sobre Protección de datos de la Unión Europea. *Revista Española de Derecho Internacional*, 69 (1), 75-108.

De Miguel Sánchez N. (2006), El derecho a la protección de datos personales en el tratado por el que se instituye una Constitución para Europa. *Revista de Administración Pública*, 169, 301-335.

De Vega Garcia, P. (2003). La eficacia frente a particulares de los Derechos Fundamentales (la problemática de la Drittwirkung der Grundrechte). *Revista de Pensamiento Constitucional*, 9, (9), 25-43.

Deighton, A. (2016). The EU-US Privacy Shield – is it strong enough?. *Privacy & Data Protection*, 16 (4), 8-10.

Delgado Valle, E. (2014). Derecho al recuerdo en Internet. En Valero Torrijos (Ed.), La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. (pp. 407-454) Pamplona: Aranzadi.

Diez Picazo, L.M. (2008). La naturaleza de la Unión Europea. *Indret: Revista para el Análisis del Derecho*, 4, 1-67.

Duaso Calés, R. (2016). Los Principios de protección de datos desde el diseño y protección de datos por defecto. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.) Reglamento General de Protección de Datos: Hacia un nuevo

modelo europeo de Privacidad (pp. 295-320). Madrid: Editorial Reus.

Duran Cardo, B. (2016). *La figura del responsable en el derecho a la protección de datos.* Madrid: Wolters Kuwer

Eden, J.M. (2005). When big brother privatizes: commercial surveillance, the privacy act of 1974, and the future of RFID. *Duke Law & Technology Review*, 4, 1-25

Fernández Conte, J. y León Burgos, D. (2016). Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.) Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 35-50). Madrid: Editorial Reus.

Focault, M. (1986). *Vigilar y castigar*. Madrid: Siglo XXI Editores.

Forsyth, B. (2015). Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection. *Washington & Lee Law Review*. 72, 1307-1341.

Galbraith, J.K. (1963). "Wealth and Poverty" Speech. National Policy Committee on Pockets of Poverty.

Galloway, H.H. (2002). Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror? *Washington & Lee Law Review*. 59, 921-974.

García Costa, F.M. (2014). La independencia de las autoridades nacionales de control de datos en la propuesta de Reglamento General de Protección de Datos. En Valero Torrijos, J. (Ed.), La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. (pp. 223-272) Pamplona: Aranzadi.

García San José, D. I. (2001). *Los derechos y libertades fundamentales en la sociedad europea del siglo XXI: análisis de la interpretación y aplicación por el Tribunal*

Europeo de derechos humanos de la cláusula "necesario en una sociedad democrática". Sevilla: Universidad de Sevilla, Secretariado de Publicaciones.

Garriga Domínguez, A. (2014). La protección de los datos personales en Internet: problemas actuales. En Sánchez Bravo, A.A. (Coord.). Derechos humanos y protección de datos personales en el Siglo XXI : homenaje a Cinta Castillo Jiménez (pp. 31-51). Sevilla: Punto Rojo Libros.

Gavison, R. (1980). Privacy and the limits of Law. *Yale Law Journal*. 89 (3), 421-471.

Gellman, R. (1999). Book Review, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive by Peter Swire & Robert Litan. *The George Washington Journal of International Law and Economics*, 32. (1), 179-201

— (1997). Does Privacy Law Work? En Agree P.E. & Rotenberg M. (Eds.) Technology and Privacy. The New Landscape. (pp. 193-218)

Goldman, E. (2006). A Coasean Analysis of Marketing. *Wisconsin Law Review,* 1151-1221.

— (2002). The Privacy Hoax. *Forbes Magazine*, 170, 42-43.

González Fuster, G. (2014).*The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht: Springer International.

— (2012). Equilibrio entre propiedad intelectual y protección de datos: el peso oscilante de un nuevo derecho. *Revista de los Estudios de Derecho y Ciencia Política de la UOC.* 14, 47-60.

Greenleaf, G. (2016). Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives. *Privacy Laws & Business International Report*,142, 14-17.

— (2012). The Influence of European Data Privacy Standards Outside Europe:

Implications for Globalisation of Convention 108. *International Data Privacy Law*, 2, (2), 68-92.

Gross, E. (2002). The Influence of Terrorist Attacks on Human Rights in the United States: The Aftermath of September 11, 2001. *North Carolina Journal of International Law & Commercial Regulation*. 28, 1-102.

Guerrero Picó, M.C. (2006). El impacto de Internet en el Derecho Fundamental a la Protección de datos de carácter personal. Madrid: Thomson Civitas.

— (2005). El Derecho Fundamental a la Protección de los Datos de carácter personal en la Constitución Europea. *Revista de Derecho Constitucional Europeo*, 4, 293-332.

Hamm R.F. (2010). *Olmstead v. United States:The Constitutional Challenges of Prohibition*. Washington D.C.: Enforcement Federal Judicial Center. Federal Judicial History Office.

Henderson, N.C. (2002).The patriot act's impact on the government's ability to conduct electronic surveillance of ongoing domestic communications. *Duke Law Journal*. 52, 179-209.

Hendricks, E. (2004). *Credit Scores and Credit Reports: How the System Really Works, What you can do*. Cabin John: Privacy Times.

Heredero Higueras, M. (1997). *La directiva comunitaria de protección de los 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 estos datos*. Pamplona: Aranzadi.

— (1983). La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de la Población de 1983. *Documentación Administrativa,*198, (139-158).

Hernández Corchete, J.A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.). Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 205-226). Madrid: Editorial Reus.

Hirsch, D.D. (2006). Protecting the Inner Environment: What Privacy Regulation can learn from environmental Law. *Georgia Law Review* 41, 1, 8-10

Hustinx P. (2015). Prólogo. En Rallo Lombarte A., García Mahamut R. (Eds.) *Hacia un nuevo derecho europeo de protección de datos* (pp.15-29) Valencia : Tirant lo Blanch.

— (2010). Privacy by design: delivering the promises. *Identity in the Information Society.* 3, 253–255.

Inness, J. C. (1996). *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.

Jaeger. P.T. (2003). The Impact of the USA Patriot Act on the Collection and Analysis of Personal Information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly.* 20, 295-314.

Janger E.J. & Schwartz, P.M. (2002).The Gramm-Leach-Bililey Act, Information Privacy, and the Limits of Default rules. *Minnesota Law Review*. 86, 1219-1262.

Jóri, A. (2013).The End of Independent Data Protection Supervision in Hungary – A Case Study. En Gutwirth S., Leenes R., De Hert P. & Poullet, Y. (Eds.). European Data Protection: Coming of Age. Dordrecht: Springer.

Juárez Pérez, P. (2012). El controvertido ‘derecho’ de residencia de los nacionales turcos en la Unión Europea: la STJUE de 15 noviembre 2011 (Asunto Dereci). *Cuadernos de Derecho Transnacional*. 4, (1), 256-276.1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review* 50, 1193-1294.

Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, 50, 1193-1294.

Karas, S. (2002). Privacy, Identity, databases. *American University Law Review*, 52, (2), 393 -445

Karras, A. (1999). The Constitutionality of the Driver's Privacy Protection Act: A Fork in the Information Access Road. *Federal Communications Law Journal*, 52, 125-153.

Kattan, I.R. (2011). Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud. V*anderbilt Journal of Entertainment and Technology Law.* 13, (3), 617-656.

Kaye, D (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. New York: U.N.Human Rights Council Recuperado de: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Kokott, J. & Sobotta C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3, (4), 222–228.

Kranenborg, H. (2014) Commentary to article 8: Protection of Personal Data. En Peers S., Harvey, T., Kenner, J. & Ward, A. (Eds.). The EU Charter of Fundamental Rights. A Commentary. Oxford and Portland: Hart Publishing.

Ku, R.S.R. (2002). Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance. *Minnesota Law Review*. 86, 1325-1378.

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review,* 25, 307-317.

Kuner, C., Cate, F. H., Millard, C. & Svantesson D.J.B (2011). Privacy: an elusive concept. *International Data Privacy Law*, 1(3), 141-142.

Lane, F. S. (2011). *American Privacy: The 400-Year History of Our Most Contested Right.* Boston: Beacon Press.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

López Aguilar, J.F. (2017). La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EUUU. *Teoría y Realidad Constitucional de la UNED,* 39, 557-581.

— (2015). Data protection package y Parlamento Europeo. En Rallo Lombarte, A. y García Mahamut, R. (Eds.) Hacia un nuevo derecho europeo de protección de datos (pp. 30 a 81). Valencia: Tirant lo Blanch.

López Calvo, J. (2017). *Comentarios al Reglamento Europeo de Protección de Datos.* Madrid: Editorial Jurídica Sepín.

Lorentz, D. (2011). The Effectiveness of Litigation Under the CAN-SPAM Act. *The Review of Litigation.* 30, 559-605.

Lucas Murillo de la Cueva, P. y Piñar Mañas, J. L. (2009). *El derecho a la autodeterminación informativa*. Madrid: Fundación Coloquio Jurídico Europeo.

— (1990). *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática*. Madrid: Tecnos,
— (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva Época),*104, 35-60.

Mcdonald, B. (2005). Privacy, Princesses and Paparazzi. *New York School Law Review*. 50, 205-236.

Macgeveran, W. (2013). The Law of Friction. *The University of Chicago Legal Forum*. 1, 15-68.

McInnis, T.N. (2010). *The Evolution of the Fourth Amendment*. Lanham: Lexington Books

MacKinnon, C. A. (1989). *Toward a Feminist Theory of the State*. Cambridge (Massachusetts): Harvard University Press

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. Revista de Internet, Derecho y Política de la UOC, 5, 47-61.

Martínez Pastor, E. (2014). La publicidad comportamental "on line" y la protección de los datos personales. En Valero Torrijos (Ed.). La protección de datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. (pp. 291-306). Pamplona: Aranzadi.

Miller, A. (1971). *The Assault on Privacy.* Ann Arbor: University of Michigan Press

Miralles, R. (2012). El Derecho de la portabilidad de datos. Blog de la página web de la Abogacía Española. Recuperado (15 de enero de 2017) de: http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales/

Monteleone, S. & Puccio, L. (2017). From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules. Brussels: (Members' Research Service) European Parliamentary Research Service.

Murphy, M.M. (2003) *Financial Privacy Laws Affecting Sharing of Customer Information Among Affiliated Institutions (CRS Report for Congress Congressional Research Service)*. Washington D.C.:The Library of Congress.

Murphy R.S. (1996). Property Rights in Personal Information: An Economic Defense of Privacy. *Georgetown Law Journal*. 84, 7, 2381-2417.

Nicol N.J. (1976). No Expectation of Privacy in Bank Records-United States v. Miller.

De Paul Law Review. 26, 146-157.

Ortega Giménez, A. (2017). Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield. *Revista Lex Mercatoria. Doctrina, Praxis, Jurisprudencia y Legislación,* 4, (12), 85-90

Orwell, G. (2014). *1984*. Barcelona: Editorial Lumen.

Pauner Chulvi, C. (2015). La libertad de información como límite al derecho a la protección de datos personales: la excepción periodística. *Teoría y Realidad Constitucional de la UNED.* 36, 377-395.

Pavón Pérez, J.A. (2002). La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. A*nuario de la Facultad de Derecho de la Universidad de Extremadura*, 19-20, 235-252.

Pérez Luño, A.E. (1991). El derecho a la autodeterminación informativa, II Jornada de Estudio sobre Protección de datos y Derechos fundamentales. En *Anuario de Jornadas, 1989-1990*. (pp. 304 y ss.). Oñate: Servicio de Estudios del IVAP.

Podesta, J. (2002). USA Patriot Act: The Good, the Bad, and the Sunset. *American Bar Association. Human Rights magazine.* 29 (1), 3-7.

Posner, R. A. (1978). The Right to Privacy. *Georgia Law Review,* 12 (3), 393-422.

Poullet, Y. (2000). “Les ""Safe Harbor Principles""Une protection adéquate?”. En Conférence IFCLA “Le droit de l'informatique au tournant du millénaire”, Paris.

Prislan, N. (2016). Carta de Europa ¿Existe una grieta digital entre EEUU y la UE? *Estudios de Política Exterior,* 172, 20-27.

Prosser, W. L. (1960). Privacy. *California Law Review,* 48, 383-423.

Puerto, M. I. y Sferrazza Taibi, P. (2018). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista Derecho del Estado*, 40, 209-236.

Puyol Montero, J. (2016). Los Principios del derecho a la protección de datos. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.). Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 135-150). Madrid: Editorial Reus.

Rallo Lombarte, A. (2017). El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet. *Teoría y Realidad Constitucional de la UNED*, 39, 583-610.

— (2016). El Delegado de Protección de Datos. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.) Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp.367-387). Madrid: Editorial Reus.

— (2015). El debate europeo sobre el derecho al olvido en internet. En Rallo Lombarte, A. y García Mahamut, R. (Eds.) Hacia un nuevo derecho europeo de protección de datos (pp.703 -737). Valencia: Tirant lo Blanch.

Rebollo Delgado, L. (2008). *Vida Privada y Protección de datos en la Unión Europea*. Madrid: Dykinson.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.

Reidenberg, J. (2001). The EU Data protection Directive: Implications for the U.S. Privacy Dabate. Hearing on Subcommittee on Commerce, Trade and Consumer Protection Committee on Energy and Commerce. Recuperado de: http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm

Richards, N.M. (2013). The dangers of Surveillance. *Harvard Law Review*. 126, 1934-1965.

Ripol Carulla, S. (2016). Aplicación Territorial del Reglamento. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.). Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 77-96). Madrid: Editorial Reus.

Rubel, A. (2007). Privacy and the USA Patriot Act: Rights, the value of rights, and autonomy. *Law and Philosophy.* 26, 119-159.

Ruiz Miguel, C. (2003). El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico. *Revista de Derecho Comunitario Europeo.* 14, 7-43.

Rysdall, R. (1992). Protección de Datos y el Convenio Europeo de los Derechos Humanos. Discurso de apertura de la XIII Conferencia de Comisarios de Protección de Datos en Novática. Citado en Campuzano Tomé, H. (2000). *Vida Privada y Datos personales: Su Protección Jurídica frente a la sociedad de la Información*. Madrid: Tecnos.(p.56)

Saldaña Diaz, M.N. (2012). The Right to Privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político de la UNED,* 85, 195-240.

Samuelson, P. (2000). Privacy As Intellectual Property? *Stanford Law Review.* 52, 1125-1173.

Sánchez Bravo, A.A. (2014). Nuevo marco europeo de protección de datos personales. En Sánchez Bravo, A.A. (Coord.). Derechos humanos y protección de datos personales en el Siglo XXI : homenaje a Cinta Castillo Jiménez (pp. 255-288). Sevilla: Punto Rojo Libros.

Sánchez Domingo, M.B. (2017). La protección de datos personales en el espacio de libertad, seguridad y justicia. Especial consideración a las transferencias de datos a terceros países y organizaciones internacionales según la Directiva 2016/680. *Revista de Estudios Europeos*, 69, 17-36.

Santolaya Machetti, P. (2005). Derecho a la vida privada y familiar: un contenido notablemente ampliado del derecho a la intimidad (art. 8 CEDH). En Santolaya Machetti, P. y García Roca, F.J. (Coords.). La Europa de los derechos: el Convenio Europeo de Derechos. (pp.487-508).
Madrid: Centro de Estudios Políticos y Constitucionales.

Santos Vara, J. (2012). La trasferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos. *Cuaderno Red de Cátedras Telefónica*, 7.

Schwartz, P.M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*. 117, 2055-2128.

— (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review,* 52, 1609-1701.

Serrano Pérez, M. (2005). El derecho fundamental a la protección de datos. Su contenido esencial. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, 1, 245-265.

Siegel R. B.(1996). ”The Rule of Love”: Wife Beating as Prerogative and Privacy. *Yale Law Review,* 105, 2117-2207.

Simitis, S. (1987). Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review,* 135, 707-746.

Simón Castellano, P. (2012). El derecho al olvido en el universo 2.0. *BiD: textos universitaris de biblioteconomia i documentació,* 28. Recuperado de:
http://bid.ub.edu/28/simon2.htm

Smith R.E. (2004). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence: Privacy Journal

Solove, D.J. (2007). The First Amendment as Criminal Procedure. *New York University Law Review*. 82, 112-176.

— (2006). *Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
— (2003). Identity Theft, Privacy, and the Architecture of Vulnerability. *Hastings Law Journal*, 54, 1227-1276.
— (2002). Conceptualizing Privacy. *California Law Review,* 90, 1087-1155.
— (2002). Digital Dossiers and the dissipation of Fourth Amendment Privacy. *Southern California Law Review*. 75,1084-1167.
— (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review.* 53, 1393-1462.

Solove D.J. & Hartzog W. (2014). The FTC and the new Common Law of Privacy. *Columbia Law Review,* 114, 583-676.

Solove, D. J. & Schwartz, P. M. (2015). *Information and Privacy Law*. New York: Wolters Kluwer.

Solozábal Echevarría, J.J. (2003). Constitución y orden constitucional en la Unión Europea. *Revista Jurídica Universidad Autónoma de Madrid.* 8, 361-384.

Sorkin, D. E. (2001).Technical and Legal Approaches to Unsolicited Electronic Mail. *University of San Francisco Law Review*. 35, 325-384.

Sovern, J. (1999). Opting in, opting out, or no options at all: The fight for control of personal information. *Washington Law Review,* 74, 1033- 1118.

Staten, M.E. & Cate, F.H. (2003). The impact of opt-in privacy rules on retail credit markets: a case study of NBNA. *Duke Law Journal*, 52, 745- 786.

Stuart Mill, J. (1997). *Sobre la libertad*. Madrid Alianza Editorial.

Suarez, S. (2017). Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should be Doing. *Law School Student Scholarship*. 882.

Sullivan, K. (2003). Under a Watchful Eye: Incursions on Personal Privacy. En Leone R.C. & Anrig, R. (Eds.). The War on Our Freedoms. New York: Public Affairs Books. (pp. 128-146)

Swire, P. (2015). *The USA Freedom Act: A Partial Response to European Concerns about NSA Surveillance.* Atlanta: Sam Nunn School of International Affairs. Georgia Institute of Technology.

Swire, P. & Litan, R. (1998). *None of your business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, D.C.: Brookings Institution Press.

Szoka, B. & Thierer, A. (2009). COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech. *The Progress and Freedom Foundation. Progress on Point.* 16,11, 1-23.

Tejerina Rodríguez, T. (2016). Interrelación con la Directiva sobre protección de datos por autoridades competentes. En Piñar Mañas J.L. (Dir.) y María Alvárez Caro, M. y Recio Gayo, M. (Coords.) Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad (pp. 97-113). Madrid: Editorial Reus.

Téllez Aguilera, A. (2002). La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores. Madrid: Edisofer.

Tountas, S.W. (2003). Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime? *Washington University Journal of Law & Policy*. 11.

Troncoso Reigada, A (2016). Autoridades de Control Independientes. En Piñar Mañas J.L.(Dir), Alvárez Caro, M. y Recio Gayo, M. (Coords.). *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de Privacidad*. (pp. 461-512) Ed. Reus: Madrid.

Van der Hof, S. (2014). No Child's Play: Online Data Protection for Children. En Simone Van der Hof, S.,Van den Berg, B. & Schermer, B. (Eds.). Minding Minors Wandering the Web: Regulating Online Child Safety (pp. 127 -141).The Hague: Springer.

Varoufakis, Y. (2012). *El Minotauro Global. Madrid:* Capitan Swing.

Vasak, K. (1977). Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights. *UNESCO Courier,* 30 (11), 29-32.

Volokh, E. (2014). Tort Law vs. Privacy. *Columbia Law Review,* 114, 879-948.

Wagner, A.R. & Finkelman, P. (2015). Security, Privacy, and Technology Development: The Impact on National Security. *Texas A&M University Law Review*. 2, 597-633

Warner, R.M. (1978) The Anatomy of a Speech: Lyndon Johnson's Great Society Address. *Michigan Historical Collections Bulletin,* 28, 1-15
http://bentley.umich.edu/exhibits/lbj1964/lbjspeech.pdf

Warren, S. D. & Brandeis L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5), 193-220.

Weiss M.A. & Archick, K. (2016) U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Washington D.C.: Congressional Research Service.

Westin, A. (2015). *Privacy and Freedom*. New York: Ig Publishing.

Whitehead, J.W. & Aden, S. H. (2002). “Forfeiting Enduring Freedom” for “Homeland Security”: A Constitutional Analysis of the USA Patriot Act and the Justice Department’s Anti-Terrorism Initiatives”. *The American University Law Review*. 51, 1081-1133.

Wolf, C. (2014). Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfer. *Washington University Journal Law & Policy.* 43, 227-257.

Wright, S. J. (2013). No Leg to Stand On: Clapper v. Amnesty International USA and the Dawn of an Increasingly Strict Standing Doctrine. *Ohio State Law Journal Furthermore.* 74, 41-46.

INFORMES Y DOCUMENTOS TÉCNICOS

Agencia de los Derechos Fundamentales de la Unión Europea / Consejo de Europa (2014). *Manual de legislación europea en materia de la protección de datos*. Luxemburgo: Oficina de Publicaciones de la Unión Europea.

— (2016). Opinion on the EU-U.S. Privacy Shield draft adequacy decision. Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

— (2016). Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2016/wp237_en.pdf

— (2015). Statement on the consequences of the Schrems judgment. Recuperada de : http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems judgement_en.pdf

— (2014). Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents. Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf
— (2012). Opinion 04/2012 on Cookie Consent Exemption Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
— (2011). Opinion 15/2011 on the definition of consent. Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
— (2011). Advice paper on special categories of data ("sensitive data") Recuperada de: http://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf
— (2010). Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento». Recuperado de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf
— (2007). Opinion 4/2007 on the concept of personal data. Recuperada de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
— (2005). Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. Recuperado de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf
— (2003). Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Recuperado de: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

AEPD (2009). The 31st Conference in Madrid adopted International Standards on the Protection of Data and Privacy (the Madrid Declaration). Madrid: AEPD.

Comisión Europea (2013). Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. Recuperada de: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290847_/com_com%282013%290847_es.pdf

— (2004) Comunicación de la comisión al Parlamento europeo y al Consejo sobre el funcionamiento del uerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52013DC0847

Comité Económico y Social Europeo (2012). Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Recuperado de: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52012AE1303

Comité de las Regiones (2012). Dictamen sobre el Paquete sobre la protección de datos Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012AR0625

Electronic Privacy Information Center (EPIC) and Privacy International (2006). *Privacy and Human Rights. An International Survey of Privacy Laws and Developments.* Washington/London: EPIC.

European Data Protection Supervisor (2016). Opinion on the EU-U.S. Privacy Shield draft adequacy decision. Recuperada de: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf

— (2015). Resumen ejecutivo del Dictamen del Supervisor Europeo de Protección

de Datos sobre «Hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios, la protección de datos desde el diseño y la rendición de cuentas». Recuperado de:https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52016XX0220%2801%29

— (2012) Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package. Recuperado de: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.192.01.0007.01.ENG&toc=OJ:C:2012:192:TOC

— (2011) Public access to documents containing personal data after the Bavarian Lager ruling. Recuperado de: https://edps.europa.eu/sites/edp/files/publication/11-03-24_bavarian_lager_en.pdf

European Digital Rights EDRI. (2013). Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels: EDRI. Recuperado de: https://edri.org/files/1012EDRi_full_position.pdf

Joint Committee on Government Operations, (1976). Legislative History of the Privacy Act of 1974 (Public Law 93-579) Washington: U.S. Government Print Office.

Federal Deposit Insurance Corporation (2016). Compliance Examination Manual. Recuperado de: https://www.fdic.gov/regulations/compliance/manual/

FTC (2013) Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003. Washington D.C.: FTC. Recuperado de: http://www.ftc.gov/reports/section-319-fair-accurate-credit-transactions-act-2003-fifth-interim-federal-trade

— (2013) Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework. Recuperado de: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-

enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf

— (2012). Privacy Framework and Implementation Recommendations en Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers. Washington D.C.: FTC

— (2010) Protecting Consumer Privacy in an Era of Rapid Change. A Proposed Recommendations for Businesses and Policymakers. A preliminary FTC Staff Report. Washington D.C.: FTC

— (2008).Definitions and Implementation Under the CAN–SPAM Act; Final Rule. Recuperado de: https://www.ftc.gov/policy/federal-register-notices/definitions-and-implementation-under-can-spam-act-16-cfr-part-316

— (2007). Implementing the Children's Online Privacy Protection Act. A Report to Congress. Washington D.C.: FTC

National Commission on Terrorist Attacks (2004). The 9/11 Commission Report. ("Final Report of the National Commission on Terrorist Attacks Upon the United States"). Recuperado de: https://www.9-11commission.gov/report/

OECD (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Recuperada de: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

United States General Accounting Office (GAO) (2002). Financial Privacy: Status of State Actions on Gramm Leach Bliley Act's Privacy Provisions. Recuperado de: https://www.gao.gov/products/GAO-02-361

U.S. Senate Select Committee on Intelligence (1976). Committe to Study Governmental Operations with Respect to Intelligence Activities, 1975-76 (Church Committee). Final Report. (S. Rep. No. 94-755).Washington D.C.: U.S. Senate

U.S.Privacy Protection Study Commission. (1977). Personal Privacy in an Information Society. The Report of The Privacy Protection Study Commission. Washington: U.S. Government Print Office

White House (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. *Journal of Privacy and Confidentiality*, 4, (2), 95-142.

ARTÍCULOS DE PERIÓDICOS

Delcker, J. (18 de abril de 2016). The way of the German privacy warrior. *Politico*. Recuperado de: http://www.politico.eu/article/the-way-of-the-german-privacy-warrior-sabine-leutheusser-schnarrenberger-germany-former-justice-minister-data-retention-law/

El Mundo (24 de septiembre de 2014). Edward Snowden gana el 'Premio Nobel Alternativo' en Suecia. *El Mundo.* Recuperado de*:* http://www.elmundo.es/internacional/2014/09/24/5422ed5c22601d7d478b458c.html

Meister, A. (2 de septiembre de 2016).Secret Report: German Federal Intelligence Service BND Violates Laws And Constitution By The Dozen. *Netzpolitik.org.*Recuperado de: https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/

Peirano, M. (13 y 14 de marzo de 2016). Entrevista a Edward Snowden (Primera y Segunda Parte). *eldiario.es.* Recuperado de: http://www.eldiario.es/internacional/entrevista_Edward_Snowden_0_494150889.html http://www.eldiario.es/internacional/teleco-usando-conectada-cordel-privacidad_0_494500669.html

The Guardian (29 de enero de 2014). Edward Snowden nominated for Nobel peace prize. *The Guardian.* Recuperado de:

https://www.theguardian.com/world/2014/jan/29/edward-snowden-nominated-nobel-peace-prize

Risen, J & Lichtblau. E. (16 de diciembre de 2005). Bush Lets U.S. Spy on Callers Without Courts. *New York Times*. Recuperado de: https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

El informe y la noticia sobre el mismo puede ser objeto de consulta en el Washington Post a través del siguiente enlace: http://apps.washingtonpost.com/g/page/world/pclobs-report-on-the-nsas-collection-of-americans-phone-records/757/
(No disponible por el nuevo RGPD)

PELÍCULAS

Poitras, L., Mathilde Bonnefoy, M., Wilutzky, D., Praxis Films, Participant Media y HBO Films (Productores) y Poitras, L. (Directora).(2014) *Citizenfour.* Estados Unidos. Praxis Films, Participant Media y HBO Films.

Borman, M., Kopeloff, E., Schulz-Deyle, P. Sulichin, F. (Productores) y Stone, O. (Director) (2016). *Snowden.* Estados Unidos. Endgame Entertainment, KrautPack Entertainment, Onda Entertainment, SachaVendian Entertainment.