

José Antonio Fernández Amor
(Director/Coordinador)

DIGITALIZACIÓN, EMPRESA Y DERECHO

DIGITALIZACIÓN, EMPRESA Y DERECHO

CONSEJO EDITORIAL

MIGUEL ÁNGEL COLLADO YURRITA

JOAN EGEA FERNÁNDEZ

ISABEL FERNÁNDEZ TORRES

JOSÉ IGNACIO GARCÍA NINET

JAVIER LOPÉZ GARCÍA DE LA SERRANA

BELÉN NOGUERA DE LA MUELA

LUIS PRIETO SANCHÍS

FRANCISCO RAMOS MÉNDEZ

RICARDO ROBLES PLANAS

SIXTO SÁNCHEZ LORENZO

JESÚS-MARÍA SILVA SÁNCHEZ

JOAN MANUEL TRAYTER JIMÉNEZ

JUAN JOSÉ TRIGÁS RODRÍGUEZ

Director de publicaciones

DIGITALIZACIÓN, EMPRESA Y DERECHO

José Antonio Fernández Amor

Director/Coordinador

Autores

Sandra Camacho Clavijo

Josep Cañabate Pérez

José Antonio Fernández Amor

Zuley Fernández Caballero

Carolina Gala Durán

Miguel Gardeñes Santiago

Carles Górriz López

Jorge Miquel Rodríguez

Susana Navas Navarro

Miguel Ángel Sánchez Huete

Josep Suquet Capdevila

El presente trabajo se encuadra en el proyecto “Reorientación de los instrumentos jurídicos para la transición empresarial hacia la economía del dato” financiado por el Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación, con referencia PID2020-113506R-100 REFERENCIA DEL PROYECTO/AEI/10.13039/501100011033. IP: Dr. José Antonio Fernández Amor

Reservados todos los derechos. De conformidad con lo dispuesto en los arts. 270, 271 y 272 del Código Penal vigente, podrá ser castigado con pena de multa y privación de libertad quien reproducere, plagiar, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística o científica, fijada en cualquier tipo de soporte, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

Este libro ha sido sometido a un riguroso proceso de revisión por pares.

© 2024 Los autores y las autoras

© 2024 Atelier

Santa Dorotea 8, 08004 Barcelona

e-mail: editorial@atelierlibros.es

www.atelierlibrosjuridicos.com

Tel. 93 295 45 60

I.S.B.N.: 978-84-10174-99-3

Depósito legal: B 18801-2024

Impresión: Podiprint

ÍNDICE

PRESENTACIÓN.	9
<i>José Antonio Fernández Amor</i>	

PRIMERA PARTE LA EMPRESA Y SU ORGANIZACIÓN

I. Empresa y organización interna

ANÁLISIS DE LA PROBLEMÁTICA DEL TELETRABAJO DESDE LA PERSPECTIVA DE LA PREVENCIÓN DE RIESGOS LABORALES.	15
<i>Carolina Gala Durán</i>	

LA CONSTITUCIÓN EN LÍNEA DE SOCIEDADES DE RESPONSABILIDAD LIMITADA. LA INCORPORACIÓN AL DERECHO ESPAÑOL DE LA DIRECTIVA 2019/1151 Y LA PROPUESTA DE REFORMA DE LA NORMATIVA EUROPEA . . .	43
<i>Jorge Miquel Rodríguez</i>	

II. Empresa y ubicación territorial

EL PRINCIPIO DEL ESTADO DE ORIGEN ENTRE LA DIRECTIVA DE COMERCIO ELECTRÓNICO, EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y EL REGLAMENTO DE SERVICIOS DIGITALES	63
<i>Miguel Gardeñes Santiago</i>	

LA PROTECCIÓN DE LOS USUARIOS DE LAS PLATAFORMAS DE INTERCAMBIO DE VÍDEOS (PIV): ASPECTOS DE INTERÉS PARA LA DETERMINACIÓN DE LA COMPETENCIA JUDICIAL INTERNACIONAL EN MATERIA CONTRACTUAL.	99
<i>Josep Suquet Capdevila</i>	

SEGUNDA PARTE
LA EMPRESA Y SUS RELACIONES CON TERCEROS

I. Empresa y responsabilidad

LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES A ESTADOS UNIDOS: EL “TRANSATLANTIC CLASH” DE DOS CULTURAS DE PRIVACIDAD	123
--	------------

Josep Cañabate Pérez

LA EMPRESA DE SALUD DIGITAL Y LA IMPLEMENTACIÓN DE SISTEMAS DE IA: CUESTIONES DE RESPONSABILIDAD CIVIL EN EL NUEVO MARCO EUROPEO	153
---	------------

Sandra Camacho Clavijo

LOS MODELOS DE INTELIGENCIA ARTIFICIAL DE PROPÓSITO GENERAL Y RESPONSABILIDAD CIVIL. APROXIMACIÓN CRÍTICA	177
--	------------

Susana Navas Navarro

II. Empresa y actividad

REGLAMENTO DE MERCADOS DIGITALES: ¿UNA SOLUCIÓN A LOS PROBLEMAS DEL ART. 102 TFUE?	195
---	------------

Carles Górriz López

BENEFICIOS FISCALES POR LA REALIZACIÓN DE ACTIVIDADES DE I+D+I PARA LAS PERSONAS FÍSICAS	221
---	------------

Zuley Fernández Caballero

III. Empresa y Administración tributaria

PERFILES DE RIESGO FISCAL CREADOS POR INTELIGENCIA ARTIFICIAL	251
--	------------

Miguel Ángel Sánchez Huete

REFLEXIONES SOBRE BIENES INTANGIBLES BASADOS EN CONJUNTOS ESTRUCTURADOS DE DATOS O CRIPTOACTIVOS Y LA APLICACIÓN DE LOS TRIBUTOS	277
---	------------

José Antonio Fernández Amor

I. Empresa y responsabilidad

LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES A ESTADOS UNIDOS: EL “TRANSATLANTIC CLASH” DE DOS CULTURAS DE PRIVACIDAD

Josep Cañabate Pérez

Profesor agregado de Historia del Derecho
Universitat Autònoma de Barcelona

ABSTRACT:

The main objective of this chapter is to analyze the controversial legal regime of personal data transfers to the United States. Using the comparative law methodology, the concept of U.S. privacy is studied to determine the reasons that lead the EU to consider that it does not have an adequate level of protection. On the other hand, it focuses on the EU-US Data Privacy Framework, an instrument to guarantee the processing of Europeans' personal data by American organizations that adhere to it, which is preceded by a series of agreements annulled by the EU judiciary.

Keywords: International data transfer, privacy, Data Privacy Framework, personal data protection.

Palabras clave: Transferencia internacional de datos, privacy, Data Privacy Framework, protección de datos personales.

SUMARIO:

1. INTRODUCCIÓN; 2. DATA PRIVACY AMERICANA VERSUS PRIVACIDAD Y PROTECCIÓN DE DATOS EUROPEA: 2.1. El surgimiento del derecho a la privacidad en el Common Law. 2.2. Las restricciones de la Primera Enmienda al derecho a la privacidad. 2.3. El derecho a la privacidad en el derecho constitucional 2.4. Statutory Law y derecho a la privacidad 3. EL NUEVO PRIVACY DATA FRAMEWORK TRANSATLÁNTICO: 3.1. Antecedentes: Safe Harbor y Privacy Shield 3.2. EU-US Privacy Data Framework 3.3. La Orden Ejecutiva 14086 “Enhancing Safeguards in United States Signals Intelligence Activities” 4. CONCLUSIONES 5. BIBLIOGRAFÍA

1. INTRODUCCIÓN

El 10 de julio de 2023 la Comisión Europea aprobó la decisión de adecuación para posibilitar la transferencia de datos personales entre entidades de la Unión Europea y de los Estados Unidos bajo el denominado *EU-US Data Privacy Framework*¹. Este nuevo instrumento supone el último, y a buen seguro no definitivo acto, del choque jurídico entre dos modelos de poderes digitales, el *market-driven* de los EEUU y el *rights-driven* de la UE, descritos por Anu Bradford en su reciente obra *Digital Empires: The Global Battle to Regulate Technology* (Bradford, 2023).

El Tribunal de Justicia de la Unión Europea (TJUE en adelante) en su sentencia de 16 de julio de 2020 en el asunto C-311/18, *Data Protection Commissioner* contra Facebook Ireland Limited y Maximillian Schrems (Schrems II en adelante) había invalidado la Decisión de ejecución de la comisión 2016/1250 sobre el flujo de datos transatlántico, el Escudo de Privacidad UE-EEUU (*Privacy Shield*). El alto tribunal europeo consideró que las limitaciones de protección de datos personales derivadas de la legislación nacional de los Estados Unidos sobre el acceso y el uso de datos transferidos de la UE al país norteamericano por parte de las autoridades estadounidenses no satisfacía los requisitos esenciales equivalentes al derecho de la Unión en relación con la necesidad y proporcionalidad. El tribunal señaló también la inexistencia de un órgano de garantía al cual pudieran dirigirse los ciudadanos europeos para presentar sus reclamaciones sobre posibles vulneraciones de su protección de datos por parte de las agencias de inteligencia norteamericanas tal como establece el artículo 47 de la Carta sobre el derecho a recurso efectivo.

Tras la nueva anulación por parte del TJUE del marco jurídico para la transferencia de datos personales a los Estados Unidos se iniciaron conversaciones entre las autoridades de este país y la Comisión (UE) para poder elaborar una nueva decisión que cumpliera con los requisitos establecidos en el apartado 2

1. Las normas sobre transferencias de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones se establecen en el capítulo V del RGPD.

del artículo 45 del Reglamento (UE) 2016/679². Esta norma establece que la adopción de una decisión de adecuación debe basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que abarque tanto las normas aplicables a los importadores de datos, así como las limitaciones y salvaguardias en materia de acceso a datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección “esencialmente equivalente” al garantizado dentro de la Unión (considerando 104 del Reglamento (UE) 2016/679).

El Tribunal de Justicia de la Unión Europea ya había señalado en su conocida sentencia de 6 de octubre de 2015 en el asunto C-362/14, Maximilian Schrems (Schrems I, en adelante) contra *Data Protection Commissioner* de Irlanda que no se requiere encontrar un nivel de protección idénticos. En este sentido, los medios a los que recurre el tercer estado para proteger los datos personales pueden diferir de los empleados en la Unión, siempre que resulten en la práctica eficaces para garantizar un nivel adecuado de protección.

El objetivo principal de este capítulo es analizar el ordenamiento jurídico de los Estados Unidos en lo referente a la privacidad a luz de los principios y estándares jurídicos de la UE para establecer si el *Data Privacy Framework* supone un instrumento adecuado de protección que colme la brecha jurídica entre los modelos que señala la mencionada autora, Anu Bradford. La hipótesis es que el *DPF* es una huida hacia adelante, pues la economía digital transatlántica no se puede detener, pero a pesar de las mejoras se está lejos de lograr un régimen de protección equivalente.

Para desarrollar el objetivo mencionado en la primera parte se realiza un análisis del concepto de *Data Privacy* en los Estados Unidos, en la segunda parte se lleva a cabo un estudio del EU-US *Data Privacy Framework*.

2. DATA PRIVACY AMERICANA VERSUS PRIVACIDAD Y PROTECCIÓN DE DATOS EUROPEA

La *privacy* es uno de los pilares de la cultura de derechos y libertades de los Estados Unidos, constituyendo un mecanismo de garantía para el sistema jurídico norteamericano de una importancia comparable, aunque menor, a la libertad de expresión recogida en la Primera Enmienda. Sus efectos jurídicos y las formas en que se manifiesta son múltiples, y en muchas ocasiones no encuentra una figura equivalente en el derecho europeo. Resulta paradójico que, a pesar de las notables diferencias actuales, el concepto original de *privacy* americano haya

2. En el artículo 45, apartado 3, del Reglamento (UE) 2016/679, establece que la Comisión podrá decidir mediante un acto de ejecución, que un tercer país, un territorio o uno o más sectores específicos dentro de un tercer país garanticen un nivel adecuado de protección. En esta condición, las transferencias de datos personales a un tercer país podrán tener lugar sin necesidad de obtener ninguna autorización adicional, según lo previsto en el artículo 45, apartado 1, y el considerando 103 del Reglamento (UE) 2016/679.

tenido una decisiva influencia en la creación y desarrollo de la privacidad y la protección de datos en los países de *civil law*. No solo el conocido artículo doctrinal de Warren y Brandeis, “The Right to Privacy” (Warren, Brandeis 1890, pp. 193-220)., sino también las primeras leyes sobre *information privacy* en los años 70, han sido importantes referentes en el desarrollo del derecho de la privacidad y protección de datos europeo.

En términos de cultura jurídica no es baladí que sea un artículo doctrinal el que sirva de arranque de un nuevo derecho en el *Common Law*, el cual acabó siendo refrendado por el Tribunal Supremo de los Estados Unidos y constituyendo el *Tort of Disclosure*. Algunos autores norteamericanos consideran que este trabajo académico ha sido el más influyente en la historia del derecho americano³. Ciertamente, supone un hito jurídico que unos académicos, en realidad ilustres juristas bostonianos, lograran este enorme impacto. Desde la Europa apegada a las solemnes declaraciones de derechos, o a las convenciones internacionales elaboradas por el restringido y exquisito club de Estados, puede parecer anecdótico. Sin embargo, este proceso de elaboración jurídica muestra como el *Common Law* americano es un derecho dúctil, dinámico y que reacciona ante los retos que le plantea la realidad.

La Europa postrevolucionaria de la codificación tuvo una vocación totalizante en el ámbito jurídico: sin Estado y sin regulación no debía haber derecho. Este fenómeno es denominado por Paolo Grossi como “absolutismo jurídico” (Grossi 1996, pp. 94-99). El liberalismo jurídico europeo abogó por la desaparición del acervo jurídico de Antiguo Régimen o lo arrojó a la marginalidad. El americano, por el contrario, ha recelado tradicionalmente de cualquier intervención del Estado y de sus regulaciones.

Esta concepción tan ontológica del derecho americano sigue vigente en la actualidad a pesar de los retos que supone la transformación digital. Ante la aprobación de legislación federal o estatal sobre protección datos algunos influyentes autores como Jack Balkin, profesor de derecho constitucional en Yale, anteponen el principio de la libertad de discurso recogido en la Primera Enmienda. Este autor sostiene, “[U]no de los desarrollos más importantes en el último cuarto de siglo es el surgimiento de la Primera Enmienda y del principio de libertad de discurso como una de las herramientas anti-regulatorias para los abogados de empresa” (Balkin, 2004, pp. 1-55). Balkin denomina a este fenómeno jurídico como *Second Gilded Age*⁴ haciendo una analogía con el momento histórico tras la Guerra de Secesión en el que se impidió la regulación del gobierno

3. Roscoe Pound afirmó sobre que el artículo “[did] nothing less than add a chapter to our law”, citado en Alpheus Manson, *Brandeis: a Free Man's Life*, 70 (1946). Harry Kalven lo ha calificado como “[the] most influential law review article of all”, *vid.* Kalven (1966), pp. 326-341.

4. La denominada *Gilded Age* (1870-1891) fue un periodo de gran expansión económica, industrial y demográfica que se inició tras la Guerra de Secesión y se extendió durante dos décadas. No obstante, se produjeron grandes desigualdades sociales y económicas, y una alta conflictividad social. En el ámbito jurídico hay que destacar como los tribunales transformaron la ideología de la libertad de trabajo en un principio constitucional de la libertad de contratación que impidió a los gobiernos

de las relaciones de trabajo. La historia del derecho del trabajo en los EEUU muestra como los *Statutes* recogen en muchas ocasiones los avances jurídicos establecidos en la jurisprudencia, mientras que algunas regulaciones acaban marginadas por su no aplicación por los tribunales.

En la Unión Europea estos postulados anti-regulatorios resultan incomprensibles, cuando la norma general y abstracta, como es el RGPD, puede ser un instrumento muy eficaz para proteger a los datos personales de los ciudadanos en todos los ámbitos. Sin embargo, el derecho a la “*information privacy*” estadounidense, tal como se ha apuntado, comprende un amplio cuerpo legal compuesto por *Common Law*, derecho constitucional *Statutory Law* (federal y estatal) y derecho extranjero. Un sistema plural, sectorizado y casuístico que desde la óptica europea puede conllevar a la desprotección.

A continuación, se va a profundizar en los orígenes y tipologías de la privacidad, y su derivada la “*information privacy*” en el sistema jurídico de los Estados Unidos.

2.1. El surgimiento del derecho a la privacidad en el Common Law

En el desarrollo de los *tort remedies* para proteger la privacidad de las vulneraciones procedentes de la tecnología, tal como se ha indicado, fue muy relevante la publicación en 1890 del artículo de Warren y Brandeis⁵. El mismo no solo supone un referente en la historia del derecho de la privacidad, sino que también es alegado por la jurisprudencia actual, como ocurrió en el caso *Kyllo v. United States* en 2001. Los autores de la publicación clásica describieron a la *privacy* “*[as not] the principle of private property but that of inviolate personality*”. James Whitman relaciona esta idea de derecho de personalidad, con el concepto de libertad de la filosofía alemana del siglo XIX. Los autores no basaron su construcción jurídica novedosa en la libertad ante el gobierno, o ante el mercado, sino en la capacidad de desarrollar libremente su potencial como individuo. Warren y Brandeis definieron este nuevo derecho a la privacidad como

regular los salarios y las condiciones de trabajo. Sobre este momento histórico-jurídico *vid.* Les Benedict (1985), pp. 293-331, Forbath (1985), pp. 767-817.

5. Los orígenes de esta sentencia han generado debate académico, *vid.* Barron (1979), pp. 875-922. En todo caso como señala Nieves Saldaña: “[p]or todo, a finales del siglo XIX el suelo constitucional norteamericano estaba ya sembrado de principios heredados de la tradición jurídica inglesa, que receptionados en el sistema jurídico de las colonias habían alcanzado plasmación constitucional en las Enmiendas ratificadas en 1791 y en las aportaciones de conocidos constitucionalistas. Sin embargo, el gran desarrollo de la prensa y la proliferación de mecanismos de reproducción de imágenes, especialmente gracias a los avances en la fotografía, generalizó que en el último tercio del siglo XIX proliferaran las publicaciones por la prensa sensacionalista de aspectos relativos a la vida privada, frente a los que no podía ejercitarse acción legal alguna en defensa de una supuesta violación de la privacidad.” Saldaña Díaz (2012), p. 207.

“*the right to be alone*”. Esta idea había sido acuñada por el Juez Thomas Cooley en su tratado sobre el *Law of Torts* (Cooley, 1888, p. 29).

Los autores del ilustre artículo habían puesto de manifiesto como las acciones existentes en el *Common Law* no resultaban adecuadas para proteger la privacidad, pero podían ser modificadas para lograr este objetivo. Esta reivindicación fue atendida en 1903 tanto por los tribunales como por el legislador creando *torts* para proteger la privacidad. En 1903 en Nueva York se creó por ley (*Statute*) un *tort* de privacidad. Georgia, en el caso *Pave v. New England Life Insurance Co.* (1905) fue el primer Estado en reconocer una *common law tort action* para las vulneraciones de la privacidad.

Unas décadas más tarde, en 1960, William Prosser escribió un conocido artículo, *Privacy*, en el cual examinando más de 300 sentencias desde la publicación de Warren y Brandeis, estableciendo el siguiente concepto de privacidad:

“The law of privacy comprises four distinct kinds of invasion of four different interest of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, “to be let alone”. Without any attempt at exact definition, these four torts may be described as follows:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for defendant's advantage, of the plaintiff's name or likeness.” (Prosser, 1960, p. 383)

En la taxonomía que hace Prosser del concepto *privacy* se puede observar, tal como el mismo autor señala, cuatro tipologías que responden a conceptos muy diversos. Si tomamos como ejemplo el derecho español, aunque sería muy similar en el resto de los ordenamientos continentales, la revelación de hechos falsos o la suplantación identidad se corresponderían con instituciones tales como la difamación o la apropiación del estado civil. Edward Bloustein, replicando la crítica que hace Prosser cuando alega que no tienen nada en común, sostiene que aquello que une a estas figuras es la protección de la “dignidad humana” y “personalidad” (Bloustein, 1964, pp. 962-1007). Robert Post, por su parte, añade que estas categorías constituyen una forma de respeto por otras personas en el seno de la comunidad (Post, 1989, pp. 957-1010).

El *Restatement of Torts*⁶ reconoció, y sigue reconociendo en la actualidad, los cuatro *torts* descritos en el artículo de Prosser. Los mismos son denominados

6. En la jurisprudencia estadounidense, *Restatements of the Law* son un conjunto de tratados sobre temas legales que tratan de informar a los magistrados y abogados acerca de los principios generales del *Common Law*.

de forma conjunta como “*invasion of privacy*”. Estos *torts* serían: (1) *intrusion upon seclusion*, (2) *public disclosure of private facts*⁷, (3) *false light*⁸, y (4) *appropriation*. (Solove, Rotenberg, Schwartz, 2005, p. 30)

A los mismos hay que añadir el *Breach of Confidentiality*, que pretende dar una compensación cuando un profesional divulga información confidencial de un paciente o de un cliente. El *Defamation Tort* intenta reparar el daño causado cuando alguien hace manifestaciones falsas sobre una persona que puede llegar a dañarla. El *Infliction of Emotional Distress* es un *Tort* concebido para proteger a aquellas personas víctimas de una conducta abusiva de un tercero que les causa una “angustia emocional severa”. Este acoso puede producirse de manera intencionada o de forma imprudente. El *Common Law* también ofrece una protección basada en la *privacy* en el ámbito del derecho que regula las pruebas en el proceso (*evidence law*). Se trataría del privilegio de mantener el secreto de las comunicaciones entre abogado y cliente, el matrimonio, médico y paciente, psicólogo y paciente, etc. (Solove, Rotenberg, Schwartz, 2005, p. 31)

La protección que brinda el *Common Law* al derecho a la propiedad, según algunos autores (Westin, 1967; Murphy, 1996, pp. 2381-2417; Posner, 1981), también sería aplicable a la privacidad. Desde esta óptica los datos personales se consideran como una forma de propiedad. Si la información personal es entendida como una forma de propiedad mueble, el *tort of conversion*⁹ sería aplicable a aquellos que recopilan y usan datos personales de manera ilícita. Por último, las políticas de privacidad, así como las condiciones de uso que contengan cláusulas sobre privacidad, pueden ser consideradas de manera análoga a un contrato, cuyo cumplimiento puede ser reivindicado ante un tribunal.

7. RESTATEMENT (SECOND) OF TORTS § 652D (1977). The tort of disclosure allows civil liability when the defendant “gives publicity to a matter concerning the private life of another,” when the “matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.”

8. El concepto de “false light” debe entenderse como una revelación de algún asunto que resulta altamente ofensivo para una persona razonable. A través de la jurisprudencia se ha definido que se entiende por este concepto.

9. Según la definición del Legal Information Institute, “[C]onversion is an intentional tort which occurs when a party takes the chattel property of another with the intent to deprive them of it. Conversion is not applicable to real property. For the purposes of conversion, “intent” merely means the objective to possess the property or exert property rights over it. As a result, a party is liable for conversion regardless of their knowledge of property’s ownership status. For example, a person who picks up a necklace off the ground with the intent to resell it because they erroneously believed it was abandoned still converted that necklace. The standard remedy for conversion is return of the property in question or damages for the fair market value of the property.” Legal Information Institute, <https://www.law.cornell.edu/wex/conversion#:~:text=Conversion%20is%20an%20intentional%20tort,exert%20property%20rights%20over%20it>.

2.2. Las restricciones de la Primera Enmienda al derecho a la privacidad

La presión de activistas de la privacidad, de académicos, y de organizaciones de consumidores para que se establezca una regulación equivalente a la europea, aunque sea muy parcialmente, está empezando a dar sus frutos con la normativa californiana o el proyecto de ley federal sobre privacidad de datos (ADPPA). La respuesta de las grandes corporaciones tecnológicas ante estos “movimientos legislativos” es alegar la Primera Enmienda. Su principal argumentación jurídica se basa en considerar como invasiva cualquier regulación invocando a la libertad más central del sistema constitucional estadounidense, la “*freedom of speech*”. Eugene Volokh se ha alineado con estos razonamientos, afirmando que muchas leyes de privacidad que regulan la venta y divulgación de información personal son inconstitucionales bajo la Primera Enmienda (Volokh, 2000, pp. 1049-1124). Según este autor, “[T]he right to information privacy — my right to control your communication of personally identifiable information about me — is a right to have the government stop you from speaking about me.” (Volokh, 2000, pp. 1051). La afirmación parece muy radical, especialmente si tenemos en cuenta las amplias posibilidades de manipulación de la opinión de los usuarios que han mostrado tener las redes sociales en casos muy críticos para la democracia de los Estados Unidos como es el escándalo de Cambridge Analytica/Facebook.

En *Sorrell v. IMS Health Inc* el Tribunal Supremo de los Estados Unidos anuló la ley estatal de Vermont que tenía como objetivo limitar la comunicación y distribución de datos personales de los médicos. A este Estado de Nueva Inglaterra le preocupaba que las farmacias vendiesen información sobre recetas médicas a compañías de minería de datos, las cuales, a su vez, generaban informes sobre patrones de prescripción de medicamentos que ponían a disposición de las compañías farmacéuticas a cambio de elevadas sumas. La preocupación del gobierno estatal era que permitiendo a estas empresas hacer “*target advertising*” a los médicos se acabase ocasionando que estos prescribiesen los medicamentos más caros.

El Tribunal Supremo sostiene que la normativa aprobada por el Estado de Vermont es inconstitucional porque establece una restricción al acceso de la información y al discurso empleado con fines comerciales, basada en el contenido (*content-based*) y en la persona que emite el discurso (*speaker-based*). La opinión mayoritaria del Juez Kennedy señala que bajo las leyes de Vermont, los farmacéuticos pueden donar o vender esta información a terceros para finalidades científicas, periodísticas u otros propósitos.

El magistrado sostiene que la elaboración, venta y difusión de información personal en forma de datos puede requerir protección en tanto que discurso bajo la Primera Enmienda. No obstante, el juez Kennedy entiende que no es necesario entrar en el fondo del asunto, es decir, si la recopilación de datos estaba desprotegida. El derecho de Vermont, según la opinión de Kennedy, era discriminatorio en el modo en que las personas y las organizaciones pueden

usar datos personales en las comunicaciones basados en la protección de contenido y en la persona que emite el discurso (*content and speaker*). Las restricciones establecidas vulneraron la Primera Enmienda, incluso bajo el test utilizado para el discurso comercial. En este caso, estaría, según este autor, legitimado su uso, incluso la venta a terceros, y no podría establecerse ninguna restricción ya que sería inconstitucional (Balkin, 2016, pp. 1193 y 1194).

Se puede argumentar que los datos cuando son recopilados, explotados, usados y vendidos en masa no son discurso, sino más bien una *commodity*, como puede ser cualquier cereal o mineral para la industria. En *Sorrell* el juez Kennedy se muestra escéptico en entender que el formato en el cual se comunican los datos sea tan decisivo para determinar si estamos ante la protección de la Primera Enmienda. Balkin entiende que en lugar de centrarnos en la forma de la información como datos digitales, es necesario centrarse en la caracterización o la función social (Balkin, 2016, pp. 1193 y 1194). Este autor pone como ejemplo el caso Facebook, tras el caso de Cambridge Analytica bastante desafortunado; el uso de datos de los usuarios de la red social para incitarles a votar se entendería como discurso ideológico, por tanto, protegido por la Primera Enmienda.

Las regulaciones de privacidad deben ser “*content-neutral*” en relación con el tiempo, lugar y modo de expresión. Se entiende por contenido neutral aquellas leyes que se aplican a toda la expresión con independencia del fondo (*substance*) del mensaje. El Tribunal Supremo explica en *Ward v. Rock Against Racism* (1989) que “*the principal inquiry in determining content neutrality, in speech cases generally ... is whether the government has adopted a regulation of speech because of disagreement with the message it conveys.*” En definitiva, según está línea jurisprudencial, las normativas federales y estatales de protección de datos deberán respetar al principio de libertad de expresión de la Primera Enmienda protegiendo el dato personal como formato, siendo “*content neutral*” sin que haya ninguna determinación de su contenido.

El profesor Balkin, tal como se había señalado más arriba, aporta una solución jurídica para evitar esta tensión anti-regulatoria a la que denomina como una segunda “*Gilded Age*”. Entiende que es necesario regular para preservar los derechos y libertades de los ciudadanos ante las nuevas formas de poder económico y social, tal como se hizo en el momento histórico mencionado. No obstante, se plantea igualmente la imprescindible protección de la libertad de expresión de la Primera Enmienda. Esta otorga restricciones a la responsabilidad procedente del *Tort Law* por la revelación de información ya sea verdadera o falsa. Balkin utiliza el concepto *information fiduciary* como elemento clave para garantizar y proteger a los datos personales de los usuarios de la red (Balkin, 2016, p. 1186). El mismo se basa en que los proveedores de servicios en Internet que recopilan, analizan, usan, venden y distribuyen información personal deben ser considerados como *information fiduciaries* en relación a sus clientes y a los usuarios finales. El ostentar esta posición jurídica conlleva el deber de actuar de manera que no pueda dañar los intereses de las personas sobre las que está llevando a las acciones mencionadas.

El concepto es muy sugerente, ya que sitúa a estas empresas en una clara posición de responsabilidad, y puede conectarse con la idea de un *softlaw* preventivo a través de la autorregulación. No obstante, bajo mi punto de vista, deja muchas zonas de sombra que pueden comportar elevados riesgos. Por tanto, considero que si bien sería interesante incorporar en el derecho de la protección de datos este concepto de los *information fiduciaries*, debería hacerse con un claro marco regulatorio como ocurre en la Unión Europea. El caso Enron con la ley Sarbanes-Oxley de 2002 y su apuesta por elementos de control y auditoría financiera, así como la introducción del *Compliance*, en las empresas cotizadas sería un buen ejemplo.

2.3. El derecho a la privacidad en el derecho constitucional

La Constitución de los Estados Unidos no menciona expresamente a la privacidad, no obstante, a partir de la interpretación jurisprudencial¹⁰ se ha entendido que diversas enmiendas de la norma suprema protegen las diferentes tipologías del derecho a la privacidad. *Griswold v. Connecticut* fue la primera sentencia en la que reconoció el “derecho a la privacidad”. En *Griswold* el Tribunal Supremo sostiene que el derecho a la privacidad deriva de las penumbras de las protecciones procedentes de otros derechos constitucionales. El Tribunal usa la Primera, la Tercera, la Cuarta y la Novena enmienda para extraer esta protección. En la resolución del alto tribunal estadounidense se sostiene que cuando se juntan las zonas de penumbra, la Constitución acaba creando una “zona de privacidad”¹¹.

La Primera Enmienda, la cual hemos visto como límite al derecho a la privacidad, garantiza la libertad de pensamiento, de asociación y el derecho a mantener el anonimato¹². Se establece la salvaguarda de los ciudadanos de preservar la confidencialidad con relación a su pertenencia a un grupo u organización¹³, tal como estableció en *NAACP v. Alabama* (1958) y *Shelton v. Tucker* (1960), teniendo en cuenta que el derecho a la libertad de expresión tiene prevalencia frente a otros derechos como resulta en el supuesto de la privacidad.

La Tercera Enmienda, relativa a la imposibilidad de alojar soldados en las residencias particulares sin el previo consentimiento del propietario, también ha sido utilizada para proteger la privacidad (Martínez Martínez, 2004). En la salva-

10. *Vid.*, entre otras: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Shelton v. Tucker*, 364 U.S. 479 (1960); *Buckley v. Valeo*, 424 U.S. 1 (1976); *Fisher v. United States*, 425 U.S. 391 (1976).

11. *Vid. Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965).

12. *Vid. McIntyre v. Ohio Election Comm'n*, 514 U.S. 334 (1995).

13. La Primera Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: “El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios”.

guarda que introduce la interpretación actual de la Cuarta Enmienda¹⁴ ante registros arbitrarios (*unreasonable searches and seizures*)¹⁵ efectuados por las autoridades administrativas sin disponer previamente de la debida autorización judicial el tribunal también ha reconocido un derecho a la privacidad. Se considera que la garantía no ampara únicamente a los elementos materiales, sino que también comprende a los datos electrónicos o las grabaciones obtenidas en las vigilancias¹⁶. En *Olmstead v. United States*¹⁷ (1928) el Tribunal Supremo había sostenido que las escuchas telefónicas no suponían una invasión bajo la Cuarta Enmienda porque no implicaba una intrusión en el domicilio del afectado. Fue justamente Brandeis, entonces juez del Tribunal Supremo, el que manifestó su opinión en contra, argumentado que el interés central protegido por la Cuarta Enmienda no era la propiedad sino “*the right to be alone*”. En 1967 en *Katz v. United States* el alto tribunal estableció la interpretación moderna de la Cuarta Enmienda señalando que esta “*protects people, not places*”.

La Quinta Enmienda también ha recibido una interpretación para garantizar el derecho de la privacidad en lo relativo a la protección frente a la propia incriminación, así como sobre la protección frente a la facultad de las autoridades gubernamentales de forzar a los afectados a divulgar cierta información personal sobre ellos en contra de su propia voluntad¹⁸. La Novena Enmienda, posibilita la realización de una interpretación extensiva en favor de aplicar garantías jurídicas sobre la privacidad en todos aquellos supuestos no regulados específicamente en las ocho primeras enmiendas¹⁹.

14. La Cuarta Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: “El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas”.

15. *Vid.*, entre otras: *United States v. Miller*, 425 U.S. 435 (1976).

16. Las garantías jurídicas efectuadas por parte de la Cuarta Enmienda fueron extendidas inicialmente a las conversaciones telefónicas, *vid. Katz v. United States*, 389 U.S. 347 (1967), y posteriormente limitado en aquellos supuestos en que el afectado voluntariamente cedía su información personal a terceros, *vid. United States v. Miller*, 425 U.S. 435 (1976). En cualquier caso, en la actualidad, la protección de la Cuarta Enmienda también se ha extendido a las comunicaciones electrónicas, en virtud de la Ley Privacidad de las Comunicaciones Electrónicas de 1986. Consultado el 24.05.2022 desde: <https://it.ojp.gov/privacyliberty/authorities/statutes/1285>; así como a los registros de los datos de ubicación que se generan mediante el uso de los dispositivos móviles, *vid. Carpenter v. United States*, 585 U.S. 84 (2018). Adicionalmente, *vid.*, entre otras: *Olmstead v. United States*, 277 U.S. 438 (1928); *Goldman v. United States*, 316 U.S. 129 (1942); *Kyllo v. United States*, 533 U.S. 27 (2001).

17. En el presente caso, el Tribunal Supremo de los Estados Unidos consideró que la Cuarta Enmienda no resultaba de aplicación sobre las intervenciones telefónicas por no implicar intromisión en la propiedad privada del hogar. Posteriormente, el Congreso daría luz verde la Sección 605 de la *Federal Communications Act* de 1934, que protegía el contenido de dichas comunicaciones mediante previa autorización, así como imponiendo la obligación de no revelar a terceros el contenido de estas.

18. *Vid. Boyd v. United States*, 116 U.S. 616, 630 (1886); *Gouled v. United States*, 255 U.S. 298 (1921).

19. *Vid. Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965).

Por último, en el concepto de libertad sustantiva previsto en la cláusula del debido proceso legal (*due process of law*)²⁰ de la Decimocuarta Enmienda llamamos una interpretación de la *Information Privacy*. En la *concurring opinion* de *Griswold v. Connecticut* el juez Harlan estableció un derecho de la privacidad derivado de la mencionada enmienda. El juez del Supremo reprodujo su *dissenting opinion* de *Poe v. Ullman* (1961): “*I consider that this Connecticut legislation, as construed to apply to these appellants, violates the Fourteenth Amendment. I believe that a statute making it a criminal offense for married couples to use contraceptives is an intolerable and unjustifiable invasion of privacy in the conduct of the most intimate concerns of an individual's personal life.*” A partir del último tercio del siglo XX, la jurisprudencia menor²¹ ha tomado esta interpretación de la Catorceava Enmienda como fundamento para considerar que el derecho a la privacidad informativa (*informational privacy*)²² ostenta rango constitucional. Sin embargo, la totalidad de los Tribunales de Circuito no se han mostrado favorables a acoger el contenido de dicha interpretación²³, así como tampoco el Tribunal Supremo de los Estados Unidos se ha pronunciado sobre el alcance constitucional de este derecho, a pesar de las numerosas críticas que ha

20. La cláusula de la Decimocuarta Enmienda que garantiza que ningún Estado “privará a ninguna persona de vida, libertad o propiedad, sin el debido proceso legal”. El Tribunal Supremo de los Estados Unidos ha interpretado la cláusula del debido proceso para establecer la “incorporación selectiva” de enmiendas en los Estados, lo que significa que ni los Estados ni el propio gobierno federal pueden limitar los derechos individuales previstos por la Constitución mediante la promulgación de leyes estatales o federales. *Vid.*, entre otros: *Roe v. Wade*, 410 U.S. 113 (1973); *Whalen v. Roe*, 429 U.S. 589 (1977).

21. *Vid.*, entre otros: *Barry v. City of New York*, 712 F.2d 1554 (2d Cir. 1983); *Slayton v. Willingham*, 726 F.2d 631 (10th Cir. 1984).

22. Podemos referirnos al derecho a la privacidad informativa (*information privacy*) como aquella nueva vertiente del tradicional derecho a la privacidad desarrollado en Estados Unidos, que surge a tenor de un cambio en la jurisprudencia del Tribunal Supremo durante la década de 1960, como consecuencia de los tratamientos masivos que se realizan de información personal mediante el uso de las nuevas tecnologías desarrolladas bajo el acervo de internet. Su principal cometido radica en dotar a los afectados de las herramientas y los mecanismos necesarios que les permita disponer del control efectivo sobre sus datos personales, como parte integrante de una manifestación más del libre desarrollo de la personalidad contenido en el concepto de libertad sustantiva que se propugna en la cláusula del debido proceso establecida en la Decimocuarta Enmienda. *Vid.* Westin (1967), p. 7; Fried (1968), pp. 475-493; Cate (1997).

p. 22; pp. 1609-1701; Kang (1998), pp. 1193-1294; Schwartz (2000), pp. 815-859.

23. A este respecto, en palabras de Nieves Saldaña: “[t]odos los Tribunales de Circuito sostienen que el derecho a la *informational privacy* no es absoluto, ponderándose el interés individual en la protección de la información personal frente al interés estatal en la adquisición o divulgación de esa información, aunque difieren en cuanto a la relevancia que otorgan al interés estatal. Así, el Cuarto, Sexto y Décimo Circuitos aplican un examen judicial riguroso (*strict scrutiny*) a las invasiones estatales de la *informational privacy*, aunque el Sexto Circuito solo reconoce una violación de la información personal cuando afecta a derechos fundamentales, exigiendo demostrar un interés estatal esencial (*compelling state interest*) para invadir derechos fundamentales a través de la revelación de información personal, mientras que el Cuarto Circuito también aplica un escrutinio riguroso para evaluar la divulgación estatal de la información personal que no afecta a derechos fundamentales.” Saldaña Díaz (2011), p. 306.

recibido por parte del sector doctrinal (Flaherty 1991, pp. 831-855; Chlapowski, 1991, pp. 133-136; Turkington, 1990, pp. 496-503).

En *Whale v. Roe* (1977) el Tribunal amplió su protección a la privacidad sustantiva durante el proceso a la *information privacy*, sosteniendo que la zona de privacidad protegida por la constitución abarca el interés individual en evitar la divulgación de asuntos personales. Esta rama del derecho a la privacidad se conoce como el derecho constitucional a la privacidad de la información. En el amplio concepto de *privacy* hay que delimitar la *information privacy* que es la que se correspondería de manera más directa con el derecho fundamental a la protección de datos personales.

La “*information privacy*” está relacionada con la recopilación, uso, y revelación de información personal. Este concepto se diferencia de la “*decisional privacy*”, el cual se corresponde con la libertad que tienen las personas de tomar decisiones sobre su propio cuerpo o familia (Solove, Rotenberg, Schwartz, 2005, p. 1). La “*decisional privacy*” tiene relación con como la anticoncepción, la procreación, el aborto y la crianza de los hijos. La misma es el centro de una serie de casos del Tribunal Supremo de los Estados Unidos relacionados con el proceso debido o el derecho constitucional a la privacidad. La reciente sentencia de 24 de junio de 2022 en el caso *Dobbs v. Jackson Women's Health Organization*, estableciendo que la Constitución no confiere un derecho al aborto y, por tanto, anulando la histórica sentencia del caso *Roe v. Wade* que protegía la libertad de una mujer para abortar sin excesivas restricciones gubernamentales, ilustraría el uso de la “*decisional privacy*”. La “*information privacy*” cada vez incorpora más elementos de la “*decisional privacy*”, ya que el uso de datos afecta decisivamente a la autonomía individual.

2.4. Statutory Law y derecho a la privacidad

El rápido avance de las tecnologías de computación produjo un profundo debate sobre la privacidad desde mediados de los 60. La privacidad, en efecto, pasó a ser una preocupación central de la sociedad estadounidense. El Tribunal Supremo, tal como se ha señalado más arriba, emitió una serie de pronunciamientos que han sido referente en la construcción del derecho a la privacidad.

En 1973 se publicó un informe que tuvo un gran impacto e influencia por el *United States Department of Health, Education, and Welfare*. Este documento realizó una profunda revisión de cómo se estaban procesando los datos en Estados Unidos, y propuso un *Code of Fair Information Practices*²⁴. El código estableció unos principios básicos para el tratamiento de los datos personales, así como responsabilidades en la recopilación y uso de la información personal. En estos cabe destacar: a) la prohibición de mantener información personal de

24. U.S. Department of Health, Education, and Welfare, *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* (1973).

forma secreta, b) el establecimiento de un derecho de acceso a las bases de datos para que los individuos conozcan si contienen información personal suya, c) la existencia de procedimientos que prevengan que los datos personales son utilizados con una finalidad distinta a la que se había consentido, d) el desarrollo de una forma para rectificar la información que los identifica, d) la obligación en cualquier organización que cree, mantenga, use o difunda registros de datos personales identificables de garantizar la confiabilidad de los datos para el uso previsto, y de tomar precauciones razonables para evitar el uso indebido de los datos.

Como ha señalado Marc Rotenberg, (Rotenberg, 2001, pp. 26-39). las recomendaciones establecidas en este código de buenas prácticas constituyeron un decisivo marco para la legislación sobre información personal que se aprobó desde mediados de los 70 en los Estados Unidos. La legislación sobre privacidad de la información en los Estados Unidos de América no cuenta con una reglamentación general al estilo del RGPD europeo que se aplique a cualquier tratamiento de datos personales. Por el contrario, se efectúa a través de diversas normativas federales y estatales de carácter sectorial²⁵.

Entre las regulaciones que se promulgaron en la década de los 70, se puede destacar a la *Privacy Act*²⁶. Esta norma fue la primera ley federal que regulaba la recopilación, el mantenimiento, el uso y la difusión de la información personal almacenada por las distintas agencias federales norteamericanas sobre sus ciudadanos y terceros que pudieran resultar relevantes para los fines perseguidos. La *Freedom of Information Act*²⁷ (1966), por su parte, obligaba a facilitar a los ciudadanos la información y documentación que obre en sus respectivos archivos o expedientes, siempre medie el consentimiento previo del afectado o la divulgación se pueda efectuar por existir una habilitación normativa en virtud de las excepciones que contiene la norma.

El sistema liberal y antirregulatorio de las corporaciones, que se ha señalado, prefiere el uso de autorregulación (Schwartz, Solove, 2009; Solove, Rotenberg,

25. Se puede citar sin ánimos de exhaustividad: la *Right to Financial Privacy Act (RFPA)* de 1978; la *Financial Services Modernization Act* de 1999, habitualmente conocida como la *Gramm-Leach-Bliley Act (GLBA)* de 1999; la *Fair and Accurate Credit Transactions Act (FACTA)* de 2003; por lo que hace referencia a datos médicos, la *Health Insurance Portability and Accountability Act (HIPAA)* de 1996; y con una relativa mayor actualidad, en lo relativo a la privacidad genética, podríamos citar la *Genetic Information Nondiscrimination Act (GINA)* de 2008, así como la *California Consumer Privacy Act (CCPA)* de 2018 relativa a la protección de la información personal de los consumidores residentes en California. Haciendo énfasis igualmente en la protección de la información personal en las comunicaciones electrónicas, cabe citar, en especial, la *Cable Communication Policy Act (CCPA)* de 1984; la *Electronic Communications Privacy Act (ECPA)* de 1986; la *Telecommunications Act* de 1996; la *Children's On-line Privacy Protection Act (COPPA)* de 1998 y la *E-Government Act* de 2002.

26. Estados Unidos. *Privacy Act*, 5 U.S.C. § 552 a), *Section 2*. Promulgada del 31 de diciembre de 1974 por parte del Congreso de los Estados Unidos de América.

27. Estados Unidos. *Freedom of Information Act (FOIA)*, 5 U.S.C. § 552. Promulgada el 4 de julio de 1966 por parte del Congreso de los Estados Unidos de América.

Schwartz, 2005) a una intervención legislativa similar a la que se opera en el sector público. Al respecto, Arribas Luque señala que: “La irrupción de las nuevas tecnologías y la escasa protección legislativa de la *privacy* motivó la pérdida de la confianza del consumidor norteamericano y forzó la autoimposición empresarial, voluntaria y como táctica comercial, de normas de conducta limitativas del libre uso de los datos personales, en la creencia de que una política, debidamente difundida, de protección de la privacidad de las personas frente a la intromisión generalizada en aquella que caracterizaba a la competencia redundaría en una mayor captación de clientela y en mayores beneficios.” (Arribas Luque, 2002, pp. 1587-1599)

Más recientemente, en 2018 se aprobó la *California Consumer Privacy Act* (“CCPA”), esto hizo que California fuera uno de los primeros Estados en elaborar una regulación para la privacidad y protección de datos de los consumidores. El principal impulso de la norma fue el apoyo popular a la iniciativa con más de 600.000 firmas. En esta norma, junto a los derechos de acceso y supresión, destaca la apelación directa a las empresas a no vender información personal: “[A] consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt-out.”²⁸

El ámbito subjetivo de protección de la CCPA se restringe a los “consumidores”, en este sentido se puede señalar una de las principales diferencias con el régimen de la protección de datos de la Unión Europea, el cual como es sabido, afecta a todos los tratamientos de datos personales, sean públicos o privados, haya o no relación de consumo. En este sentido, vemos dos modelos de cultura jurídica, una que ha constituido un nuevo derecho fundamental, y la otra que prefiere adoptar la perspectiva del consumidor, del “ciudadano administrado”, o en algunos casos del paciente, o del menor.

Recientemente diversos Estados han seguido la senda de California y han aprobado leyes sobre protección datos. Las mismas, en efecto, siguen el modelo de la *California Consumer Privacy Act* CCPA, así como adoptan una definición del concepto de datos personal muy similar a la del Reglamento General de Protección de Datos (RGPD). No obstante, se debe insistir en que el ámbito de aplicación es únicamente consumo, que las causas de legitimación no se corresponden con el RGPD, y que hay muchas excepciones y salvades procedentes de otras normas de privacidad. En todo caso, las conocidas como “States Privacy Laws” son: la *Colorado Protect Personal Data Privacy Act* (ColoPA) de 7 de julio de 2021, que entrará en vigor en la misma fecha del 2023, la *Connecticut Privacy Act* (CTPA), de 10 de mayo de 2022, que entrará plenamente en vigor el 1 de julio de 2023; la *Virginia Consumer Data Protection Act* (VCDPA) de 2 de marzo de 2021 que entrará en vigor el 1 de enero de 2023; y la *Utah Consumer Privacy*

28. Art. 1798.120, letra a) de la California Consumer Privacy Act of 2018 [1798.100 — 1798.199.100] (*Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3*).

cy Act (UCPA) de 24 de marzo de 2022 que entrará en vigor el 31 de diciembre de 2023.

Para acabar este análisis se debe hacer referencia la mencionada iniciativa legislativa federal que está suscitando gran interés a ambos lados del Atlántico: la *American Data Privacy and Protection Act* (a partir de ahora ADPPA). Tras décadas de inactividad en el ámbito de la protección de datos se quiere establecer un “*federal privacy statute*”. Entre los aspectos más relevantes de este nuevo régimen jurídica estaría la “*data minimization*”. En este concepto hallamos una trasposición del principio recogido en el artículo 5 del RGPD, según el cual, los datos de personales serán “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”. Igualmente, introduce el principio de “limitación de la finalidad” de la norma europea. La compañía solo podrá recopilar datos si es necesario para alguno de los diecisiete propósitos permitidos en el proyecto de ley. Se puede destacar una sustancial diferencia entre este *numerus clausus* de finalidades permitidas, y el complejo sistema de causas de legitimación del RGPD²⁹, en el cual figuras como el “interés legítimo” han ganado relevancia ante el tradicional “consentimiento del afectado”.

La elaboración de la ADPPA está suscitando cuestiones competenciales entre el derecho federal y el estatal. Se está planteando si la futura legislación federal debería prevalecer sobre la legislación estatal, hecho que ha planteado la firme oposición de los Estados que han elaborado normativa y han constituido agencias de protección de datos. La creación de un “derecho de acción privado” que permita a las personas, no solo al gobierno, demandar a las empresas por violaciones es otros de los aspectos que está desatando mayor polémica en sede parlamentaria. Los demócratas generalmente están en contra de la preferencia del derecho federal y a favor de un derecho de acción privado, los republicanos lo contrario.

A buen seguro este nuevo régimen de la protección de datos no supondrá un cambio en la consideración de Estados Unidos como un país con un nivel no adecuado de protección, pues sigue manteniéndose la sectorización, y su ámbito de aplicación no afecta a la seguridad nacional, principal preocupación del Tribunal de Justicia de la Unión Europea como se analizará a continuación.

3. EL NUEVO DATA PRIVACY FRAMEWORK TRANSATLÁNTICO

Las transferencias de datos personales desde la Unión Europea hacia los Estado Unidos tienen un impacto muy significativo en las relaciones comerciales y en las inversiones entre las dos potencias económicas. Por otra parte, refuer-

29. Según el artículo 6 del RGPD son: a) consentimiento, b) relación contractual, c) Intereses vitales del interesado o de otras personas, d) cumplimiento de una obligación legal para el responsable, e) interés público o ejercicio de poderes públicos.

zan la comunicación on-line, sirven para monitorizar las cadenas mundiales de abastecimiento, establecen servicios transfronterizos y fomentan la innovación tecnológica, entre muchos otros aspectos. En el año 2020, el tráfico mercantil de los servicios de tecnologías de la información y la comunicación ascendió a 264 miles de millones, cifra que revela la enorme importancia de las relaciones transatlánticas. En este sentido, la obtención de una decisión de adecuación se convierte en un elemento crítico para el desarrollo de la economía digital entre ambas áreas. En los siguientes apartados se va a analizar sintéticamente la evolución de este régimen especial hasta llegar al marco actual, el *Data Privacy Framework*.

3.1. Antecedentes: Safe Harbor y Privacy Shield

Las diferentes concepciones sobre la privacidad y la protección de datos entre los Estados Unidos de América y la Unión Europea condujeron a la Comisión Europea a no considerar que el primero cuenta con un nivel adecuado de protección. Sin duda la diversidad y pluralidad del derecho a la privacidad que hemos visto en los apartados anteriores ha condicionado a que su régimen jurídico no sea homologado. Aunque las acciones de vigilancia masiva llevadas a cabo por parte de las agencias de inteligencia de los Estados Unidos, reguladas por la *Foreign Intelligence Surveillance Act* (FISA) de 1978 son las que marcaron el verdadero escollo para obtener la homologación.

Estas problemáticas se manifestaron durante la negociación del primer acuerdo de intercambio de datos entre ambos territorios, articulado a través de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, la *EU-US Safe Harbor Principles*. El órgano consultor en materia de protección de datos de la UE denominado “Grupo de trabajo del Artículo 29” (GT 29) denunció reiteradamente las carencias de las que adolecía. Las mismas se sustentaban esencialmente en las particularidades propias de la legislación interna de los Estados Unidos, basada en la prevalencia de la seguridad nacional frente a la protección de otros bienes jurídicos³⁰.

A la situación descrita se suma que las autoridades norteamericanas competentes no velaban por la aplicación de la propia Decisión. Se establecieron, además, una serie de excepciones que socavaban peligrosamente las garantías de los ciudadanos europeos. Las mismas se relacionaban con el cumplimiento de las exigencias de seguridad nacional, interés público y cumplimiento de la ley. En 2013 la Comisión Europea propone una serie de recomendaciones y propuestas para apaciguar las crecientes críticas al acuerdo con los Estados Unidos.

Las revelaciones de exagente de la NSA, Edward Snowden, no hicieron más que acrecentar las denuncias de vulneración masiva de los datos personales europeos. Una figura crucial en estas reivindicaciones fue el abogado y activista

30. Vid. Castellanos Rodríguez (2022).

austriaco Maximilian Schrems. En 2013, tal como se ha apuntado más arriba, presentó una denuncia contra Facebook Ireland Ltd en el *Irish Protection Commissioner*, ya que en este país están situados las oficinas centrales de la red social en Europa. En la misma se solicitaba que se prohibiese la transferencia de datos desde Irlanda a Estados Unidos alegando que Facebook USA estaba implicado en el programa de vigilancia masiva conocido como PRISM. La base jurídica de la petición se sustentaba en que la normativa de protección de datos de la Unión Europea no autorizaba la transferencia internacional de datos a países que no garantizasen “un adecuado nivel de protección”. Tras ser rechazada por la autoridad de protección de datos irlandesa, interpuso una demanda al *Irish High Court*. El tribunal planteó una cuestión prejudicial al Tribunal de Justicia de la Unión Europea (TJUE) en el cual se solicitaba la interpretación del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea que recoge el derecho a la protección de datos personales.

El 6 de octubre de 2015 el TJUE dictó una resolución que supuso un verdadero movimiento sísmico en las relaciones económicas digitales entre las dos potencias. Se determinó la invalidez de la Decisión (*Safe Harbor*) y se declaró la imposibilidad de efectuar transferencias internacionales a los Estados Unidos de América. En esta sentencia, conocida como *Schrems I*, el Alto Tribunal comunitario aprovechó para responsabilizar a la Comisión Europea de no haber efectuado las comprobaciones necesarias que hubieran permitido determinar con exactitud que los Estados Unidos no gozaban de un nivel de protección adecuado para ser el destinatario de los datos personales de ciudadanos de la Unión.

Como reacción a las revelaciones efectuadas por Snowden, el país norteamericano aprobó una serie de instrumentos normativos en los cuales supuestamente se trataba de garantizar que no se produjesen prácticas abusivas en materia de vigilancia y obtención de información por parte de las agencias de inteligencia norteamericanas. Tras más de dos años de negociaciones, el 16 de julio de 2016, se aprobó el segundo acuerdo de intercambio de datos entre la Unión Europea y los EE. UU., a través de la Decisión de Ejecución (UE) n° 2016/1250, de la Comisión Europea bautizado con un nombre muy significativo “*Privacy Shield*”. A pesar de que introdujo una serie de novedades en virtud de los mandamientos contenidos en el pronunciamiento del TJUE, las mismas no resultaron suficientes. En idénticos términos que le había sucedido a su antecesor, desde un primer momento fue objeto de críticas por parte de distintos organismos comunitarios —como el GT29, el Supervisor Europeo de Protección de Datos y el propio Parlamento Europeo— motivadas precisamente por las deficientes garantías que se establecían en su contenido respecto la protección de los derechos y libertades de los afectados situados en la Unión.

Dichas deficiencias serían sucesivamente puestas de manifiesto en las distintas revisiones que se efectuaban sobre la eficacia del acuerdo por parte del GT29 o la propia Comisión, entre otros organismos comunitarios. La situación se sustanciará nuevamente con la invalidación del acuerdo *Privacy Shield* por el TJUE en la sentencia *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (C-311/18) conocida como *Schrems II*. Entre las diversas cues-

ciones que fundamentaran el pronunciamiento por parte del TJUE, se puede encontrar la ausencia de límites tangibles que impusieran restricciones a las actuaciones realizadas por las agencias de inteligencia norteamericanas bajo el mandato de la Sección 702 de la FISA³¹, así como la inexistencia de garantías específicas que pusieran de manifiesto la efectividad e independencia de la figura del Defensor del Pueblo respecto al poder ejecutivo³².

El caso *Schrems II* pone de manifiesto nuevamente las vulneraciones a la privacidad y protección de datos de los usuarios europeos de Facebook causadas por la revelación masiva de los mismos a la *National Security Agency* (NSA) y al *Federal Bureau of Investigation* (FBI) para la lucha contra el terrorismo. La compañía de Mark Zuckerberg, además de este asunto, amparado dudosamente en la seguridad nacional, ha protagonizado en la última década numerosos escándalos relacionados con la cesión ilegal de datos personales. En julio de 2019 marcó un hito, le fue impuesta por la *Federal Trade Commission* (FTC en adelante) la multa más elevada de la historia, no sólo en Estados Unidos sino también en el resto del planeta³³. La FTC sancionó a la red social con 5.000 millones de dólares, así como muy elevados requerimientos para impulsar la “*accountability*” y la transparencia³⁴, por la venta indiscriminada y sin ninguna legitimación de millones de datos personales de sus usuarios³⁵. El caso *Facebook-Cambridge Analytica* constituye otra muestra del enorme riesgo del tratamiento ilícito de datos no solo para los derechos y libertades fundamentales de los ciudadanos europeos o americanos sino para el núcleo mismo de la demo-

31. *Vid.* Apartados 291, 292 y 297 de las conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18.

32. *Ibidem*, apdo. 337.

33. La multa monetaria fue casi diez veces superior a la punición de 575 millones de dólares impuesta a Equifax por la FTC y por el *Consumer Financial Protection Bureau* (CFPB) por una violación de seguridad en sus datos. “Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach”, nota de prensa de la FTC, <https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related>. (Recuperado el 11 de agosto de 2019).

34. Véase “FTC Approves Final Settlement With Facebook. Facebook Must Obtain Consumers’ Consent Before Sharing Their Information Beyond Established Privacy Settings”, nota de prensa de la FTC, 10 de agosto de 2012, <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook> (Recuperado el 11 de agosto de 2019).

35. La resolución se basa en la Sección 5 (a) y (l) y 16 (a) (l) de la *Federal Trade Commission Act* (“FTC Act”), 15 U.S.C., 45 (a) y (l) y 56 (a) (l), por las violaciones de la orden de 2012 de la FTC por las violaciones de la Section 5 (a) de la FTC. Véase “COMMISSION ORDER” In Re Facebook Inc., C-4365, 2012 FTC LEXIS 135 (F.T.C. 2012) (Decision and Order). La sanción se basó en la vulneración de los requerimientos que habían sido impuestos a Facebook en la Orden de la FTC de 2012. Esta sanción estaba motivada en el engaño a los usuarios sobre su capacidad de controlar la privacidad de su información personal. El acuerdo, igualmente, imponía nuevas restricciones a las operaciones de negocio de Facebook y crea múltiples canales de “*Compliance*”. La orden requiere a la compañía reestructurar su aproximación a la privacidad desde el nivel de dirección de la compañía (Corporate Board) hacía abajo. Se impone, por tanto, una nueva estructura de privacidad a Facebook y nuevas herramientas a la FTC para monitorear su actividad.

cracia³⁶. Supuso la recopilación de millones de datos de usuarios de la red social sin su consentimiento con fines de propaganda política en la campaña presidencial de Trump en el 2016 o en el referéndum del Brexit del mismo año.

Estos oscuros affaires, que tienen el común denominador del mayor conglomerado de redes sociales del mundo, revelan la enorme tensión que están sufriendo los mecanismos de garantías de derechos y libertades en los principales sistemas jurídicos del ámbito occidental. Grandes cantidades de información usadas por los gobiernos y por las empresas. Los afectados en el primer caso son los ciudadanos, y en el segundo los consumidores.

Por último, el pasado 25 de marzo 2022 la Unión Europea y los Estados Unidos realizaron un anuncio conjunto de una importancia trascendental: la tramitación de un nuevo acuerdo sobre el régimen legal de las transferencias de datos personales entre ambos territorios, al cual se denominó *Trans-Atlantic Data Privacy Framework*³⁷. Este marco jurídico pretende dar respuesta a las graves problemáticas señaladas por el Tribunal de Justicia de la Unión Europea a *Schrems II*. Sin embargo, todo apunta a que el nuevo acuerdo no será más que un ejercicio de maquillaje, pues Estados Unidos no va a modificar ni un ápice su política de seguridad nacional, y las nuevas iniciativas legislativas, muy orientadas al ámbito de consumo, no alteraran la consabida fragmentación del régimen jurídico de la protección de datos.

3.2. EU-US Data Privacy Framework

El 10 de julio de 2023, tal como se ha señalado, la Comisión Europea aprobó la decisión de adecuación para posibilitar la transferencia de datos personales entre entidades de la Unión Europea y de los Estados Unidos bajo el denominado *EU-US Data Privacy Framework*³⁸. El sistema se compone de tres partes: la decisión de adecuación del “Marco de Privacidad de Datos UE-EEUU” de la Comisión Europea, los “Principios del Marco de Privacidad de Datos UE-EE.UU.” del Departamento de Comercio de EE.UU., y otros documentos complementarios del lado estadounidense para el marco, incluida la Orden Ejecutiva 14086 que se examinará más adelante.

El DPF se basa en un sistema de certificación, que debe renovarse anualmente, mediante el cual las organizaciones estadounidenses³⁹ se comprometen a respetar un conjunto de principios de privacidad. En este sentido, el DPF toma

36. Véase sobre la manipulación digital de elecciones a Zittrain (2014).

37. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 (Consultado)

38. Las normas sobre transferencias de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones se establecen en el capítulo V del RGPD.

39. Para que una organización puede acogerse al DPF debe estar sujeta a los poderes de investigación de la *Federal Trade Commission* (FTC) o del Departamento de Transporte.

como base el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), así como los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. La decisión, por otra parte, recoge los principios establecidos en el artículo 5 del RGPD⁴⁰. Estos exigen un tratamiento lícito, leal, transparente, limitado a la finalidad y al tiempo por los cuales se recogieron. Asimismo, establece obligaciones con relación a la exactitud, minimización y seguridad de la información (confidencialidad, integridad y disponibilidad).

Cuando una organización haya decidido certificarse voluntariamente según el DPF el cumplimiento efectivo de los principios es obligatorio y exigible. Estas deberán tomar las medidas para verificar que sus políticas de privacidad se ajustan a los principios y a que se cumplan, así como deberán implementar estos principios en su política de privacidad. En este sentido, la decisión aboga por los mecanismos de autoevaluación, las auditorías tanto internas como externas, así como por la capacitación de los empleados.

El DPF acoge la definición de dato personal del RGPD, como “datos sobre un individuo identificado o identificable recibidos por una organización en los Estados Unidos desde la UE registrados por cualquier medio”. La aplicación de concepto de protección de datos del reglamento europeo implica que también se extienda a los datos pseudonimizados, incluso cuando la organización norteamericana receptora no tenga acceso a la clave de decodificación. Del mismo modo, se trasladan las salvaguardas para las categorías especiales de datos establecidas en el RGPD, es decir, datos personales que especifican condiciones médicas o de salud, origen racial o étnico, opiniones políticas, creencias religio-

40. Artículo 5 del RGPD,

Principios relativos al tratamiento

1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

sas o filosóficas, afiliación sindical, información sobre la vida sexual del individuo o cualquier información recibida de un tercero que sea identificada por esta como sensible. De manera similar, la noción de procesamiento se define como “cualquier operación o conjunto de operaciones que se realiza sobre datos personales, ya sea por medios automatizados o no, tales como recolección, registro, organización, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación o difusión y supresión o destrucción.”⁴¹

Los interesados deben tener determinados derechos que puedan oponerse al responsable o al encargado del tratamiento, en particular el derecho de acceso a los datos, el derecho a oponerse al tratamiento y el derecho a que los datos sean rectificados y suprimidos. Estos son los conocidos como derechos ARCO plus por la normativa europea y suponen el núcleo del *habeas data*, es decir, el derecho de los interesados a contar con mecanismos e instrumentos para ejercer un control efectivo de sus datos personales.

El considerando 35 de la decisión de adecuación hace referencia a diversas normas que pueden ofrecer un nivel de protección similar en la “improbable situación” (en palabras del considerando), de que las decisiones automatizadas fueran adoptadas por la propia organización. En cualquier caso, en aquellos ámbitos donde las empresas probablemente recurran al procesamiento automatizado de datos personales para tomar decisiones que afectan a los individuos (por ejemplo, préstamos de crédito, ofertas hipotecarias, empleo, vivienda y seguros), la legislación estadounidense proporciona protecciones específicas contra decisiones adversas. Estas leyes generalmente establecen que las personas tienen derecho a ser informadas de los motivos específicos que fundamentan la decisión (como el rechazo de un crédito), a cuestionar la información incompleta o inexacta (así como la dependencia de factores ilícitos) y a buscar reparación.

En el ámbito del crédito al consumo, la Ley de Informes Crediticios Justos (FCRA) y la Ley de Igualdad de Oportunidades Crediticias (ECOA) contienen salvaguardias que otorgan a los consumidores el derecho a una explicación y la posibilidad de impugnar la decisión. Estas leyes son relevantes en una amplia gama de contextos, incluyendo el crédito, el empleo, la vivienda y los seguros. Además, ciertas leyes contra la discriminación, como el Título VII de la Ley de Derechos Civiles y la Ley de Vivienda Justa, proporcionan protección a las personas frente a los modelos utilizados en la toma de decisiones automatizadas que podrían conducir a la discriminación basada en determinadas características, y les otorgan derechos para impugnar tales decisiones, incluidas las automatizadas.

En relación con la información de salud, la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) establece que cualquier decisión basada en el procesamiento automatizado normalmente será tomada por el responsable de tratamiento en la Unión Europea, que es quien tiene una relación directa con el

41. (Anexo I, apartado I.8.b).

interesado y, por ende, está directamente sujeto al Reglamento (UE) 2016/679. Esto incluye escenarios de transferencia en los que el procesamiento es llevado a cabo por un operador comercial extranjero (por ejemplo, en Estados Unidos) que actúa como agente (encargado de tratamiento) en nombre del responsable del tratamiento en la Unión Europea (o como subencargado que actúa en nombre del encargado del tratamiento en la Unión Europea que recibió los datos de un responsable del tratamiento en la Unión Europea que los recopiló) y, sobre esta base, toma la decisión. La regla de privacidad de la HIPAA crea ciertos derechos que son análogos a los establecidos en el Reglamento (UE) 2016/679 en cuanto al acceso a la información de salud personal. Asimismo, la orientación de las autoridades estadounidenses exige que los proveedores médicos reciban información precisa y completa.

Por último, se debe señalar que el Departamento de Comercio es el encargado de supervisar de forma continua el cumplimiento efectivo de los principios por parte de las organizaciones adheridas al DPF. En este sentido, llevará a cabo diversas acciones tales como verificaciones aleatorias de las organizaciones seleccionadas, supervisión de aquellas en las que se identifiquen problemas de cumplimiento para verificar posibles quejas o solicitudes de los interesados, o revisar la política de privacidad. Si hay elementos probatorios suficientes el Departamento de Comercio envía un cuestionario al cual si no se responde se podrán tomar posibles acciones coercitivas. Para garantizar en la práctica un nivel adecuado de protección existirán autoridades de control independientes con competencias para controlar y hacer cumplir las normas de protección de datos. En este sentido, es necesario que las organizaciones estadounidenses que se quieran acoger al DPF se hallen bajo la jurisdicción de la *Federal Trade Commission* o del Departamento de Comercio.

3.3. La Orden Ejecutiva 14086 “Enhancing Safeguards in United States Signals Intelligence Activities”

La Orden Ejecutiva 14086 “*Enhancing Safeguards in United States Signals Intelligence Activities*” de 7 de octubre de 2022 estableció un nuevo proceso para que las personas puedan buscar reparación con respecto a presuntas violaciones de la ley en relación con actividades de inteligencia de señales⁴² que afecten a sus datos transferidos desde un “Estado calificado” (todos los miembros de la UE lo son) a los Estados Unidos. La normal presidencial creó una figura de garantía jurisdiccional, el denominado, Tribunal de Revisión de Protec-

42. Inteligencia de señales (en inglés: signals intelligence; SIGINT) es la forma de recopilación de información, inteligencia militar, mediante la interceptación de señales, bien a partir de comunicaciones directas entre personas (inteligencia de comunicaciones; en inglés: communications intelligence, COMINT), bien de distintos medios electrónicos que no sirven para las comunicaciones directas (inteligencia electrónica; en inglés: electronic intelligence, ELINT), o bien una combinación de ambos.

ción de Datos (DPRC, por sus siglas en inglés). Esta novedosa institución forma parte de un nuevo proceso de revisión independiente e imparcial en dos niveles de las denuncias presentadas por ciudadanos de países considerados como “Estados calificados”, entre los que se encuentran todos los Estados miembros de la UE. La denuncia debe estar basada en una vulneración de los datos personales por Inteligencia de señales (SIGINT).

La función principal del DPRC es revisar las decisiones del Oficial de Protección de Libertades Civiles de la Oficina del director de Inteligencia Nacional (CLPO) con respecto a las denuncias presentadas por individuos en países u organizaciones regionales de integración económica que el Fiscal General de EEUU ha designado como “estados calificados” bajo la Orden Ejecutiva 14086. Para utilizar el proceso de reparación del DPRC, los individuos deben pasar por el primer nivel del mecanismo de reparación, el mecanismo de reparación del CLPO.

Los ciudadanos de la UE, en tanto que nacionales de Estados calificados, pueden presentar sus quejas ante sus autoridades de control, alegando que Estados Unidos violó su propia ley de inteligencia al recolectar o manejar sus datos a través de actividades de inteligencia de señales. Tras las verificaciones pertinentes la autoridad de control remitirá la denuncia al CLPO. Esta figura revisa que la denuncia cumpla con los requisitos, investigará el caso y dictará una resolución. Si el denunciante no está conforme con la decisión podrá solicitar la revisión por parte del DPRC, el cual revisará la decisión del CLPO y podrá solicitar información adicional con el fin de averiguar si se produjo una vulneración, y en caso afirmativo, establecería la indemnización o las medidas oportunas para compensar el daño.

Los cambios introducidos por la EO 14086 han incrementado las garantías y salvaguardas por las actividades de inteligencia de señales en relación con PPD-28, el cual fue parcialmente revocado por National Security Memorandum de 7 de octubre de 2022. En particular se establece la obligatoriedad de emplear criterios de “necesidad” y “proporcionalidad” para el uso de SIGINT. Por otra parte, se limita la recopilación masiva de inteligencia de señales en tres modos: 1) la información necesaria no puede ser “razonablemente” adquirida por una recopilación dirigida, 2) los datos recopilados se deben circunscribir a los necesarios, 3) debe cumplirse con al menos uno de los seis objetivos establecidos en la norma. A pesar de estos avances, la norma puede vulnerar los principios del RGPD y con la jurisprudencia del TJUE.

Los conceptos de necesidad y proporcionalidad no son interpretados a la luz de la tradición europea, con lo cual las prioridades de inteligencia de los Estados Unidos no pueden ser aceptadas desde el punto de vista de la protección de datos y el derecho a la intimidad de la UE. En cuanto al concepto de “proporcionado” reproduciendo las palabras de Schrems:

“The EU and the US now agree on the use of the word ‘proportionate’ but seem to disagree on the meaning of it. In the end, the CJEU’s definition will prevail — likely killing any EU decision again. The European Commission is

turning a blind eye on US law again and allowing the continued surveillance of Europeans.”

En conclusión, se puede afirmar que las salvaguardas introducidas por el DPF son insuficientes para cumplir con el estándar europeo de protección de datos e intimidad, lo cual nos sitúa ante más que una probable Sentencia Schrems III.

3. CONCLUSIONES

La comparación es el ejercicio de encontrar las diferencias entre dos culturas jurídicas o dos sistemas jurídicos para hallar el mejor modelo, o al menos extraer lecciones aplicables al derecho propio. En el ámbito de la privacidad y la protección de datos está premisa de la ciencia comparatística se convierte en una necesidad acuciante ante los retos y las amenazas que plantea el “capitalismo vigilante” de Zuboff o la cosificación que sufre el individuo “dataficado” descrito por Han. Si atendemos a la posición hegemónica y monopolística de los grandes proveedores de servicios estadounidenses la protección que ofrece el derecho de la Unión Europea a sus ciudadanos sufre una preocupante merma. El afán regulatorio del gigante europeo trata de equilibrar el inmenso poder del club de grandes corporaciones conocido como GAFAM.

La aprobación del Reglamento General de Protección de Datos en 2016 fue un notable avance, más bien una “actualización”, dicho en términos informáticos. A pesar del enorme impacto mundial de la legislación europea de protección de datos, que se está convirtiendo en estándar internacional, desde la fecha de su aprobación no han dejado de sucederse los escándalos, las vulneraciones masivas de la protección de datos de los europeos por parte de las grandes corporaciones tecnológicas, y lo que es más grave del propio gobierno de los Estados Unidos. Esta situación está tensionando las relaciones económicas entre las dos potencias, ya que la UE está poniendo grandes trabas jurídicas a las transferencias internacionales de datos a EEUU.

Este desencuentro no es nuevo, la UE nunca ha considerado que los EEUU tienen un nivel adecuado de protección de los datos personales. Resulta curioso que el país que “inventó” un derecho personalísimo para proteger la dignidad de sus ciudadanos ante el avance las tecnologías a finales del siglo XIX, y que en la década de los 70 fue pionero en regular el uso de los datos de los ciudadanos por las agencias gubernamentales, no reciba tal consideración. Todavía más, si observamos que estos logros son indiscutiblemente el origen también de la privacidad y protección de datos en Europa. Estamos ante un interesante caso de trasplante jurídico de instituciones que en la tierra nueva echa raíces más profundas y da muchos más frutos.

Se puede concluir que hay una diferencia muy sustancial entre ambas culturas jurídicas que imposibilitan esta homologación. Es cierto que en Estados Unidos hay una protección jurisdiccional enorme a través del derecho de *torts* del *Common Law*, que empequeñece al sistema de responsabilidad civil por

vulneración de protección de datos europeo. La fuerza disuasoria que tiene para las empresas en los EEUU la posibilidad de ser demandados por cantidades millonarias ha abierto tradicionalmente la puerta a una autorregulación. Por otra parte, el dinamismo y ductilidad del derecho creado por los jueces es una característica sumamente útil y eficiente cuando estamos ante fenómenos como la vertiginosa transformación digital.

No obstante, son los propios jueces los que han anulado en muchas ocasiones legislaciones de protección de datos por entender que vulneraban la libertad de expresión de la Primera Enmienda. Los recelos antirregulatorios no son solo de los jueces, sino también de un importante sector doctrinal, y estudiando la privacidad y el impacto del artículo de Warren y Brandeis, se antoja innecesario subrayar la importancia que tiene en Estados Unidos el sector académico. En cuanto a las empresas, sería una obviedad señalar que no desean ser reguladas. Desde la concepción de la libertad de expresión de la Unión Europea resulta totalmente incomprensible este “balance” entre los derechos, en el cual sale perdiendo la protección de datos.

En el derecho constitucional americano la privacidad está muy desarrollada, aunque no hay una mención expresa, el Tribunal Supremo ha interpretado su existencia en un total de cinco enmiendas de su Constitución. Esto ha convertido a la privacidad en un elemento central de su sistema constitucional de garantías, creando figuras como la “*decisional privacy*”, clave en el derecho al aborto, que no encuentran un equivalente en el derecho europeo. Sin embargo, ha originado una gran fragmentación del derecho a la privacidad, y consecuentemente a la “*information privacy*”, que puede redundar en un debilitamiento del mismo.

El régimen general y abstracto europeo rechazado desde el *Common Law* y desde los sectores más libertarios de la academia americana, seduce muy notablemente al gobierno federal, y a muchos gobiernos estatales. Además, cuenta con firmes defensores entre los activistas de la privacidad. El Estado de California está a la cabeza de este movimiento, seguido de Colorado, Connecticut, Virginia y Utah. A estas leyes estatales se suma el proyecto federal de una ley de protección de datos. No obstante, estas normas están orientadas al ámbito de consumo, y a pesar de algunas similitudes con el RGPD, cuentan con sustanciales diferencias en las causas de legitimación, las obligaciones a las empresas, etc. Tampoco es descabellado que puedan sufrir algún importante recorte por parte del Tribunal Supremo por colisionar con otros derechos constitucionales. Sin olvidar que no se aplican a ámbitos como la seguridad nacional que el tema más conflictivo en las relaciones entre EEUU y la UE.

Por otra parte, los cambios introducidos por la Orden Ejecutiva 14086 (EO 14086) han incrementado las garantías y salvaguardas en las actividades de inteligencia de señales, especialmente en relación con la Directiva Presidencial de Política-28 (PPD-28), que fue parcialmente revocada por el Memorándum de Seguridad Nacional del 7 de octubre de 2022. La EO 14086 establece la obligatoriedad de emplear criterios de “necesidad” y “proporcionalidad” para el uso de inteligencia de señales (SIGINT). Además, limita la recopilación masiva de inte-

ligencia de señales a través de tres modos específicos: primero, cuando la información necesaria no puede ser “razonablemente” adquirida por una recopilación dirigida; segundo, los datos recopilados deben restringirse a lo necesario; y tercero, debe cumplirse al menos uno de los seis objetivos establecidos en la norma.

A pesar de estos avances, se observan importantes discrepancias con los principios del Reglamento General de Protección de Datos (RGPD) y la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE). Los conceptos de necesidad y proporcionalidad no son interpretados según la tradición europea, lo que significa que las prioridades de inteligencia de los Estados Unidos no pueden ser aceptadas desde el punto de vista de la protección de datos y el derecho a la intimidad de la UE. Mientras que la UE y los EE.UU. están de acuerdo en el uso de la palabra “proporcional”, parece que no concuerdan en su significado real. Al final, es probable que prevalezca la definición del TJUE, lo que podría llevar nuevamente a la anulación de cualquier decisión de la UE en este ámbito.

La Comisión Europea, en su intento de encontrar un equilibrio, parece ignorar las diferencias fundamentales en la interpretación de la legislación estadounidense, permitiendo así la continua vigilancia de los ciudadanos europeos. Esto representa una situación delicada y crítica, pues las salvaguardas introducidas por el Data Privacy Framework (DPF) resultan insuficientes para cumplir con el estándar europeo de protección de datos e intimidad.

En resumen, las modificaciones establecidas por el DPF y la EO 14086, aunque representan un avance, no logran alinearse completamente con los requisitos europeos de protección de datos. La falta de una interpretación compartida de conceptos clave como “necesidad” y “proporcionalidad” crea una discordancia significativa entre ambos sistemas legales. La aparente condescendencia de la Comisión Europea frente a las prácticas estadounidenses pone en riesgo la privacidad de los ciudadanos europeos y abre la puerta a futuras disputas judiciales, siendo muy probable que se emita una Sentencia Schrems III. Esta sentencia, como sus predecesoras, podría invalidar nuevamente los acuerdos de transferencia de datos entre la UE y los EE.UU., subrayando la necesidad de un marco más robusto y armonizado que garantice efectivamente la protección de los datos personales en el contexto transatlántico.

BIBLIOGRAFÍA

- ARENAS RAMIRO, M. (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Ed. Tirant lo Blanch.
- ARRIBAS LUQUE, J. M. (2002), “Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE. UU.: El sistema de principios de Puerto Seguro”, en *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, pp. 1587-1599.

- ARZOZ SANTIESTEBAN, X. (2009), “Artículo 8: derecho al respeto de la vida privada y familiar”, en *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Navarra: Ed. Thomson-Reuters (Civitas).
- BALKIN, J. M. (2004), “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society”, *New York University Law Review*, 79, pp. 1-55.
- (2016), “Information Fiduciaries and the First Amendment”, en *UC Davies Law Review*, 49, pp. 1183-1234.
- BARRON, J. H. (1979), “Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation”, 13 *Suffolk Law Review*, pp. 875-922.
- BLOUSTEIN, E. J. (1964), “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser”, *New York University Law Review*, pp. 962-1007.
- BRADFORD, A. (2019), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press.
- BRAGE CAMEZANO, J. (2005), “Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos”, en *Revista Española de Derecho Constitucional*, n.º 74, pp. 111-137.
- CASTELLANOS RODRÍGUEZ, A. (2022), *Deconstruyendo las transferencias internacionales de datos personales*, Cizur Menor, Thomson Reuters-Aranzadi.
- CATE, F. H. (1997), *Privacy in the Information Age*, Washington, Ed. Brookings Institution Press.
- CHLAPOWSKI, F. S. (1991), “The Constitutional Right to Informational Privacy”, en *Boston University Law Review*, n.º 71, pp. 133-136.
- CHUECA SANCHO, A. G. (2004), “Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos”, en *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Madrid: Ed. Dykinson, pp. 37-58.
- COOLEY, T. C. (1888), *Law of Torts*, Chicago, Callaghan & Co.
- DAVARA RODRÍGUEZ, A. (1988), *La protección de datos en Europa*, Madrid, Ed. Grupo ASNEF-Equifax / Universidad Pontificia de Comillas.
- FLAHERTY, D. H. (1991), “On the Utility of Constitutional Rights to Privacy and Data Protection”, en *Case Western Reserve Law Review*, nº 41, pp. 831-855.
- FORBATH, W. E. (1985), “The Ambiguities of Free Labor: Labor and the Law in the Gilded Age”, *Wisconsin Law Review*, pp. 767-817.
- FRIED, C. (1968), “Privacy”, en *The Yale Law Journal*, n.º 77, pp. 475-493.
- GARZÓN, G. (1981), “La protección de datos y la función formativa del Consejo de Europa”, *Revista de Instituciones Europeas*, vol. 8, núm. 1, pp. 9-25.
- GROSSI, P. (1996). “Absolutismo jurídico y derecho privado en el siglo XIX”, en *Derecho & Sociedad*, n.º 11, pp. 94-99.
- HAN, B.-C., (2014), *Psicopolítica, Neoliberalismo y nuevas técnicas de poder* Barcelona., Herder.
- HORNUNG, G., SCHNABEL, C. (2009), “Data protection in Germany I: The population census decision and the right to informational self-determination”, en *Computer Law & Security Review*, 25, pp. 84-88.

- KALVEN, H. Jr. (1966), "Privacy in Tort Law – Were Warren and Brandeis Wrong?", n.º 31, *Law & Contemporary Problems*, pp. 326-341.
- KANG, J. (1998) "Information Privacy in Cyberspace Transactions", en *Stanford Law Review*, 50, pp. 1193-1294.
- KAISER, B. (2019) *La dictadura de los datos. La verdadera historia desde dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia, y cómo puede volver a pasar*, Madrid, HarperCollins.
- LES BENEDICT, M. (1985), "Laissez-Faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-Faire Constitutionalism", 3 *Law & History Review*, pp. 293-331.
- LESSIG, LAWRENCE (1999), *Code and Other Laws of Cyberspace*, New York, Basic Books.
- LUCAS MURILLO DE LA CUEVA, P. (1993), "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid, Ed. Fundación Colóquio Jurídico Europeo, pp. 81-179.
- MARTÍNEZ MARTÍNEZ, R. (2004), *Una aproximación crítica a la autodeterminación informativa*, Madrid, Ed. Civitas.
- MANSON, A. (1946), *Brandeis: a Free Man's Life*, New York, Viking.
- MURPHY, R. S. (1996), *Property Rights in Personal Information: An Economic Defense of Privacy*, 84, *Georgia Law Journal*, 84, 2381-2417.
- POSNER, R. A. (1981), *The Economics of Justice*, Harvard University Press.
- POST, R. C. (1989), "The Social Foundations of Privacy: Community and Self in Common Law Tort", en *California Law Review*, 77, pp. 957-1010.
- PROSSER, W. (1960), "Privacy", en *Californian Law Review*, 48, pp. 383-423.
- ROIG BATALLA, A. (2020), *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*, Barcelona, Bosch Editor.
- ROTENBERG, M. (2001), "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)", *Stanford Technology Law Review*, pp. 26-39.
- RUÍZ MIGUEL, C. (1944), *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos*, Pamplona, Thomson — Reuters (Civitas).
- SALDAÑA DÍAZ, M. N. (2011), "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego", en *Teoría y Realidad Constitucional*, Universidad Nacional de Educación a Distancia (UNED), n.º 28 (2011), Madrid, pp. 279-312.
- (2012), "«The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario de Warren y Brandeis", *Revista de Derecho Político*, n.º 85, pp. 195-240.
- SCHWARTZ P. M. (1999), "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, pp. 1609-1701.

- (2000), “Internet Privacy and the State”, en *Connecticut Law Review*, pp. 815-859.
- SCHWARTZ, P. M. y Solove, D. J., (2009), *Information Privacy: Statutes and Regulations 2010-2011*, New York, Ed. Wolters Kluwer (Aspen Publishing Co.).
- SOLOVE, D. J., ROTENBERG, M., SCHWARTZ, P. M. (2005), *Information Privacy Law (Second Edition)*, New York, Aspen.
- TURKINGTON, R. C. (1990), “Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy”, en *Northern Illinois University Law Review*, n.º 10, pp. 496-503.
- VOLOKH, E. (2000), “Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You”, en *Stanford Law Review*, 52, pp. 1049-1124.
- WARREN, S., Brandeis, L. (1890), “The Right to Privacy”, *Harvard Law Review*, 4, n.º 5, pp. 193-220.
- WESTIN, A. F. (1967), *Privacy and Freedom*, New York, Athenum.
- ZIMMERMAN, D. (1983), “L. Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort”, 68, *Cornell Law Review*, pp. 291-367.
- ZITTRAIN, J. (2014), “Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy”, 127 *Harvard Law Review Forum*, 335 Disponible en www.harvardlawreview.org/2014/06/engineering-an-election/ (Consultado el 5-09-2022).
- ZUBOFF, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs.