Foro, Nueva época, vol. 22, núm. 1 (2019): 17-57 ISSN: 1698-5583
https://dx.doi.org/10.5209/foro.66632

ENSAYO GANADOR DEL X PREMIO ENRIQUE RUANO CASANOVA

VIGILANCIA MASIVA Y EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

Concepción Delgado Franco
Estudiante del Grado en Derecho
Universidad de Valladolid
teresa-concha@hotmail.com

RESUMEN

El objetivo de este trabajo de investigación es mostrar cómo la vigilancia masiva evidenciada por Edward Snowden tiene un impacto irreversible sobre los derechos fundamentales de los ciudadanos, viola el derecho a la privacidad, el derecho a la no discriminación, el derecho a la libertad de expresión y el derecho a la protección de datos. Numerosos organismos comunitarios e internacionales han expresado su preocupación y desacuerdo con el modelo que plantean los líderes mundiales de escoger entre libertad o seguridad. La vigilancia puede admitirse, pero solo cuando cumpla los estándares internacionales de derechos humanos que impiden el menoscabo de los derechos fundamentales que nos corresponden.

Palabras clave: intimidad, privacidad, era digital, *big data,* datos personales.

ABSTRACT

The purpose of this piece of work is to show how the massive surveillance shown by Edward Snowden has a non reversible impact on basic rights of citizens, how it violates the principle of privacy, the right to non discrimination, the right to freedom of expression as well as the right to data protection. A number of EU and international bodies have shown their concern and disagreement on the pattern presented by international leaders to choose between freedom or safety. Surveillance is ok, but only in compliance with international standards of those human rights which prevent our basic rights from lessening.

Keywords: privacy, intimacy, digital era, big data, personal data.

ZUSAMMENFASSUNG

Das Ziel dieser Forschungsarbeit ist aufzuzeigen, wie die massive Überwachung , wie sie von Edward Snowden augenscheinlich gemacht wurde, einen irreversiblen Einfluss auf die Grundrechte der Bürger, das Recht auf Privatssphäre, die Nicht-

Diskriminierung und das Recht auf freie Meinungsäußerung nimmt sowie das Recht auf Datenschutz verletzt. Zahlreiche Organe der Gemeinschaft —nationale und internationale— haben Ihrer Befürchtung und Ihrer Missbilligung gegenüber dem Modell Ausdruck verliehen, das die weltweit führenden Politiker der Nationen zur Wahl stellen: Freiheit oder Sicherheit. Überwachung kann zugestanden werden, jedoch nur, wenn gleichzeitig internationale Standards der Menschenrechte eingehalten werden, die verhindern, dass die fundamentalen Menschenrechte, die uns zustehen, eingeschränkt werden.

Schlüsselwörter: persönlichkeitsschutz, privatsphäre, digitales zeitalter, big data, personengebundene daten.

> «Cada frontera que cruzas, cada compra que haces, cada número que marcas, cada antena de telefonía que pasas, cada amigo que tienes, artículo que escribes, web que visitas, título que tecleas y paquete que envías, están en manos de un sistema cuyo alcance es ilimitado pero cuya seguridad no lo está».
>
> Edward SNOWDEN

I. INTRODUCCIÓN

Las revelaciones filtradas por el exanalista de la agencia de seguridad estadounidense Edward Snowden en junio de 2013 a través de *The Guardian* han demostrado la escala mundial de vigilancia de los Gobiernos estadounidense y británico.

La historia demuestra que la información es poder, pero nunca ha alcanzado un sentido tan amplio como en la sociedad actual, en la que ni siquiera el Gran Hermano de George Orwell hubiera podido imaginar un mundo en el cual la Nacional Security Agency estadounidense y su equivalente británico (el GHCQ) son capaces de investigar la vida de cualquier individuo.

En el momento actual es habitual plantear un falso dilema entre seguridad o privacidad, y es la privacidad la que pierde importancia en favor de leyes cada vez más agresivas en nombre de la seguridad. En particular, merece la pena resaltar que nos referimos a estas cuestiones desde la perspectiva de cuánta privacidad está dispuesta a sacrificar la sociedad civil para garantizar la seguridad. Sin embargo, la solución pasa por comprender que la seguridad y la privacidad no deben contraponerse, sino que son conceptos íntimamente vinculados.

El aumento del terrorismo ha dado lugar a leyes más invasivas y peligrosas en las que se permite el acceso a todas las comunicaciones con el pretexto de la seguridad y de evitar nuevos ataques, pero esto se opone a la presunción de inocencia de todo ciudadano, ya que las agencias de seguridad se dedican a buscar pruebas aleatoriamente sin tener indicios de que se esté cometiendo un delito.

No se trata de criminalizar cualquier vigilancia llevada a cabo por los Gobiernos, es decir, puede estar legitimada en ciertas ocasiones, pero siempre cumpliendo con unos requisitos. Dado que la vigilancia supone una injerencia en el derecho a la privacidad y a la libertad de expresión, solo podrá llevarse a cabo cuando cumpla unos criterios estrictos: debe ser selectiva, estar basada en sospechas razonables, llevarse a cabo conforme a la ley, cuando sea estrictamente necesaria para alcanzar un objetivo legítimo, realizada de forma proporcionada a tal objetivo y no discriminatoria.

Ocurre que la vigilancia masiva se ha dado de forma indiscriminada e injustificada. Estando en un Estado de Derecho las leyes deben proteger la seguridad y la privacidad, pero la intimidad es un derecho fundamental que no puede ser cedido bajo ningún pretexto. La protección de la intimidad en el ámbito de las tecnologías y de Internet se plasma, a través del derecho fundamental a la protección de datos personales.

Internet ha supuesto la opción de recopilar todo el conocimiento humano y ponerlo al servicio del público de forma libre y gratuita. Sin embargo, observamos que progresivamente la actividad privada ha ido restringiendo el acceso a este conocimiento y no solo eso, sino que existe la posibilidad de interferir en el comportamiento de los individuos con fines comerciales o financieros; ello se demuestra al observar una tendencia al registro masivo de datos concernientes a la vida privada de las personas. La vigilancia masiva afecta a los derechos humanos, pero no solo desde la perspectiva del derecho a la intimidad y a la protección de datos. Debe tenerse en cuenta que desde el momento en que una persona es consciente de la

posibilidad de estar sometida a vigilancia, cambia su modo de expresarse y comportarse en la red. Por tanto, nos encontramos con un claro ataque a la libertad de expresión, La supresión de la espontaneidad es el resultado directo de desproteger la intimidad, como lo entiende R. S. Gerstein en *Intimacy and privacy*. Al respecto de la espontaneidad se manifiesta en la misma línea Wasserstrom, que expresa que la misma desaparece cuando se tiene la certeza de ser observado por otros.

II. ERA DIGITAL Y DERECHO

1. Evolución de las telecomunicaciones

La comunicación es tan antigua como el ser humano, es inherente a las personas por su naturaleza social, la cual les impulsa a relacionarse con el entorno. En este sentido, la telecomunicación o comunicación a distancia ha estado presente desde la Antigüedad. Entonces se limitaba al correo postal, pero a medida que la sociedad se desarrolla surgen nuevos medios como el telégrafo, el teléfono, la radio, la televisión e Internet. Concretamente es en el siglo XIX cuando, por primera vez, se emplea la corriente eléctrica para transmitir mensajes. Luego llega la difusión mediante ondas electromagnéticas.

La culminación de las telecomunicaciones ha llegado con los ordenadores; herramienta que condiciona nuestra vida cotidiana y que se ha consolidado como un instrumento imprescindible en el siglo XXI. Por ello es necesario hacer un breve recorrido por la historia de los ordenadores debido a su vinculación con la evolución de las telecomunicaciones.

El inicio se remonta a 1940 y desde entonces hasta el presente se diferencian cinco generaciones de ordenadores. Esta clasificación parte de la tecnología empleada para la fabricación y el tipo de información procesada. No merece la pena entrar en detalles técnicos sobre la evolución del *hardware* por la amplitud de la materia. Basta con señalar que la primera computadora digital de la historia fue la ENIAC (Electronic Numerical Integratos and Computer), construida en 1947 por la Universidad de Pensilvania. Algunos autores consideran que la primera computadora fue creada en 1951, la UNIVAC 1, que fue adquirida por Estados Unidos y empleada para fines militares. La quinta generación comenzó en 1990 y se prolonga hasta ahora, y es aquí donde aparecen los primeros *laptops*. Esta quinta generación es fruto de un proyecto de Japón iniciado a finales de

los setenta que finaliza en 1983; el objetivo era integrar tecnologías de inteligencia artificial.

La sociedad industrial trata de llevar la evolución del *software* al mismo nivel. De forma paralela asistimos al progreso de los sistemas de comunicación que comienzan a desarrollarse a partir de 1970. En esta época la prioridad era unificar los sistemas y las arquitecturas de comunicación de los distintos fabricantes de cara a garantizar la defensa nacional; conjuntamente, el sistema debía permitir que la red de ordenadores no dependiera de uno solo, es decir, que ninguno de los nodos fuera imprescindible para el funcionamiento del conjunto. Con esta meta el Departamento de Defensa de Estados Unidos desarrolló ARPANET, antecesor de Internet.

Internet llega en 1983 y actúa como base que posibilita infinitas carreteras electrónicas cruzando el mundo. Sin embargo, no hay que confundirlo con la *world wide web (www),* que equivaldría a un vehículo empleando las vías que ofrecía Internet. La llegada de la *www* en 1990 de manos de Tim Berners-Lee supuso para Internet lo que el motor de combustión interna en los vehículos; las relaciones en Internet nunca volverían a ser lo mismo**.**

Aparece un nuevo lenguaje HTML (Lenguaje de Etiquetas de Hipertexto) que permitía enviar imágenes y vídeos además de enlaces que daban acceso a documentos de ordenadores remotos, los conocidos como *links.*

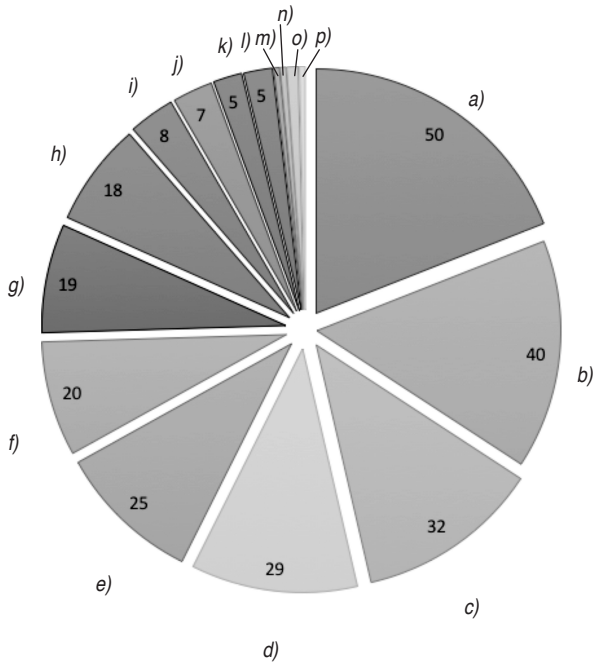
La red se hace accesible para el público cuando la NCSA (National Center for Supercomputing Applications) lanzó el navegador Mosaic. En la carrera por conquistar la red, Microsoft lanzó el navegador Internet Explorer.

2. La información en la era del *big data*

En el actual panorama mundial dominado por Internet y las redes sociales se complica cada vez más la salvaguarda de la intimidad de los usuarios en la red. Hemos llegado a un punto en que nuestros datos se han convertido en el producto más valioso de una sociedad en donde la información constituye todo un mercado.

La evolución tecnológica acelerada ha desembocado en la era de los grandes datos *(big data),* que se han convertido en la materia prima, una fuente de inmenso valor económico y social. La obtención de datos (nombres, apellidos, números de teléfono, direcciones, compras, etc.) proporciona perfiles de los sujetos que pueden ser utilizados con fines comerciales, fraudulentos, de seguridad o simplemente de control de la población. Lo

cierto es que existe un gran abanico de riesgos vinculados a almacenamiento de información personal *online*. De acuerdo con los datos publicados por el Eurobarómetro en 2015, los riesgos potenciales son los siguientes:



a) Becoming a victim of fraud
b) Your online identity being used for fraudulent purposes
c) Your information being used without your knowledge
d) Your personal information being stolen
e) Your information being shared with third parties (companies or government agencies) without your consent
f) Information being used in different contexts from those in which you provided it
g) Your information being used to send you unwanted commercial offers
h) Your personal safety being at risk
i) Your personal information being lost
j) Your reputation being damaged
k) Becoming the victim of discrimination (e. g. in job recruitment, being charged high prices, not being able to access a service)
l) Your views and behaviours being misunderstood
m) Others
n) None
o) You never provide personal information online
p) Don't know

Las bases de datos incluyen información de carácter personal, cuyo contenido lo conforman datos privados sobre la identidad (fecha de nacimiento o muerte, estado civil, propiedades, permiso de conducir...), profesión, datos económicos y fiscales, ideológicos, de salud e incluso valoraciones de la personalidad.

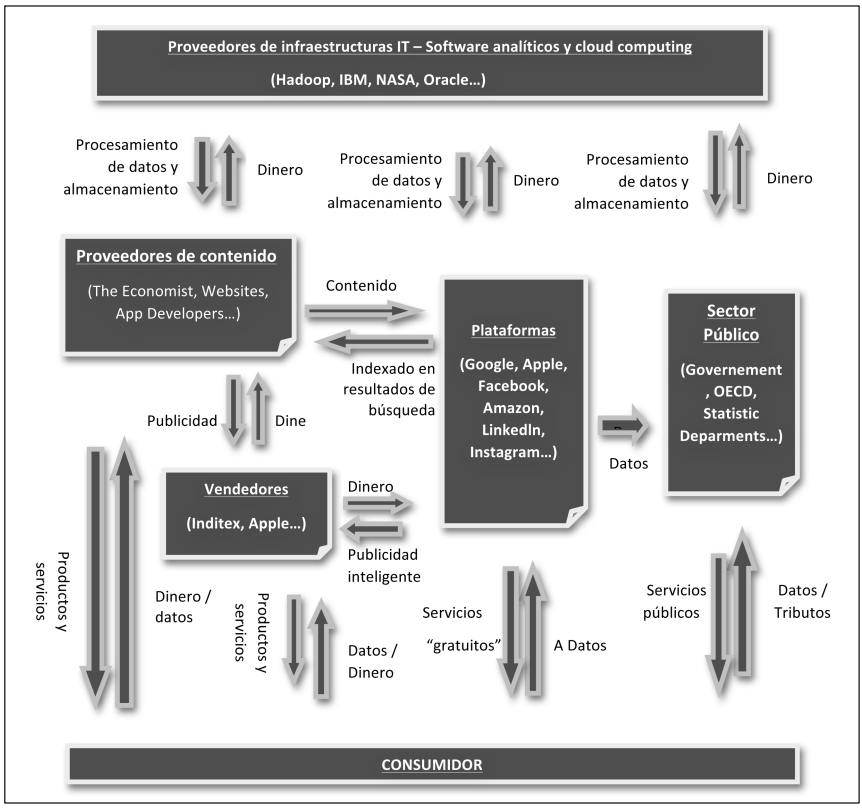
El fundamento del *big data* es doble, por un lado, hace referencia a la gran cantidad de datos disponibles, e íntimamente conectado con esto, el tratamiento masivo de la información mediante herramientas y sistemas informáticos especializados.

Aunque no sea un tema que se trate habitualmente en los medios de comunicación, las cifras que arroja el Eurobarómetro acerca de la opinión de los ciudadanos europeos sobre la protección de sus datos son muy reveladoras. Solo el 15 por 100 de la población siente que controla la información que vierte a la web, frente a un 31 por 100 que opina lo contrario. La preocupación acerca de la ausencia de control sobre la propia información se eleva al 67 por 100 de los encuestados. La conclusión que se deduce de esta encuesta, realizada en marzo de 2015, es que la protección de datos genera una gran preocupación para los ciudadanos.

La principal amenaza derivada del almacenamiento masivo de datos no solo implica a empresas privadas y operadores de Internet como Microsoft y Windows, como veremos más adelante, sino que también incluye a los Gobiernos que adquieren esos datos almacenados. Es aquí cuando chocamos con la esfera del derecho a la intimidad y a la protección de datos.

Ante la vasta cantidad de formas en que el ecosistema del *big data* actúa y por la imposibilidad de abordar todas las vías de actuación, mostramos un gráfico (página siguiente) para entender mejor este sistema antes de ampliar algunos aspectos más adelante.

Como se puede observar, la recogida de datos se puede dar de múltiples formas, mediante nuestros perfiles en redes sociales (Facebook, Instagram o Twitter), a través de compras *online,* consultas de cuentas bancarias incluso búsquedas en Google. Toda esta actividad deja un rastro y reunida puede acabar teniendo mucho valor, pues sirve para extraer conocimiento. Este conocimiento, combinado, ordenado y filtrado, proporciona patrones de comportamiento y preferencias valiosas y fundamentales para desvelar la personalidad del usuario de la red; se crean perfiles artificiales basados en el comportamiento de las personas en Internet. Esto no solo vulnera la privacidad de las personas, sino que afecta al derecho a la no discriminación y a la igualdad. La obtención de un perfil basado en una correlación entre posesión de determinadas características y comportamientos concretos sirve para encuadrar a la población en determinados grupos.



Tales previsiones serán generalmente discriminatorias, ya que estas técnicas de elaboración de clasificación de perfiles favorecen la formación de estereotipos sociales determinando tanto la atribución de privilegios y derechos como la exclusión social. Ello puede suponer una valoración desfavorable de los rasgos de una persona provocando su discriminación para la obtención de un crédito o de un empleo, o convertirla en alguien susceptible de ser vigilada y controlada por encajar en el perfil de un delincuente. Por otra parte, puede determinar incluso el acceso a la información, lo cual limita nuestro derecho a recibir información veraz; incluso se producen manipulaciones emocionales de los usuarios con base en sus intereses o perfil ideológico. De hecho, en marzo de 2018 se ha revelado cómo Cambridge Analytica obtuvo datos de los usuarios de Facebook que pudieron influir en el resultado electoral de Donald Trump en las últimas elecciones estadounidenses.

No solo los motores de búsqueda, los operadores de Internet o las redes sociales ejecutan esta función, unido a ello está el progresivo desarrollo del «internet de las cosas» [Internet of Things (IoT)], que busca conectar objetos de la vida diaria con la red global. Dentro del ámbito de la conexión ubicua, la integración de sistemas de geolocalización y una nueva tecnología llamada RFID (Radio Frecuency Identification) han suscitado una gran preocupación en relación con la posibilidad de recopilar y procesar datos personales y los efectos que esto tiene sobre el derecho fundamental a la intimidad.

Los dispositivos de geolocalización consisten en sistemas que localizan con gran precisión la posición geográfica de un objeto determinado y asociado a una persona. Las tres principales infraestructuras que posibilitan estos servicios son: las estaciones de base GSM (Global System for Mobile Communications), el Wi-Fi y el GPS. La principal vía de invasión de nuestra privacidad mediante estos sistemas va integrada en los Smartphones a través de los servicios de mapas y etiquetado geográfico de contenidos (Instagram, Snapchat o Twitter)[1].

La otra tecnología empleada para la recolección masiva de información personal son los sistemas RFID. Estos dispositivos utilizan una onda emisora integrada en el dispositivo de origen para identificar y localizar objetos. Esta tecnología plantea dos grandes amenazas: el rastreo individual y obtención de acceso a datos personales, y el uso inadecuado de información adquirida con fines de rastreo y creación de perfiles[2].

Ante las necesidades y retos que se plantean con el desarrollo de las nuevas tecnologías cobra especial importancia analizar desde una perspectiva basada en derechos humanos el derecho a la intimidad.

3. De la intimidad y privacidad al derecho a la protección de datos

El derecho a la protección de datos personales ha estado íntimamente vinculado con el derecho fundamental a la intimidad. De hecho, aun-

[1] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, Grupo de Trabajo sobre protección de los datos establecido por el art. 29, adoptado el 16 de mayo de 2011.

[2] Dictamen 9/2011 relativo a la propuesta revisada de la industria para un marco de evaluación del impacto sobre la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia, Grupo de Trabajo sobre protección de los datos establecido por el art. 29, adoptado el 11 de febrero de 2011.

que en la actualidad se ha reconocido como derecho con identidad propia separado del derecho a la intimidad, originariamente se entendió por gran parte de la doctrina como una faceta de este. Por ello es importante delimitar el contenido de la protección de datos personales frente a la intimidad antes de profundizar en el estándar internacional.

El origen de la tutela de la intimidad asociada a la vida privada proviene de Estados Unidos; en concreto, su origen se remonta a 1890 cuando Samuel Warren y Louis Brandeis invocan la noción de privacidad como derecho del individuo en su artículo «The Right to Privacy» para la *Harvard Law Review*. La definen como «el derecho de cada individuo a compartir o no con otros individuos información sobre su vida privada, hábitos, actos y relaciones». Warren y Brandeis consideraban necesario un cuerpo legal que defendiera este derecho a la privacidad, ya que la difusión al público de información sobre su vida privada podía dañar el núcleo de la personalidad del individuo. En conclusión, entendían la privacidad como la facultad de la persona de defender su integridad controlando la información que reflejaba y afectaba a su vida personal.

El *right to privacy* no era una noción verdaderamente nueva, había tenido un precedente que mencionan Warren y Brandeis en su artículo, *«the right to be let alone»* o «el derecho a estar solo», presente en la obra de Thomas Cooley *Treatise on the law of torts* (1879).

Esta concepción va evolucionando con el desarrollo de tecnologías que implican nuevos riesgos. Hay que tener en cuenta que «The Right to Privacy» se publica en un entorno en que las mayores amenazas para la privacidad eran las publicaciones en diarios y la difusión de fotografías.

En 1967 Alan F. Westin, siguiendo la línea de Charles Fried, dio una nueva definición de la *privacy.* Estamos en un contexto mundial muy distinto. Desde la Segunda Guerra Mundial se incrementan los dispositivos electrónicos de vigilancia, aunque aún no se acercan a la vigilancia masiva actual. Según su definición, la privacidad consiste en «la pretensión de los grupos, personas o instituciones de determinar por su cuenta cómo y en qué medida se distribuye información que les atañe».

A Westin le debemos el nuevo concepto de privacidad desde el enfoque de la autodeterminación. La autodeterminación de la información debe convivir con los procesos comunicativos y participativos, por ello la pretensión de privacidad del individuo no es absoluta, sino que debe ponderarse en cada caso con la voluntad de participar en la sociedad.

En Europa la evolución de las tecnologías y su efecto sobre la libertad personal es tratada de forma especialmente relevante por Vittorio Frosini,

que introduce la «libertad informática». Hasta entonces el contenido de la libertad personal se entendía únicamente en sentido negativo, a través de impedir la distribución y uso de la información del individuo; sin embargo, Frosini reconoce una libertad positiva mediante el control sobre los propios datos personales que pasan al tráfico informático.

Al mismo tiempo, hacia la mitad del siglo XX se desarrolla un debate sobre los contornos del derecho a la intimidad relevante a efectos de determinar la separación con el derecho a la protección de datos. En este campo Heinrich Hubmann formula la teoría de las esferas en 1953. Esta teoría diferencia tres sectores de la intimidad: la esfera individual, la esfera privada y la esfera de secreto, y es matizada por Henkel que añade un nuevo espacio de protección, la esfera de confianza sita entre la esfera privada y la esfera de secreto. Esta teoría, sin embargo, fue rechazada por la mayoría de la doctrina; en concreto, Morales Prats condena el planteamiento de las esferas como base del concepto de intimidad, ya que llevaría a una situación contradictoria, el individuo estaría totalmente aislado de la sociedad a medida que el sector reservado se amplía. Como solución a esto, Madrid Conesa propone la teoría de los mosaicos, que entiende que la intimidad solo tiene valor si se compagina con la participación en la sociedad.

R. S. Gerstein, por su parte, ve la privacidad y la intimidad como dos derechos distintos, aunque reconoce que uno funciona como el pilar del otro; en concreto entiende que la privacidad sirve de contexto a la intimidad. Esta misma línea sigue Shoeman, cuyo argumento se basa en que la privacidad es el marco ideal para que el individuo desarrolle las facetas de su personalidad.

En España el pionero en tratar la degradación de los derechos fundamentales por causa de las nuevas tecnologías es Antonio Enrique Pérez Luño, destacado jurista y filósofo iusnaturalista. Su obra se caracteriza por desarrollar el concepto del *habeas data* o *habeas scriptum.* Pérez Luño plantea el problema de la contaminación de las libertades en lo que denomina la tercera generación de derechos humanos. Entiende que el surgimiento del *habeas data* es consecuencia natural de las crecientes amenazas a los derechos humanos que supone el mal uso de la informática, de ahí que surja un «cauce procesal para salvaguardar la libertad de la persona en la esfera informática». Equipara el *habeas data* de los derechos de tercera generación al *habeas corpus* en los derechos de la primera generación. El estatus que se le otorga al *habeas data* como consecuencia de la consagración de la libertad informática y el derecho a la autodeterminación se concibe, según Erhard Denninger, como «facultad de cada individuo para

participar activamente y asumir su propia responsabilidad en los procesos que le afectan».

Finalmente ha sido esencial la jurisprudencia para consagrar la protección de datos personales como un derecho fundamental autónomo. Así pues, ocupa un lugar especial la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 por ser la primera vez que se reconoce el derecho a la autodeterminación informativa. Este reconocimiento parte de la interpretación del derecho al libre desarrollo de la personalidad incluido en la Ley Fundamental de Bonn, que básicamente reconoce al individuo la facultad general de disponer de sus propios datos. Denninger destaca al respecto de esta sentencia histórica que la autodeterminación como derecho se extiende tanto a los datos como a su elaboración, es decir, al uso y la aplicación que se va a dar a esos datos al margen del contenido de estos.

En España hay dos sentencias decisivas de nuestro Tribunal Constitucional: en primer lugar, la STC 254/1993, de 20 de julio, que establece que el art. 18.4 CE otorga a las personas un conjunto de facultades positivas de control sobre sus datos; esto supone el reconocimiento de un nuevo derecho fundamental autónomo del derecho a la intimidad y que podría encuadrarse en el marco más amplio que ofrece el derecho a la privacidad. Esta separación entre la intimidad y el control sobre los datos como derechos independientes se afianza a partir de la STC 292/2000, que entiende que el control sobre los datos de carácter personal otorga facultades jurídicas frente a terceros a su titular que permiten proteger otros aspectos de la dignidad de la persona y relativos a la vida privada del individuo.

III. VIGILANCIA MASIVA: EDWARD SNOWDEN

En junio de 2013 Edward Snowden filtró millones de documentos que revelaban cómo las agencias de seguridad estatales utilizaban la vigilancia masiva para recoger, almacenar y analizar en secreto millones de comunicaciones privadas de personas de todo el mundo.

La información fue publicada por *The Guardian* y *The Washington Post* de forma escalonada a lo largo del mes de junio de 2013. La fuente fue el antes citado Edward Snowden, antiguo técnico de la CIA (Central Intelligence Agency) y empleado de la NSA (National Security Agency). La información la había obtenido valiéndose de sus conocimientos informáticos y la accesibilidad que su puesto le daba a documentos clasificados. Decidió

viajar a Hong Kong para mantener su seguridad y allí se reunió con Glenn Greenwald (periodista de *The Guardian),* Laura Poitras (directora del film documental que grabó todo el proceso con Snowden en *Citizenfour)* y Ewen MacAskill (corresponsal de defensa e inteligencia de *The Guardian).*

Las publicaciones comienzan el 6 de junio y en ellas se divulga que la NSA, en virtud de una orden judicial confidencial, tenía acceso a registros telefónicos y de Internet de millones de usuarios de la operadora de telefonía Verizon en Estados Unidos. Esto permitía que Verizon enviara al FBI (Federal Bureau of Investigation) números de teléfono, datos de la localización, hora y duración de la llamada. El FBI, a su vez, lo enviaba a la NSA.

El 7 de junio se publica la existencia del programa de vigilancia PRISM (recoge correos electrónicos, voz, texto y conversaciones en vídeo de extranjeros y ciudadanos estadounidenses con extranjeros). Se descubre un sistema que permite a la inteligencia estadounidense acceder a los servidores de las principales compañías de Internet en busca de conexiones con el terrorismo internacional. Esto se traduce en que tanto la NSA como el FBI tenían acceso directo a los datos almacenados por Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube y Apple. Estas prácticas de vigilancia se realizaban simultáneamente en Reino Unido. Sale a la luz que la agencia británica de inteligencia GCHQ interceptaba comunicaciones de diplomáticos extranjeros además de grandes cantidades de datos transmitidos por fibra óptica a través de Tempora. La información recogida se compartía con la NSA.

Entre los operadores de telecomunicaciones que tuvieron un papel fundamental en el acceso de la GCHQ a las comunicaciones por fibra óptica se encuentran Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing o Viatel. Cada uno de ellos encargado de un área específica del mundo. En septiembre de 2013 salió a la luz que la GCHQ contaba con un equipo para formar «grietas» en el tráfico de datos de Hotmail, Google, Yahoo y Facebook. Tanto la agencia británica como la estadounidense contaban con la colaboración secreta de Israel, Suecia, Italia, Francia y Alemania. La agencia de inteligencia alemana, en concreto, intercambiaba información y *software* de espionaje con la NSA.

Asimismo, *The Guardian* informaba el 31 de julio sobre el sistema *Xkeyscore*, tecnología que empleaba metadatos que informan sobre quién, cuándo y dónde accede alguien a una cuenta o a quién envía un mensaje. Con ello se extraía, filtraba y clasificaba información incluida en correos electrónicos y conversaciones digitales o cualquier búsqueda en los historiales de los navegadores de Internet. Más adelante, *The New York Times*

dio a conocer que la NSA había empleado esta tecnología descrita desde 2010 para crear perfiles individuales y gráficos complejos que describían las interrrelaciones entre usuarios en las redes sociales.

El diario alemán *Der Spiegel* publicó información que demostraba el espionaje llevado a cabo por la NSA en múltiples misiones diplomáticas de la Unión Europea y en la sede de la ONU en Nueva York. Las invasiones de la NSA se produjeron también en compañías telefónicas chinas y en el operador asiático de redes de fibra óptica.

Por lo que respecta a España, se dio a conocer que «la NSA espió sesenta millones de llamadas en España entre el 10 de diciembre de 2012 y el 8 de enero de 2013, si bien la información recabada no incluyó el contenido de las llamadas, pero sí el número de teléfono del receptor y del emisor, sus ubicaciones, la duración y el número de serie de los teléfonos».

Estos fragmentos son solo una pequeña parte de los millones de documentos e información que hizo públicos Edward Snowden. Sus actos le han llevado a ser perseguido por el Gobierno de Estados Unidos por espionaje, robo y transferencia de propiedad del Gobierno. En concreto se le acusaba de violar la Espionage Act (Ley de Espionaje) de 1917, ley que prohibía de forma muy amplia el intercambio o difusión de la denominada «Información de Defensa Nacional». Nacida en el contexto de la Primera Guerra Mundial, no diferencia entre las filtraciones a la prensa por el interés público y la venta de secretos a enemigos, por lo que impide que la defensa se ampare en el interés público de la información revelada; tampoco prevé la necesidad de que se produzca un daño para el Gobierno, no exige que la actuación produzca consecuencias. Todo ello hace imposible un juicio justo para Edward Snowden.

La vigilancia masiva que había llevado a cabo Estados Unidos fue posible gracias a una estructura legal configurada por tres pilares: Foreign Intelligence Surveillance Act (FISA, 1978), USA Patriot Act (2001) y FISA Amendments Act (2008).

La Ley de Vigilancia de la Inteligencia Extranjera (FISA) nace como respuesta a los recursos federales empleados por Richard Nixon en su espionaje ilegal a grupos políticos. Surge para establecer una supervisión judicial de las actividades de vigilancia secretas realizadas sobre entidades y personas extranjeras en Estados Unidos. En caso de que en la comunicación participara un estadounidense se requería autorización judicial para intervenir.

La USA Patriot Act se aprueba durante le legislatura de George Bush como parte del conjunto de medidas legislativas antiterroristas tomadas a

partir de los atentados del 11 de septiembre de 2001 contra el World Trade Center y el Pentágono. Esta ley reconoce a los poderes públicos la potestad de vigilar e interceptar la correspondencia y comunicaciones en Internet o por teléfono de cualquier sospechoso de vinculación al terrorismo.

En 2008 se aprobaron una serie de enmiendas de la FISA que dieron lugar a la FISA Amendments Act (FAA). Con esta modificación se ampliaban los poderes de las autoridades para intervenir comunicaciones de estadounidenses en contacto con considerados «objetivos extranjeros». La propia NSA reconoció que pueden recogerse comunicaciones domésticas de forma accidental, lo que denominaron «colección de accesorios». En 2011 la Administración Obama consiguió el permiso del Tribunal de Vigilancia de Inteligencia Extranjera para eliminar las restricciones a la vigilancia de llamadas y correos por parte de la NSA. Este tribunal surgió al amparo de la Sección 702 de la FISA Amendment Act y otorgaba permisos por tiempo limitado de un año para la recogida de datos que se consideraran de interés para Estados Unidos. Las búsquedas para recoger datos se realizaban a través de un programa de vigilancia autorizado en 2011 por el Congreso bajo la Sección 702 de la Ley de Vigilancia de la Inteligencia Extranjera. Así se posibilitaba espiar a estadounidenses sin autorización ninguna cuando existiera «causa probable de que la persona se comunique con terroristas, espías o potencias extranjeras».

Las filtraciones de Snowden revelaron la existencia de la Sección 702 del FAA en los siguientes términos:

> «Los procedimientos de minimización que la FAA 702 aprobó el 3 de octubre de 2011 ahora permiten la utilización de ciertos nombres de personas de Estados Unidos y los identificadores como términos de consulta en la revisión de datos recogidos por la FAA 702».

El término «identificadores» en el lenguaje de la NSA sirve para aludir a la información relativa a una persona (incluye su número de teléfono, dirección de correo electrónico, dirección IP, nombre del usuario y nombre propio).

Las pruebas aportadas por Snowden en los millones de documentos publicados tuvieron un impacto mundial e impulsaron la denuncia de estas actividades por parte de distintas instituciones y organizaciones internacionales.

La Asamblea General de la Organización de las Naciones Unidas aprobó el 18 de diciembre de 2013 la resolución 68/167 relativa al derecho a

la privacidad en la era digital, con motivo de la propuesta de Brasil y Alemania pidiendo respeto y protección para el derecho a la privacidad. La ONU expresa mediante esa resolución su preocupación por los «efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones»; menciona, en concreto, la «interceptación extraterritorial» y «a gran escala», haciendo clara referencia a la red de espionaje masivo operada por Estados Unidos a través de la NSA.

La misma preocupación recoge Frank William la Rue (relator especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y de expresión) en un informe conjunto en que colabora con Catalina Botero Marino (relatora especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos de la OEA). Ambos entienden que el pleno goce de los derechos humanos no puede verse restringido por estrategias antiterroristas y muestran su preocupación al respecto de la inadecuada legislación en materia de inteligencia y seguridad frente al desarrollo de las nuevas tecnologías en la era digital. En consonancia con la resolución de la Asamblea General 68/167 resaltan que «preocupan de manera especial los efectos intimidatorios que el acceso indiscriminado a datos sobre la comunicación de las personas pueda generar sobre la libre expresión del pensamiento, búsqueda y difusión de información».

El Parlamento Europeo reaccionó a las revelaciones filtradas teniendo en cuenta la legislación que amparaba la red de vigilancia masiva y se pronunció en el verano de 2013 a través de la Dirección General de Políticas Interiores en una publicación en materia de justicia, igualdad y seguridad relativa a «Los programas de vigilancia de los Estados Unidos y sus repercusiones sobre los derechos fundamentales de los ciudadanos de la UE», donde declara lo siguiente:

> «El empleo de estos programas de vigilancia por la agencia de seguridad de Estados Unidos refleja la indiferencia de las autoridades ante el derecho humano de la privacidad de los ciudadanos no americanos. Los programas de vigilancia y la legislación estadounidense (Patriot Act, FISA y FAA) indican que estas actividades se llevaron a cabo sin respeto por los derechos de los residentes y ciudadanos no estadounidenses. En concreto, FAA (Fisa Admendments Act) tiene un alcance que permite vigilar de forma masiva datos de ciudadanos no estadounidenses que estén fuera de los Estados Unidos, lo cual elude la normativa europea en materia de protección de datos».

Continuando en el ámbito europeo, fue decisiva la Directiva 95/46/CE en virtud de la cual se creó el Grupo de Trabajo del art. 29. Se trata de un órgano consultivo europeo independiente sobre la protección de datos y la vida privada. El Grupo del art. 29 emitió el Dictamen 4/2014 sobre la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional, en el que condenaba el comportamiento de las agencias nacionales de seguridad en los siguientes términos:

> «El derecho a la intimidad y a la protección de los datos de carácter personal es un derecho fundamental consagrado en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta de Derechos Fundamentales de la Unión Europea. De ello se deduce que el respeto del Estado de Derecho implica necesariamente que este derecho recibe el mayor grado de protección posible.
>
> A partir de este análisis, el Grupo concluye que los programas de vigilancia secretos, masivos e indiscriminados son incompatibles con nuestras leyes fundamentales y no pueden justificarse por motivos de lucha contra el terrorismo u otras importantes amenazas a la seguridad nacional. Las restricciones en los derechos fundamentales de todos los ciudadanos solo pueden ser admisibles si son estrictamente necesarias y proporcionadas en una sociedad democrática».

Cabe mencionar que el Grupo de Trabajo del art. 29 ya se había pronunciado antes del escándalo de 2013. Destaca la preocupación transmitida a través del Dictamen 10/2001 sobre la necesidad de un enfoque equilibrado en la lucha contra el terrorismo. Posteriormente tendría lugar la Decisión del Consejo de 17 de mayo de 2004, referida a la celebración del Acuerdo entre la Comunidad Europea y Estados Unidos de América sobre el tratamiento y la transferencia de los datos relativos a expedientes de pasajeros de las compañías aéreas al departamento de seguridad nacional. A pesar de que fue anulada por el Tribunal de Justicia de la Unión Europea en una Sentencia de 30 de mayo de 2006, merece la pena recoger la respuesta del Grupo del art. 29 plasmada en los Dictámenes 6/2002 y 4/2003 que ponía en duda la finalidad de tal acuerdo por la inseguridad que generaba al respecto de los datos obtenidos, su conservación, transferencia y uso.

IV. PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES

A continuación, vamos a tratar de configurar el estándar internacional del derecho a la protección de datos personales basado en un enfoque de derechos humanos. De entrada, es imprescindible explicar el desarrollo de este derecho a lo largo del tiempo y su origen.

La invisibilidad de este derecho fundamental dificulta gravemente la concienciación de la sociedad civil ante las continuas amenazas o riesgos a los que se enfrenta nuestra privacidad. No obstante, desde 1990 se denota un paulatino progreso en cuanto a la consideración de estos riesgos.

Al referirnos al derecho a la protección de datos, nos referidos a un derecho fundamental de la denominada tercera generación. Esta categoría de derechos humanos se emplea para recoger una nueva tipología de derechos que nacen como consecuencia de un nuevo contexto tecnológico, sociológico, económico y cultural.

Una vez alcanzado el concepto de protección de datos o autodeterminación informativa como un derecho fundamental autónomo conviene precisar qué datos son los protegidos. El Tribunal Europeo de Derechos Humanos ayuda a concretar el concepto en la sentencia *Malone c. Reino Unido.* En ella se entiende que no solo los datos de una conversación o de la comunicación deben ser protegidos; al margen de estos existen los denominados metadatos[3], que son los que la sentencia incluye bajo el amparo del art. 8 de la Carta de Derechos Fundamentales en los siguientes términos:

> «Como el Gobierno señala con razón, un contador, dotado de un aparato impresor, anota las informaciones que el servicio de teléfonos puede, en principio, conseguir lícitamente, especialmente para asegurar la exactitud de los cargos que se exigen al abonado, examinar sus reclamaciones o descubrir posibles abusos. El recuento es distinto, por su propia naturaleza, de la interceptación de las comunicaciones, la cual y en principio no es deseable ni lícita en una sociedad democrática. El Tribunal no acepta, sin embargo, que la utilización de los datos así obtenidos no pueda plantear problemas en relación con el art. 8. En los registros así efectuados se

[3] Según la RAE los metadatos son datos sobre otros datos. En el contexto informático que a nosotros nos interesa, los metadatos hay que entenderlos como las circunstancias que rodean la comunicación o la expresión del individuo, es decir, en una llamada los datos será el contenido de la conversación y los metadatos la hora de la llamada, la duración, destinatario, localización y operador telefónico.

> contienen informaciones —en especial, los números marcados— que son parte de las comunicaciones telefónicas. En opinión del Tribunal, ponerlos en conocimiento de la policía sin el consentimiento del abonado se opone también al derecho confirmado por el art. 8».

Aclarado el origen y desarrollo del derecho a la protección de datos se procede a analizar el marco jurídico en que se enmarca este derecho a distintos niveles para deducir el estándar internacional de la protección de datos.

1. Marco internacional

En el contexto contemporáneo de la sociedad de la información, tratar de conciliar el principio general de libre circulación de la información con las libertades individuales fundamentales es, sin duda alguna, una preocupación internacional constante. Existe la necesidad de procurar un marco legal de protección de la libertad informática frente al tratamiento automatizado de los datos personales. Este marco legal internacional se articula a través de distintos instrumentos tales como la Declaración Universal de Derechos Humanos (DUDH), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), las Observaciones e informes de Naciones Unidas, directrices de la OCDE y de la Organización de Estados Americanos.

En primer lugar, la Declaración Universal de Derechos Humanos, documento proclamado por la Asamblea General de la ONU en 1948, surge como ideal común para todos los pueblos y naciones, y en ella se establecen los derechos fundamentales que deben ser protegidos en todo el mundo. En concreto protege el derecho a la intimidad en su art. 12, dentro de los derechos del individuo en relación con la comunidad:

> «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

En los mismos términos se expresa el Pacto Internacional de Derechos Civiles y Políticos[4]. Dentro de este cuerpo normativo y de forma muy simi-

[4] El Tratado multilateral general que reconoce los derechos civiles y políticos fue adoptado por la Asamblea General de Naciones Unidas a través de la Resolución 2200 A (XXI),

lar a la Declaración Universal de Derechos Humanos, el art. 17 regula el derecho fundamental a la intimidad:

> «Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación».

Tanto en la DUDH como en el PIDCP se emplea el término «injerencias arbitrarias». El Comité de Derechos Humanos de la ONU ha interpretado este concepto entendiendo que con «arbitrariedad» se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto, y sea, en todo caso, razonable en las circunstancias particulares.

Esta interpretación está incluida dentro de la Observación General núm. 16 de 1998[5]. Es la respuesta del Comité de Derechos Humanos al respecto del art. 17 del Pacto Internacional de Derechos Civiles y Políticos, cuyo precepto reproduce casi exactamente la redacción del art. 12 de la Declaración Universal de los Derechos Humanos. En ambos casos se hace referencia al concepto de «vida privada»; sin embargo, en la Observación se prevé el «derecho a la intimidad».

La Observación tenía como objetivo aclarar el concepto de injerencias ilegales y arbitrarias a la vida privada, la familia y domicilio, etc. Sin perjuicio de lo anterior, en el mismo texto se amplía el ámbito de la privacidad y se tiene en cuenta el derecho a la autodeterminación informativa en la vertiente que nos ocupa, el control sobre los propios datos:

> «La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley [...]. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos».

---

de 16 de diciembre de 1966. Entró en vigor el 23 de marzo de 1976 y ha sido ratificado por 167 Estados.

[5] Observación General núm. 16, Comentarios generales adoptados por el Comité de los Derechos Humanos, art. 17, Derecho a la intimidad, 32.º periodo de sesiones, UN Doc. HRI/GEN/1/Rev.7 at 162 (1988).

No obstante, esta no era la primera vez que se prestaba atención a este tema. La ONU ya había comenzado a tomar conciencia de la incidencia del uso de la electrónica en los derechos individuales a raíz de la Conferencia Internacional de Derechos Humanos celebrada en Teherán en 1968. Como resultado de la Conferencia la ONU adoptó una resolución, la «Proclamación de Teherán», en la que instaba al secretario general a profundizar en el estudio del impacto de la electrónica en la esfera jurídica de las personas y los límites que la sociedad democrática debería imponer. El texto adoptado reconoce expresamente la creciente preocupación al respecto en el apartado 18:

> «Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evolución puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente».

Sin embargo, a pesar de los intentos por profundizar y clarificar los límites en este tema tanto del secretario general como del Comité de Derechos Humanos se lograron escasos avances. El debate internacional quedó paralizado en gran medida por la creencia de la mayoría de la comunidad internacional de que era prematuro abordar el impacto de la informática en los derechos humanos. No se puede obviar que en el momento en que se desarrollan estos trabajos, históricamente asistíamos al nacimiento de los primeros ordenadores personales de Apple y Macintosh e Internet estaba dando sus primeros pasos, pero estaba aún lejos de ser la red mundial que es ahora.

La preocupación por la invasión en la autonomía personal y la concienciación intelectual de la limitación que esta amenaza supone para el reconocido derecho de autodeterminación informativa, junto con los recientes acontecimientos acerca de la realidad de programas de recopilación masiva de datos, justifican que las Naciones Unidas hayan puesto el foco de interés en esta nueva manifestación del derecho a la intimidad.

En concreto, se da un importante avance en 1991 con la Resolución de la Asamblea General de Naciones Unidas de 29 de enero, por la que se aprueban un conjunto de directrices de Naciones Unidas para la regulación de ficheros automáticos de datos personales, así como para tratar de establecer unos parámetros globales en defensa de la privacidad informática.

Las directrices introducidas se caracterizan por su generalidad y flexibilidad, pero esto, lejos de ser visto como un posible problema, se traduce en una gran facilidad para ser incorporadas por los Estados; finalidad con que se conciben. Una característica relevante es la introducción del término «datos sensibles». Esta categoría más detallada hace referencia a «datos susceptibles de dar lugar a discriminaciones ilícitas o arbitrarias». La doctrina jurídica internacional inserta aquí todo tipo de información relativa al origen racial o étnico, opiniones políticas o religiosas, color de piel, vida sexual, opiniones filosóficas o incluso afiliación sindical.

La OCDE ha tenido también un papel fundamental en la creación de un marco jurídico para la protección de la vida privada y los datos personales. A este respecto destacan las líneas directrices de la OCDE que gobiernan la protección de la vida privada y la transmisión internacional de datos personales («The OCDE guidelines governing the protection af privacy and transborder flows of personal data»), expresamente recogidas en la Recomendación del Consejo de 23 de septiembre de 1980.

En la parte segunda de estas directrices se establecen unos principios básicos para la correcta aplicación de las mismas. Estos principios se perfilan como un primer estándar internacional de este derecho:

1. Principio de recogida limitada: debe haber límites a la hora de recoger datos personales y su recogida debe ser por medios legítimos y justos y, en su caso, con el conocimiento o consentimiento de la persona afectada.
2. Principio de calidad de datos: los datos personales deben ser relevantes para los fines para los que se van a emplear, así como precisos, completos y actualizados.
3. Principio de finalidad específica: deben especificarse los fines para los que se recogen esos datos y el posterior uso limitado a los fines previstos.
4. Principio de limitación de uso: los datos personales no deben ser puestos a disposición de terceros o revelados, pues supondría una violación del anterior principio. No obstante, si media consentimiento del sujeto de datos o por autoridad de la ley, sí cabe emplear los datos para fines distintos.
5. Principio de salvaguarda de seguridad: los datos personales deben ser protegidos con medidas de seguridad razonables contra riesgos tales como pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación.

6. Principio de apertura: debe haber una política de apertura sobre los medios empleados y desarrollados para la obtención de datos.
7. Principio de participación individual: el sujeto tendrá derecho a obtener información de un controlador de datos acerca del uso de sus propios datos. La información comunicada debe ser en un tiempo razonable y de forma fácilmente inteligible. En caso de que le sea negada esta información o no se aporte adecuadamente, el sujeto tendrá derecho a desafiar tal negación para conseguir la eliminación, modificación o actualización de sus datos.
8. Principio de responsabilidad: un controlador de datos tiene la obligación de ser responsable a la hora de cumplir las exigencias de los principios anteriores.

Todo lo relativo a la transmisión internacional de los datos personales ha sido enfatizado y reformado en 1985 fruto de la adopción el 22 de marzo de 1985 de la «Organization's Comittee on Information, Computers and Communications».

Si bien es cierto que las Recomendaciones de la OCDE no son vinculantes jurídicamente, incitan a los Estados a mantener un buen equilibrio en el campo de la protección de datos personales.

A estas disposiciones se suma la inestimable aportación de Frank William la Rue, relator especial de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión. En concreto se pone de especial relieve el tema que nos ocupa en su informe del 17 de abril de 2013. El informe «analiza las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión. Al tiempo que se analizan los efectos de los importantes adelantos tecnológicos en las comunicaciones, en el informe se subraya la necesidad urgente de seguir estudiando nuevas modalidades de vigilancia y de examinar las leyes nacionales que reglamentan estas prácticas de conformidad con las normas de derechos humanos».

A pesar de ser previo a las revelaciones de Edward Snowden, aborda muy acertadamente las cuestiones que cobrarían mayor protagonismo a partir del verano de 2013. Las recomendaciones del experto se centran en actualizar y fortalecer las normas jurídicas a la vista de que «la vigilancia de las comunicaciones debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos de libertad de expresión y a la intimidad, y que atenta contra los fundamentos de la sociedad

democrática». Para ello propone un marco jurídico que garantice que las medidas de vigilancia de comunicaciones:

a) estén en consonancia con la ley, cumplan con las normas de claridad y precisión suficientes para que las personas sean notificadas por adelantado y puedan prever su aplicación;
b) sean estricta y fehacientemente necesarias para lograr un objetivo legítimo, y
c) se ajusten al principio de proporcionalidad y no se empleen cuando se disponga de técnicas menos invasivas o cuando estas no se hayan agotado.

Estos principios configuran el estándar internacional del derecho a la protección de los datos personales. Se consolidan así las directrices enunciadas por la OCDE, pero adaptándolas al momento histórico y a los avances y acontecimientos de la sociedad.

También se desprende de las conclusiones el mandato de crear mecanismos o tribunales que supervisen la provisión de datos por parte de los Estados.

Por último, Frank la Rue recomienda aumentar el acceso público a la información, la comprensión y el conocimiento de las amenazas a la intimidad y la reglamentación de la comercialización de tecnología de vigilancia, así como el fomento de la evaluación de las obligaciones pertinentes de derechos humanos. Al respecto de esto último pone de manifiesto la necesidad de actualizar la Observación General núm. 16 (1988), sobre el derecho a la intimidad, del Comité de Derechos Humanos.

A consecuencia de la creciente preocupación sobre los peligros que acechan a la privacidad, la ONU creó el cargo de relator especial sobre privacidad en 2015, ocupado actualmente por Joseph Cannataci, quien ha mostrado su preocupación acerca del modo en que los Gobiernos líderes mundiales están impulsando medidas de vigilancia excesivamente intrusivas gracias al juego de la «carta del miedo» con los ciudadanos.

Recientemente ha sido abordado el tema sobre el tratamiento y recogida de datos por la Asamblea General de la Organización de Estados Americanos (OEA), la cual en marzo de 2014 compiló una serie de principios relativos a la privacidad y protección de datos. El documento fue resultado de la Resolución AG/RES.2811 (XLIII-O/13), por la que se encomendó al Comité Jurídico Interamericano que «formule propuestas a la Comisión de Asuntos Jurídicos y Políticos sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de ley modelo

sobre protección de datos personales, tomando en cuenta los estándares internacionales alcanzados en la materia».

En el texto legal resultante se llegan a diferenciar cuatro principios que ya enunciaba Frank la Rue en el informe antes mencionado. En primer lugar, el principio de legitimidad de propósito; en segundo lugar, exigencia de claridad y consentimiento; en tercer lugar, principio de necesidad y pertenencia, y, por último, uso limitado y retención. A la luz de estas exigencias, el derecho a la protección de datos se regulará en los siguientes términos:

— Los datos y la información personales deben ser recopilados solamente para fines legítimos y por medios justos y legales.
— Se deben especificar los fines para los cuales se recopilan los datos y la información personales en el momento en que se recogen. Como regla general, solamente deben ser recopilados con el conocimiento o el consentimiento de la persona a que se refieran.
— Deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación.
— Deben ser mantenidos y utilizados solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más tiempo del necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente.

2. Legislación europea

Los pilares de la defensa del derecho a la protección de datos en la Unión Europea son la Carta Europea de Derechos Fundamentales; el Convenio Europeo de Derechos Humanos, al que ya hemos hecho mención; la Directiva 95/46/CE en virtud de la cual se crea el Grupo de Trabajo del art. 29 (GT 29), y el Reglamentos de 25 de mayo de 2016 que entrará en vigor este año 2018.

2.1. *Carta Europea de Derechos Fundamentales*

El único instrumento normativo de garantía en materia de derechos fundamentales en Europa hasta el año 2000 era el CEDH, ya que fue entonces cuando quedó proclamada en Niza la Carta de Derechos Funda-

mentales de la Unión Europea. Su elaboración fue encargada a una convención que siguió un método intermedio entre el parlamentario y el intergubernamental, lo que aportó transparencia al procedimiento confiriendo al documento final un plus de legitimidad.

Hay que destacar que reconoce el derecho a la protección de datos como derecho autónomo del derecho a la vida privada[6], lo que no ocurría en el CEDH. Expresamente se recoge en el art. 8, que establece lo siguiente:

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

La redacción de este artículo estaba inspirada en cuatro elementos: el art. 286 del Tratado Constitutivo de la Comunidad Europea[7], la Directiva 95/46/CE, el art. 8 CEDH y el Convenio núm. 108.

Con la entrada en vigor del Tratado de Lisboa en diciembre de 2007, las instituciones europeas proclamaron solemnemente la Carta y con ello se hizo jurídicamente vinculante para los Estados miembros (art. 6 TUE). No fue un proceso fácil, ya que numerosos países se oponían a ello, como Suecia, Dinamarca, Irlanda o Reino Unido, pero finalmente pasó a formar parte del denominado *«soft law»,* como norma que permite interpretar o completar las disposiciones comunitarias dotadas de fuerza jurídica[8].

---

[6] Art. 7 CDFUE.

[7] Art. 286: «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 art. 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».

[8] Al respecto *vid.* M. Arenas Ramiro, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, 2006, pp. 214-218.

2.2. *Directivas*

Las Directivas forman parte del Derecho derivado de la UE, solo son obligatorias para los Estados miembros respecto del objetivo que proponen y su contenido no sustituye directamente al Derecho nacional. Los Estados deben adecuar su normativa a la legislación comunitaria mediante la transposición.

La protección de datos personales en el marco de la Unión Europea pasa inexcusablemente por el estudio de la Directiva 95/46/CE de protección de datos, antecedente de la legislación española que luego veremos brevemente.

Hasta el momento, en Europa se había intentado armonizar los diferentes regímenes de protección de datos de los Estados miembros sin mucho éxito, pues tanto las resoluciones del Comité de Ministros de 1973 y 1974 sobre la protección de datos en el sector público y privado respectivamente como el Convenio núm. 108 del Consejo de Europa[9] al que precedían acusaban importantes debilidades en su aplicación. Cabe destacar que el Convenio fijaba un estándar mínimo de protección y tenía por objeto resguardar los datos personales como forma de proteger el derecho a la vida privada, con el fin de liberalizar la circulación de datos entre los países de la Unión Europea.

La puesta en marcha del mercado interior requería un régimen unificado en la política de transmisión de datos dentro de la Unión Europea. De esta y otras necesidades resulta la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El contenido de este texto de referencia a escala europea en materia de protección de datos personales se sintetiza en la fijación de unos límites estrictos para la recogida y utilización de datos personales. Establece unos principios para poder calificar como lícito el tratamiento de datos:

— el interesado ha dado inequívocamente su consentimiento;
— el tratamiento es necesario para el cumplimiento de un contrato en el que sea parte el interesado;

[9] Convention 108 of the Council of Europe (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in Strasbourg on January 28th, 1981).

— el tratamiento es necesario para el cumplimiento de una obligación legal del responsable del tratamiento;
— el tratamiento es necesario para proteger los intereses vitales de la persona de cuyos datos se trate;
— el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero, o
— el tratamiento es necesario para los fines de interés legítimo del responsable del tratamiento o de un tercero, siempre que sobre dichos intereses no prevalezcan los intereses del interesado en el ámbito de los derechos y libertades que requieren protección.

De forma complementaria y análoga al modelo que venían marcando las resoluciones de organismos internacionales, recoge unos principios de calidad de los datos en virtud de los cuales enuncia que «todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados».

Este sería a grandes rasgos el régimen jurídico aplicable en las operaciones de tratamiento de datos realizadas dentro de la Unión Europea.

Ocurre que el mayor problema es el intercambio más allá de las fronteras europeas y a ello se refiere el capítulo IV de la Directiva relativo a la «Transferencia de datos personales a países terceros». El art. 25 admite *la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia*, previo examen de la Comisión acerca de si el país destinatario de la información garantiza un nivel de protección adecuado.

No obstante, el artículo siguiente admite varias excepciones, permitiendo que incluso en aquellos Estados donde no existan unas garantías de seguridad en el tratamiento de datos, podrán transferirse siempre que la entidad receptora concreta se comprometa a cumplir las normas de la Unión Europea (así se recoge en la Consideraciones 58, 59 y 60 de la Directiva).

2.3. *Decisión 520/2000*

Gracias a esta posibilidad que abre la Directiva, el 26 de julio de 2000 la Comisión Europea aprueba la Decisión 2000/520 —acuerdo Safe Harbor («Puerto Seguro») con el Departamento de Comercio de Estados Unidos—. En virtud de este sistema, las empresas estadounidenses interesadas en adquirir datos de ciudadanos europeos podrían acceder a ellos asumiendo voluntariamente el cumplimiento de la normativa europea por lo que respecta al tratamiento de esos datos. Dice así la consideración quinta de la Decisión:

> «El nivel adecuado de protección de la transferencia de datos desde la Comunidad a Estados Unidos de América, reconocido por la presente Decisión, debe alcanzarse si las entidades cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un Estado miembro a Estados Unidos de América [...]. Además, las entidades deben dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la Federal Trade Commission (Comisión Federal de Comercio, FTC) a tenor de lo dispuesto en el art. 5 de la Federal Trade Commission Act, en la que se prohíben actos o prácticas desleales o fraudulentas en el comercio o en relación con él, o a la jurisdicción de otros organismos públicos que garanticen el cumplimiento efectivo de los principios y su aplicación de conformidad con las FAQ».

Estos mecanismos de ingeniería jurídica fueron los que posibilitaron que la NSA recopilara información de forma masiva no solo de ciudadanos o residentes en Estados Unidos, sino en toda Europa, contando con la colaboración de servidores de Internet y agencias de seguridad estatales como la de Reino Unido.

Los efectos de las revelaciones de 2013 tuvieron también repercusión sobre la fiabilidad de este mecanismo de Puerto Seguro y por ello salió al paso la Comisión Europea, que en fechas posteriores a la publicación de las filtraciones adoptó la Comunicación al Parlamento Europeo y al Consejo de 27 de noviembre de 2013 que lleva por título «Restablecer la confianza en los flujos de datos entre la UE y Estados Unidos» (COM 2013). Complementariamente se publicó un informe en la misma fecha que contiene las «Conclusiones de los copresidentes de la Unión Europea del

grupo de trabajo *ad hoc* Unión Europea-Estados Unidos sobre protección de datos personales»[10].

En estos informes la Comisión reconocía que *algunas empresas estadounidenses certificadas no respetaban los principios enunciados en el art. 1, apartado 1, de la Decisión 2000/520 (en lo sucesivo, «principios de puerto seguro»)*. A continuación pone de manifiesto la necesidad de mejorar algunos ámbitos de la Decisión 2000/520 al señalar que «deben subsanarse las deficiencias estructurales relacionadas con la transparencia y la aplicación, y deben reforzarse los principios sustantivos del régimen de puerto seguro y la aplicación de la excepción por motivos de seguridad nacional».

Sin embargo, más allá de estas correcciones, en ningún caso se manifiesta duda alguna de la legalidad de la Decisión 2000/520; al contrario, se intenta recuperar la confianza perdida en el sistema europeo de protección de datos, cuyas bases quedaron seriamente cuestionadas ante la demostración de que existían varios programas de vigilancia que comprendían la recogida y el tratamiento de información a gran escala de datos personales.

Pero lo cierto es que al Safe Harbor no le quedaría mucho tiempo. La Gran Sala del Tribunal de Justicia de la Unión Europea, en su Sentencia de 6 de octubre de 2015, resolvió la cuestión prejudicial planteada por la High Court irlandesa a raíz del litigio iniciado por Max Schrems contra el Data Protection Commissioner. Lo relevante a efectos de la legislación europea existente hasta 2013, y en concreto respecto a la Decisión 2000/520/CE, es que el Tribunal declaró la invalidez de esta legislación. Las consecuencias de esta resolución fueron enormes, ya que la Decisión invalidada era la base legal que permitía el tráfico de datos con Estados Unidos. Adicionalmente, tuvo un impacto económico directo sobre las empresas que de facto se dedican a la transferencia, almacenamiento y tratamiento de datos como Facebook, Google o Amazon, entre otras.

Aunque el Safe Harbor no fue tumbado hasta la sentencia del TJUE, una institución que ocupa un papel primordial en la protección de datos, el Grupo de Trabajo del art. 29 creado por la Directiva 95/46/CE, ya había manifestado ciertas preocupaciones que despertaba aquel acuerdo Unión Europea-Estados Unidos.

Por presentar brevemente el Grupo Europeo de Protección de Datos del art. 29, es un órgano consultivo independiente integrado por las auto-

[10] «Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection».

ridades de protección de datos de todos los Estados miembros, el supervisor europeo de protección de datos y la Comisión Europea. El GT 29 tiene como labor el estudio de las cuestiones relativas a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva 95/46, emite dictámenes sobre el nivel de protección dentro de la Unión Europea y en países terceros, asesora a la Comisión y formula recomendaciones en materias relacionadas con la protección de datos. Aunque sus decisiones no son jurídicamente vinculantes, tienen un gran valor doctrinal y son tenidas en cuenta por los legisladores y órganos jurisdiccionales nacionales y europeos.

El GT 29 fue muy crítico con la solución tomada en el 2000, como se desprende de distintos dictámenes, recomendaciones y opiniones (por ejemplo, en el Dictamen 5/2007, de 17 de agosto).

Adicionalmente se pronunció el 16 de octubre de 2015 al respecto de la sentencia del TJUE en el caso C-362/14, que invalidaba la decisión de Puerto Seguro. EL GT 29 consideró que la vigilancia masiva llevada a cabo por la NSA era incompatible con la normativa europea de protección de datos. A partir de ello hace un llamamiento a los Estados miembros con el fin de buscar soluciones que proporcionen garantías suficientes en esta materia.

La Directiva 95/46/CE fue sustituida por la Directiva 97/66/CE, de 15 de diciembre de 1997, sobre tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones. Esta segunda norma tenía por objeto actualizar su precedente, pero su vigencia fue corta, la sustituyó la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas. Más recientemente se aprobó la Directiva 2006/24/CE relativa a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones, pero fue invalidada por el TJUE en abril de 2014.

2.4. *Reglamento Europeo de Protección de Datos*

La clásica Directiva 95/46/CE será derogada este mismo año por el Reglamento Europeo de Protección de Datos, que ya entró en vigor el 25 de mayo de 2016, pero el mismo día de este año finaliza el periodo de dos años de adaptación dado a los Estados miembros, convirtiéndose ya definitivamente en obligatorio en todos sus elementos y directamente apli-

cable en los Estados. Algunas de las novedades más significativas son la unificación de la normativa, creando unidad de criterio tanto en privacidad como en protección de datos, y el surgimiento de la figura del delegado de protección de datos encargado de supervisar el cumplimiento de la normativa correspondiente. Además, las autoridades nacionales tendrán la competencia de autorizar previamente los flujos de datos antes de que estos se produzcan y no solo después de que se produzcan vulneraciones de la normativa, y el nuevo régimen sancionador establece multas del 4 por 100 del volumen de negocios total anual.

3. Jurisprudencia del Tribunal de Justicia Europea: C. Max Schrems, *Europa vs. Facebook*

El señor Max Schrems, de nacionalidad austriaca y usuario de Facebook, decidió presentar una reclamación pidiendo que sus datos personales no pudieran ser transferidos más a Estados Unidos en función de que no estaba garantizada una protección suficiente de los mismos, como había quedado demostrado al conocerse las actividades de vigilancia practicadas por el Gobierno de ese país. Pedía además que el comisario europeo para la protección de datos realizara un examen sobre la seguridad en estas transferencias.

Max Schrems comenzó tres procedimientos: una petición ante el comisario de protección de datos en Irlanda para que iniciase una investigación sobre Facebook, una demanda en la Corte Suprema de Austria y el procedimiento ante el comisario de protección de datos irlandés por el Safe Harbor.

El tercer procedimiento es en el que me voy a centrar, ya que aborda la cuestión más importante, la validez o no de la Decisión 520/2000. En este marco, el hecho de que el sujeto demandado sea Facebook no es especialmente relevante, ya que solo es un ejemplo más de lo que hacen las compañías privadas.

El señor Schrems comenzó a preocuparse por su privacidad a partir de las revelaciones de Edward Snowden sobre la recogida de datos de la NSA mediante PRISM o Tempora. Estas filtraciones servirían de base para respaldar sus pretensiones como luego veremos.

La estrategia legal que siguió Schrems se basaba en el hecho de que, si existía vigilancia masiva desde Estados Unidos, era lógico deducir que equivalía a una ausencia de protección adecuada de los datos.

Hay que partir de que los datos de los ciudadanos situados fuera de Estados Unidos y Canadá con cuenta en Facebook están sometidos a un contrato con Facebook Ireland Ltd., domiciliado en Irlanda, y no con Facebook Inc. (Estados Unidos). Técnicamente la información es legalmente recogida, pero pasa a los servidores de Facebook Inc. De acuerdo con el Safe Harbor, el envío de datos a terceros países fuera de la UE exige un nivel adecuado de protección en el país de destino. Ocurre que en Estados Unidos se demostró que no había tales niveles de protección debido a las evidencias que Edward Snowden había presentado.

3.1. *Procedimiento*

El procedimiento comenzó con la presentación de una queja ante TRUSTe, autoridad que establece los requisitos de privacidad a cumplir por las empresas en la recogida de información personal y vigila el cumplimiento de los marcos regulatorios. La reclamación no prosperó, ya que la empresa se declaró no competente para conocer del asunto, a saber, interrumpir la relación entre Facebook Inc. y PRISM. A continuación acudió ante la Comisión Federal de Comercio[11], obteniendo la misma respuesta. Lo cierto es que ninguna de estas dos instituciones tenía poder para intervenir en el objeto de litigio.

El siguiente paso fue enviar una petición a Billy Hawkes, el comisario de protección de datos[12] irlandés en aquella fecha. Este, al igual que las instancias anteriores, con las que por cierto no guarda relación, desestimó la reclamación. Hay que destacar que de las peticiones que le llegaban en un año, alrededor del 98 por 100 no eran admitidas. No obstante, el caso de Max había adquirido gran importancia mediática, y poco tiempo después, Billy Hawkes fue entrevistado en la radio acerca de las quejas recibi-

[11] La Comisión Federal de Comercio (Federal Trade Commission o FTC) es una agencia independiente del Gobierno de Estados Unidos establecida en 1914 por el Acta de la Comisión Federal de Comercio (Federal Trade Commission Act). Su misión principal es promover los derechos de los consumidores y la eliminación y prevención de prácticas que atentan contra la libre competencia.

[12] La Oficina del Comisionado de Protección de Datos trabaja a través de varias estrategias de cumplimiento, incluida la acción judicial cuando sea necesario, para defender los derechos de las personas a acceder a sus propios datos personales, ya sea en el ordenador o en un archivo en papel. La Oficina también desempeña un papel en el desarrollo de un enfoque armonizado para la protección de datos en toda la Unión Europea. Transcripción propia a partir de *www.dataprotection.ie*

das sobre protección de datos, a lo que este respondió: «No creo que sea una sorpresa el hecho de que los servicios de inteligencia estadounidenses tengan acceso a las compañías estadounidenses».

Esta simple afirmación supuso una gran esperanza para Schrems, porque suponía que una autoridad había admitido la veracidad de la vigilancia masiva. Fue muy importante porque una de las cuestiones más complejas del procedimiento era probar que estos sistemas de vigilancia eran reales. Es obvio que las compañías lo negarían.

A pesar de esta aparente victoria, el señor Hawkes respondió desestimando la queja de Max sobre la base de una dudosa interpretación de los términos de la Data Protection Act de 1988-2003; en concreto alegó que el art. 10 no establecía un mandato irrenunciable para investigar las peticiones, ya que *«shall»* debe interpretarse como *«may»*. Todo se redujo a la relativa imperatividad del término empleado. Además, el comisario mantuvo que el señor Schrems carecía de *locus standi* para realizar estas quejas, ya que no tenía pruebas de que la NSA hubiera accedido a su información personal. Se dijo que la reclamación era esencialmente hipotética y especulativa.

La única vía que quedaba era la Irish High Court (por ser Irlanda el domicilio social de Facebook en Europa), ante la cual demandó al comisionario por no cumplir con su deber. Al tener lugar la vista ante el juez, este reconoció la pretensión y se pronunció en los siguientes términos:

> «Si el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente».

Aunque formalmente no se impugna la validez de la Directiva 95/46 ni de la Decisión 2000/520, en el planteamiento del recurso por parte del señor Schrems subyace la idea de si es lícito el régimen de «puerto seguro» y si de verdad garantiza en la práctica protección en la transferencia de datos personales.

La High Court entendía que el asunto de fondo planteaba dudas acerca de la aplicación del Derecho de la Unión, sobre el sentido del art. 51 de la Carta de Derechos Fundamentales, por lo que acordó suspender el procedimiento en curso y plantear al Tribunal de Justicia de la Unión Europea una cuestión prejudicial:

> «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 arts. 7, 8 y 47 de la Carta y no obstante lo dispuesto en el art. 25, apartado 6, de la Directiva 95/46/CE?
>
> En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que han tenido lugar desde que se publicó por vez primera la Decisión 2000/520?».

3.2. *Fundamentos jurídicos*

El envío de datos desde Facebook a la NSA implica una doble dimensión, la vigilancia es doble, pública (NSA) y privada (Google, Facebook, etc.). Facebook está sometido a la ley estadounidense pero también a la ley europea que regula las transferencias con tercetos países. Si bien solo hay jurisdicción sobre las compañías privadas como Facebook o Google por estar domiciliadas aquí, pero no sobre la labor de la NSA, son estas las que al fin y al cabo hacen posible la vigilancia masiva.

La estrategia legal que se siguió partía de que el art. 25 de la Directiva 95/46 debía ser interpretado a la luz de los arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea que amparan el respeto a la vida privada y familiar y la protección de datos de carácter personal, respectivamente.

Es necesario poner en relación el art. 3 del Safe Harbor con el art. 25 de la Directiva, el cual faculta a las autoridades competentes de los Estados miembros para ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales en el caso de que «existan grandes probabilidades de que se estén vulnerando los principios [art. 25 de la Directiva]; existen razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión».

El problema de la Decisión de Puerto Seguro llega al acudir a los principios del Anexo I, concretamente al párrafo 4.º, que reconoce una serie

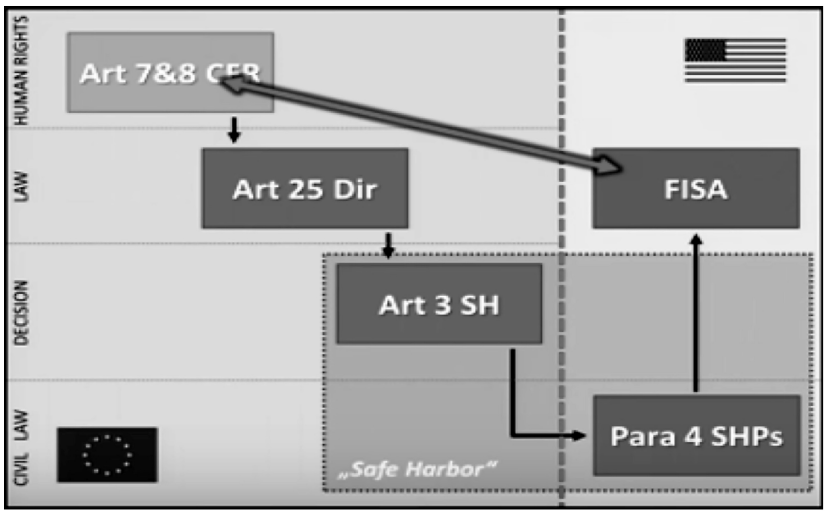
de excepciones que pueden alegarse para eximir de la adhesión a los principios del Safe Harbor. Las excepciones son:

a) razones de seguridad nacional;
b) conflicto de obligaciones o autorizaciones con disposiciones legales o reglamentarias, o jurisprudencia del tercer país;
c) excepción prevista en la Directiva o normas de Derecho interno de los Estados miembros.

En virtud de esta disposición se legitima la aplicación de la ley FISA, la cual contradice directamente los arts. 7 y 8 CDFUE. Así, todo el sistema de protección queda *de facto* desarticulado por la vía de estas amplísimas excepciones.

3.3. *Resolución*

El Tribunal de Luxemburgo solo decide acerca de la adecuación a la legalidad o no, no entra a juzgar los hechos en el caso concreto. En este caso el asunto llegó a la Gran Sala compuesta por el presidente del TJUE Vassilios Skouris, el ponente Thomas von Danwitz, el abogado general Yves Bot y la secretaria L. Hewlett, en colaboración con dos presidentes de la Sala y otros ocho jueces.



Finalmente, en la Sentencia de 6 de octubre de 2015 el TJUE declaró la invalidez del Puerto Seguro con eficacia inmediata. Estableció que la vigilancia masiva supone una violación de la esencia del art. 7 CDFUE. Fue una resolución sin precedentes, pues es extremadamente difícil que se llegue a estimar vulneración de la esencia de un derecho. Implica que se trata de una actuación que va más allá de toda legalidad, que no puede estar justificada en ningún caso y que viola directamente el núcleo de un derecho fundamental, es totalmente inadmisible.

Resumiendo, es inválida, esencialmente, por dos motivos:

— Entiende que prevalece incondicionalmente y sin ninguna limitación «*la seguridad nacional, el interés público o el cumplimiento de la ley*» sobre los derechos fundamentales a la intimidad y la protección de datos, sin otorgar a los ciudadanos europeos ningún medio para obtener la tutela efectiva de esos derechos.
— No otorga a los Estados miembros un margen suficiente para suspender las transferencias en caso de que estos apreciaran una vulneración de los derechos de los ciudadanos europeos (Nota de la AEPD de 6 de octubre de 2015), pues la Comisión carece de competencia para restringir las facultades de las autoridades nacionales de control.

Otro punto clave de la resolución radica en la concreción de la expresión «nivel adecuado» por lo que respecta a la protección del tercer país. Se determinó que es un término indeterminado vacío de contenido legal y se cambió por nivel de seguridad «esencialmente equivalente».

A consecuencia de la sentencia, la autoridad irlandesa de protección de datos quedó obligada a examinar la reclamación del señor Schrems con la diligencia exigible para decidir si, en virtud de la Directiva, debe suspenderse la transferencia de datos de los usuarios de Facebook europeos a Estados Unidos.

V. CONCLUSIÓN

De las consideraciones jurídicas que se derivan del análisis de la vigilancia masiva expuesta por Edward Snowden, pasando por la legislación internacional y europea con la que entra en conflicto, así como la respuesta de los tribunales y organizaciones internacionales, queda reforzada y justificada la tesis de que la vigilancia masiva es una realidad de nuestros días, propiciada por el desarrollo de unas nuevas tecnologías al servicio de los pode-

res públicos y empresas privadas y el creciente valor de la información en nuestra sociedad. Una realidad que es manifiestamente contraria a Derecho, y en especial invasiva de nuestra privacidad, por vulnerar el derecho fundamental a la protección de datos personales y, colateralmente, menoscabar el derecho a la libertad de expresión y a la no discriminación.

La cuestión en la práctica, más allá de si estos sistemas se ajustan o no a la ley, es si los Estados policía son efectivos y proporcionan realmente seguridad nacional. Cuando han ocurrido ataques terroristas no cabe duda de que existían datos sobre quienes los cometían, y esta es la verdadera realidad de la vigilancia masiva. Es el hecho de que cuando se vigila a todo el mundo sabes que esos individuos están en las bases de datos, existe la información necesaria para prevenir tales atrocidades. Pero el problema es que cuando se abarca una red inmensa de datos, cuando se recopila todo, no es posible entender nada.

La conclusión es que no son sistemas efectivos en la lucha contra el terrorismo y suponen una vulneración inadmisible de un derecho fundamental. Por tanto, no es real ni legal ofrecer seguridad a cambio de tener acceso a la vida privada de todo el mundo, porque los resultados no llevan a ninguna parte, simplemente se están violando derechos fundamentales gracias a discursos de terror.

VI. BIBLIOGRAFÍA

Calvo, D.: «Empresa privada y participación digital: modelo de negocio y derecho de petición en Change.org», *OBETS, Revista de Ciencias Sociales,* vol. 11, núm. 1 (2016), pp. 97-128.

Denningek, E.: «El derecho a la autodeterminación informativa», en A. E. Pérez Luño (ed.), *Problemas actuales de la documentación y la informática jurídica (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986),* Madrid, Tecnos-Fundación Cultural Enrique Luño Peña, 1987, pp. 268 y ss.

— «Government Assistance in the Exercise of Basic Rights (Procedure and Organization)», en C. Joerges y D. M. Trubek (ed.), *Critica/Legal Thought: An American-German Debate,* Baden-Baden, Nomos, 1989.

Frosini, V.: *Informática y Derecho,* trad. de J. Guerrero y M. Ayerra Redín, Bogotá, Temis, 1988.

Galán Muñoz, A.; Arribas León, M., *et al.*: *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación,* Valencia, Tirant lo Blanch, 2014.

GARRIGA DOMÍNGUEZ, A.: *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua*, Madrid, Dykinson, 2015.

GERSTEIN, R. S.: *Intimacy and Privacy* y *Philosophical Dimensions of Privacy,* Cambridge, Cambridge University Press*,* 1984.

GILLIES, J., y CAILLIAU, R.: *How the Web was Born: The Story of the World Wide Web*, Oxford, Oxford University Press, 2000.

GLANCY, D. J.: «The Invention of the Right to Privacy», *Arizona Law Review,* vol. 21 (1979), pp. 1-39.

GREENWALD, G.: «XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"», *The Guardian,* 31 de julio de 2013.

HERRÁN ORTIZ, A. I.: «El derecho a la protección de datos personales en la sociedad de la información», *Cuadernos Deusto de Derechos Humanos,* núm. 26 (2003).

LYON, D.: «Surveillance Studies. An Overview», *Canadian Journal of Sociology/ Cahiers canadiens de sociologie,* vol. 33, núm. 2 (2008).

MARTÍNEZ, R.: «El derecho fundamental a la protección de datos: perspectivas», *IDP: Revista D'Internet, Dret i Política,* núm. 5 (2007).

MURILLO DE LA CUEVA, P. L.: «La construcción del derecho a la autodeterminación informática», *Revista de Estudios Políticos,* Nueva Época, núm. 104 (1999), pp. 35-60.

PÉREZ LUÑO, A.: «Del habeas corpus al habeas data», *Informática y Derecho. Revista iberoamericana de Derecho informático,* núm. 1 (1992), pp. 153-161 (ponencia presentada a las Jornadas sobre el proceso informatizado dentro del XIV Curso sobre «Informática y Derecho» organizado por el Centro Regional de la UNED de Extremadura).

RIGAUX, F.: *La protection de la vie privée et des autres biens de la personnalité,* Bruxelles, Bruylant, 1990.

RISEN, J., y POITRAS, L.: «NSA Gathers Data on Social Networks of US Citizens», *The New York Times,* 28 de septiembre de 2013.

SALDAÑA, M. N.: «La protección de la privacidad en la sociedad tecnológica: el derecho constitucional a la privacidad de la información personal en los Estados Unidos», *Araucaria: Revista iberoamericana de filosofía, política, humanidades y relaciones internacionales,* núm. 18 (2007), pp. 85-115.

SERRA, R.: «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *Revista de Derecho Político,* núm. 92 (2015), pp. 73-118.

STEWART, D. P.: «Privacidad y protección de datos», 84.º Periodo ordinario de sesiones de la Asamblea General de la OEA, marzo de 2014 (CJI/doc. 450/14).

WARREN, S. D., y BRANDEIS, L.: *El derecho a la intimidad,* ed. de B. PENDÁS y P. BASELGA, Madrid, Civitas, 1995.

WASSERSTROM, R. A.: «Privacy, Some Arguments and Assumptions», en F. SCHOEMAN (ed.), *Philosophical Dimensions of Privacy,* Cambridge, Cambridge University Press*,* 1984, pp. 315-332.

WEBER, R. H.: «Internet of Things, New Security and Privacy Challenges», *Computer Law and Security Review,* vol. 26, núm. 1 (2010), pp. 23-30.

WESTIN, A. F.: «Privacy and Freedom», *Washington and Lee Law Review,* vol. 25, núm. 1, art. 20, 1968.

WRIGHT, D.; GUTWIRTH, S.; FRIEDEWALD, M.; HERT, P.; LANGHEINRICH, M., y MOSCIBRODA, A.: «Privacy, Trust and Policy-Making: Challenges and Responses», *Computer Law & Security Review*, vol. 25, núm. 1, 2009, pp. 69-83.

Otras fuentes (páginas web, medios de comunicación, etc.)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: «Resolución de Madrid adoptada por la 30.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad», *Estándares Internacionales sobre Protección de Datos Personales y Privacidad, www.agpd.es.*

— *Guía de Protección de Datos para Responsables de Ficheros*.

ÁLVAREZ CARO, M.ª: «El nuevo paradigma de la privacidad en la era digital», 11 de marzo de 2014, disponible en *http://www.abogacia.es/2014/03/11/el-nuevo-paradigma-de-la-privacidad-en-la-era-digital/.*

AMNISTÍA INTERNACIONAL: *https://www.es.amnesty.org/en-que-estamos/temas/vigilancia-masiva/.*

CAZURRO BARAHONA, V.: «Peligra el Sistema de Transferencia de Datos Personales entre la Unión Europea y Estados Unidos», disponible en *https://www.ui1.es/blog-ui1/peligra-el-sistema-de-transferencia-de-datos-personales-entre-la-union-europea-y-eeuu.*

Citicenfour, 2014, documental disponible en *https://www.youtube.com/watch?v=4EgTXEn15ls&t=495s.*

«El origen de la privacidad: The Right to be Alone», *Revista Internacional de Protección de Datos*, disponible en *https://revistaprotecciondatos.wordpress.com/2015/03/05/el-origen-de-la-autodeterminacion-informativa-the-right-to-be-alone/*.

«La NSA rastreó 60 millones de llamadas telefónicas en España», *ABC,* 29 de octubre de 2013.

MARTÍN, A.: «¿Qué es el Safe Harbor y qué implica su anulación para los ciudadanos de la UE?», disponible en *https://hipertextual.com/2015/10/anulacion-safe-harbor.*

Nota sobre «Los programas de vigilancia de los Estados Unidos y sus repercusiones sobre los derechos fundamentales de los ciudadanos de la UE», a cargo de la Dirección General de Políticas Interiores del Parlamento Europeo (PE 474.405), 2013.

SALAMANCA AGUADO, E.: «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», *Revista del Instituto Español de Estudios Estratégicos,* núm. 4 (2014).

SCHREMS, M.: *Safe Harbor,* disponible en *https://www.youtube.com/watch?v=xBZUHrHIhQU*.

«Un vacío legal permite a la NSA registrar las comunicaciones de estadounidenses», *Actualidad RT,* 10 de agosto de 2013.

www.theguardian.com.

www.harvardlawreview.org.

www.europe-v-facebook.org.

www.derechoshumanos.net.

www.oas.org.

www.un.org.