LAS EMPRESAS TECNOLÓGICAS EN INTERNET COMO AGENTES DE SEGURIDAD INTERPUESTOS

Technology companies on the Internet as inserted security agents

MIRYAM RODRÍGUEZ-IZQUIERDO SERRANO
Universidad de Sevilla
miryamrizq@us.es

Cómo citar/Citation
Rodríguez-Izquierdo Serrano, M. (2019).
Las empresas tecnológicas en Internet como agentes de seguridad interpuestos.
Revista Española de Derecho Constitucional, 117, 77-100.
doi: https://doi.org/10.18042/cepc/redc.117.03

Resumen

Este trabajo se inicia con una reflexión sobre las amenazas que las filtraciones masivas de datos personales suponen para los derechos de participación y para el mantenimiento de las garantías de los sistemas democráticos. Considerando la responsabilidad que en tales filtraciones tienen las empresas tecnológicas que operan en Internet, se analizan algunas de las disposiciones que regulan la actividad de las mismas. La finalidad del análisis es poner de relieve las obligaciones que estas empresas tienen para con la protección de derechos fundamentales y la colaboración con las autoridades. La tesis que subyace es que dichas empresas tienen una posición como intermediarias entre los poderes públicos y los usuarios de Internet para la realización de ciertos fines, de naturaleza constitucional, relacionados con la seguridad y con la salvaguarda del sistema democrático.

Palabras clave

Empresas tecnológicas; redes sociales; proveedores de servicios de Internet; derecho a la intimidad; protección de datos; seguridad; opinión pública; derechos fundamentales; democracia.

Abstract

This works proposes an initial reflection on massive leaks of personal data as a threat to civil rights and constitutional guarantees and on the responsibility of technology companies on the Internet, social networks or search engines, in several of those massive leaks. The article analyses the legal regulation of the activity of such companies and highlights the legal duties of tech companies which are closely related to protection of fundamental rights and cooperation with state authorities. The underlying theory is that technology companies hold an institutional position. As intermediaries between state power and citizenship, they have a relevant role in security achievements and in the defense of constitutional rights.

Keywords

Technology companies; social networks; Internet service providers; right to privacy; data protection; security; public opinion; constitutional rights; democracy.

SUMARIO

I. INTRODUCCIÓN[1]

Corría el mes de abril de 2018 y el creador y presidente de Facebook, Mark Zuckerberg, acaparaba, una vez más, titulares y primeras planas de informativos de todo el planeta. Pero en esta ocasión no era a causa de una nueva compra y fusión de su red social con otra con la que compitiera ni con motivo de espectaculares alzas de sus cotizaciones en bolsa. La noticia era su comparecencia ante el Senado de los Estados Unidos para dar arrepentida cuenta de cómo un fallo en la seguridad de su plataforma digital había permitido que datos de millones usuarios se filtraran. La preocupación de las autoridades estadounidenses ante tales hechos se extremó al constatar que esos datos habían sido utilizados, como mínimo y según se supo, para influir en

[1] El presente trabajo recoge y actualiza la comunicación presentada en el XVII Congreso de la Asociación de Constitucionalistas de España, celebrado en Santiago de Compostela en abril de 2019, en el que se participó a través del Grupo de Investigación SEJ-199 de la Universidad de Sevilla, financiado por la Junta de Andalucía. El artículo conecta con los objetivos del proyecto de investigación «Desafíos en la construcción del espacio europeo de derechos fundamentales» (DER-2017-83779-P), financiado por el Ministerio de Economía y Competitividad. Todas las fuentes electrónicas incluidas han sido recuperadas en fecha 1-10-2019.

procesos electorales a través de su tratamiento por parte de la compañía Cambridge Analytica, implicada directamente en el *hackeo*[2].

Por aquellos días no hubo alzas en el valor de las acciones de Facebook en los mercados financieros. Al contrario, su precio se desplomó. En paralelo, la confianza de los usuarios de la red social, si bien no se hundió en la mayoría de los casos, se tambaleó en muchos de ellos. Pero el hecho de que Zuckerberg compareciera ante los representantes del pueblo de los Estados Unidos para explicar lo ocurrido tenía una segunda lectura que iba más allá de los aspectos de imagen, financieros y comerciales de una marca. El mero requerimiento por parte del Congreso de los Estados Unidos al fundador de la red social para que informase en persona sobre aquellas filtraciones ponía de relieve dos cuestiones clave, interrelacionadas entre sí: la primera es cuán fuertemente los errores de configuración de la plataforma estaban vinculados a la formación libre de la opinión pública, y la segunda, en qué medida, una muy grande, tales errores podían afectar a las garantías propias del sistema democrático.

II. LA ASCENDENTE POSICIÓN INSTITUCIONAL DE LAS EMPRESAS TECNOLÓGICAS

Junto con los derechos de intimidad y privacidad digital de los titulares de los datos, cualesquiera filtraciones masivas de información personal ponen en peligro la libre formación de la opinión pública. En defecto de un carácter institucional en sentido formal, o propio (Habermas, 2002: 203), a la opinión pública se le atribuye una dimensión institucional en sentido material al reconocerla como sustento del Estado constitucional. Así lo ha afirmado el Tribunal Constitucional: la opinión pública «es una institución ligada de manera inescindible al pluralismo político, valor esencial del Estado democrático» (STC 121/1989, FJ 2), y su necesaria protección confiere un valor prevalente al ejercicio de las libertades comunicativas. La dimensión institucional de la opinión pública proviene de su pretensión de influencia (Allport, 1937: 23) y de su función conformadora de la masa crítica, que, con las limitaciones que se le vienen reprochando (Habermas, 2002: 221; Bourdieu, 1973), preconfigura, antes, y refuerza, después, las legitimidades producidas a través de la participación política en sentido estricto (Habermas, 1992: 25). La salvaguarda de esa

[2] Este escándalo de seguridad de datos no es el único en el que Facebook se había visto inmerso a esas alturas, pero incrementó notablemente el grado de alerta sobre el funcionamiento y la seguridad de los datos en esta red social. Sobre los fallos de seguridad previos y sobre el asunto concreto da cuenta Moreno Muñoz (2018).

función estaría conectada con los sistemas y procesos de selección, elaboración y difusión de los contenidos informativos, publicitarios y propagandísticos. La existencia de negocios basados en la recopilación de datos personales a cambio de servicios de comunicación, con diversos formatos y objetos, no tendría más remedio que condicionar dichos sistemas y procesos, compitiendo con el predominio que hasta muy recientemente habían tenido en tal ámbito los medios de comunicación (Berzosa López, 2016: 240).

En la investigación sobre el impactante asunto *Cambrigde Analytica*, la dependencia existente entre la actividad de las redes sociales y las garantías democráticas se mostró, o se demostró, en la realidad y en una doble vertiente. Por una parte, y sin duda, esas filtraciones afectaban a la participación política, pues los datos personales sustraídos se habían utilizado para crear perfiles específicos a los que dirigir propaganda o información susceptible de influir en resultados electorales (Moreno Muñoz, 2018). Por otra parte, al ser extraídos burlando la custodia del responsable de su tratamiento, los datos abandonaban también el campo de control de sus propios titulares, provocando una situación continuada de exposición y riesgo para la privacidad de estos. Se daba la razón, así, a las denuncias que desde mucho antes se habían venido haciendo en relación con las tecnologías como amenazas para la vida colectiva sobre la base de su incidencia en la intimidad (Pérez Luño, 1999: 345).

En efecto, la repercusión que las filtraciones masivas de datos personales tienen sobre las garantías del Estado democrático de derecho, a través de la opinión pública, se puede analizar partiendo de una concepción del derecho principal en riesgo, la privacidad, en la medida en que sus contenidos normativos conectan sustantivamente con las garantías de participación política (Rodríguez Ruiz, 1998a: 26; Fernández Rodríguez, 2004: 69). Más allá de la dimensión estrictamente individual de la intimidad, dominante en la terminología del constituyente español, que la identifica con un ámbito de reserva personal, la privacidad también se referiría al ámbito de acción individual en el que intromisiones no consentidas afectarían a la libertad de actuación general del ciudadano y, con ella, a la de participar en los asuntos públicos[3]. La vulnerabilidad del ciudadano, con sus derechos de participación, aumenta con el seguimiento permanente o vigilancia y se agudiza bajo la influencia del

[3] Parafraseando a la autora citada, para mayor precisión: de las dos concepciones posibles de la intimidad, como bien individual y como bien «cuya protección responde a intereses que trascienden el ámbito de lo puramente individual, ya que hace posible la libre participación en la vida pública, tanto política como social, incluyendo el libre ejercicio de los derechos fundamentales» (Rodríguez Ruiz, 1998a: 26), la problemática aparejada a filtraciones como las de Facebook se enmarcaría en la segunda.

poder sugestivo de la propaganda y de la publicidad comercial. Los efectos distorsionadores sobre la opinión pública de estas últimas (Habermas, 2002: 221) se agravan a causa de su introducción selectiva y vinculada a la información personal hallada en las plataformas digitales. Si a ello se suma la creciente proliferación de contenidos no verificables sobre hechos de actualidad e interés público[4], la preocupación de las autoridades de los Estados democráticos por la actividad de esas plataformas resulta justificada.

La comparecencia de Zuckerberg ante el Senado estadounidense podría verse, por tanto, como una confirmación escénica de la tesis que se propone en este trabajo: la posición fáctica de las empresas tecnológicas, en particular de las que difunden contenidos, como agentes mediadores en la conformación de opinión pública y como responsables de las condiciones de la participación democrática libre sobre la base del control y custodia de la información personal, de la que se nutren[5].

Aunque la posición institucional que se predica de estas empresas se acaba de calificar como fáctica, la tesis planteada apunta algo más alto: las compañías tecnológicas tienen una posición institucional en sentido normativo, derivada de una regulación específica, funcionando como agentes interpuestos entre ciudadanía y poderes públicos. Esta afirmación puede verificarse en una exégesis jurídica que, al menos en el ámbito del derecho de la Unión Europea, y, por consiguiente, en el español, permite establecer los perfiles de una posición institucional que se eleva sobre lo fáctico y es, también en un sentido incremental, ascendente[6].

El reto adicional que se plantea es alcanzar el plano constitucional desde el sustento que ofrezcan los resultados de la exégesis normativa. La intuición que orienta esta búsqueda es que sistemas como los del DUE y los de sus

---

[4] Las noticias falsas, como fenómeno, han llevado a distintos Estados a implementar medidas concretas que afectan a redes sociales y motores de búsqueda para prevenir sus efectos nocivos, en particular sobre los procesos electorales (Pauner Chulvi, 2018: 299).

[5] Una dimensión institucional de las empresas tecnológica ya aparecería frente a los particulares, de una manera fáctica, en la medida en que se así se las percibe en relación con el tratamiento de la información personal (Pöschl, 2015: 94, 106-107). Por otra parte, que las redes sociales son mediadores en la distribución de contenidos informativos de todo tipo, y también de los que forjan la opinión pública como condición participativa, da fe el papel que tienen en la «viralización» de noticias falsas (Pauner Chulvi, 2018: 302 y ss.).

[6] La de las empresas tecnológicas, por tanto, se trataría de una institucionalización que va más allá del sentido social, o no formal, en el que se institucionaliza la opinión pública como consecuencia de su raíz liberal (Habermas, 2002: 203; Walton, 2010: 34).

Estados miembros, que atribuyen a las empresas tecnológicas obligaciones de custodia y protección de derechos fundamentales, serían equiparables, tanto en el contexto actual como en su progresión, a los que los medios de comunicación convencional fueron adquiriendo a lo largo del proceso que llevó desde el Estado liberal al democrático. La propuesta teórica se explicaría de la siguiente forma: en cuanto vehículos para garantizar la conformación de la libre opinión pública, los medios alcanzaron una posición institucional que incluía garantías constitucionales específicas[7] o, dicho de otra manera, la función institucional de la opinión pública, su condición de fuente social de legitimación del poder en el Estado constitucional, dio pie a la centralidad de los medios de comunicación como instituciones básicas en el reconocimiento de las libertades que garantizan aquella.

Como es lógico, al equiparar medios de comunicación convencional y empresas tecnológicas hay que considerar los respectivos contextos histórico-sociales de su emergencia y salvar las diferencias presentes, y obvias, que hay en las características básicas de las funciones sociales y económicas que desempeñan unos y otras. No se olvida que, antecediendo a la regulación normativa de sus servicios a la sociedad, y en el mercado, hay un sustento comercial que define modelos de negocio y, con ello, formas distintas de gestión de contenidos, información o, en el caso de las tecnológicas, datos personales. Son modelos, el de los medios y el de las empresas tecnológicas, que solo se solapan cuando el soporte digital, Internet, los hace converger, conservando, aun en ese caso, características, objetos y objetivos propios.

Obsérvese, como ejemplo para la diferenciación, el modelo de empresa tecnológica de las redes sociales. Estas ofrecen interacción social-virtual a cambio de datos personales de todo tipo. La vida de los usuarios, en lugar de la información y opinión sobre hechos relevantes como núcleo de la actividad

[7] En cualquier caso, conviene puntualizar que la de los medios de comunicación tampoco se trata de una institucionalización normativa en sentido propio, sino de una en sentido instrumental: por una parte, basada en su situación privilegiada en el ejercicio de las libertades de comunicación pública, y, por otra parte, necesaria para vehiculizar aquellas. En efecto, sostiene Solozábal Echevarría (1988: 146) que la atribución de una función institucional a las libertades de comunicación pública, como la efectuada por la doctrina constitucional cuando define cuál es su contribución a la realización del principio democrático, no transforma la naturaleza jurídica las libertades de comunicación, de derechos de libertad individual a garantías institucionales. Sin embargo, y por otra parte, las garantías normativas de la pluralidad mediática tienen una innegable dimensión constitucional y se concretan en medidas que afectan a la estructura empresarial de los medios, pudiendo considerarse en cierto sentido garantías de dimensión institucional.

de los medios, es el centro de su negocio. El rol institucional de las redes, por tanto, no tiene una relación directa, ni tampoco indirecta, con la veracidad o el interés público de los contenidos intercambiados, sino con la utilidad de esos datos de carácter personal. Se trata de datos que primero recopilan como objeto de negocio y luego deben cuidar. El deber de cuidado se anuda, al menos, a tres razones distintas: mantener la confianza de los usuarios, y, por tanto, su actividad y existencia; cumplir con las obligaciones y límites que les imponen las leyes regulatorias, evitando sanciones de diferente coste económico y social, y cumplir la función colaborativa que el mercado y el Estado les otorgan, al no ser capaces, por sí mismos —al menos claramente el segundo no lo es—, de facilitar y ordenar un flujo de interacción e información personal de tamaña importancia[8].

Pero hay una cuarta razón que, aunque no sea la originaria, está vinculada a las anteriores y desciende al terreno de lo normativo que interesa a este estudio. Las empresas tecnológicas se emplean en el adecuado tratamiento y en la custodia de los datos personales que recaban para sus fines porque, en línea con la argumentación o tesis de fondo y volviendo a ella, se han transformado en agentes interpuestos, mediadores entre ciudadanía y Estado, adquiriendo un rol institucional. Dicho rol, si bien tiene el coste de anudarlos, como agentes, al cumplimiento de una regulación y autorregulación cada vez más meticulosas, también retroalimenta su objetivo inicial, que no es otro que el de conseguir usuarios, afiliados, público al fin y al cabo, dispuestos a facilitar datos personales y a interactuar en las plataformas, dejando en ellas otro tipo de rastro aprovechable para fines estadísticos y comerciales. Desde esa perspectiva, las tecnológicas serían entes a los que se pone a cargo de las necesarias condiciones de la seguridad en la red y, con ellas, de la garantía de derechos básicos para la participación, la privacidad, entre otros. En términos de teoría del discurso, se diría que se sitúan como actores necesarios en el mantenimiento de las condiciones básicas para la correcta deliberación que requieren las concepciones discursivas del Estado constitucional y democrático de derecho (Rodríguez Ruiz, 1998b). Y, no obstante, no ha de olvidarse, su interés sigue siendo el negocio.

En efecto, y retomando la comparativa con los medios de comunicación convencionales, a estos se les ha exigido y se les exige, constitucional y socialmente, una especial diligencia en el tratamiento de información y de las opiniones, como contrapartida a la privilegiada posición desde la que ejercen las

[8] Explica Magdalena Pöschl (2015: 107) que «la capacidad del prestador del servicio de Internet para acercarse a la intimidad de las personas, de masas humanas, le hace, más allá de su dinero, especialmente interesante para un Estado hambriento de datos».

libertades de comunicación pública. En su turno, a las empresas tecnológicas se les han ido atribuyendo deberes específicos relacionados con la custodia y con la protección de los perfiles personales y virtuales de los ciudadanos-usuarios. Esos deberes sirven, en parte, como imposición a cuenta de los beneficios que obtienen gracias al acceso, también privilegiado, a esa información personal, pero, en otra parte, son el único modo que los poderes públicos tienen para asegurar condiciones mínimas de seguridad, y libertad, en el tratamiento de esos perfiles.

Para desarrollar los perfiles normativos que den apoyo a la tesis de partida, en las páginas que siguen se realizará esa exégesis anunciada, revisando disposiciones vigentes que, atribuyendo a empresas tecnológicas obligaciones de garantía y custodia de derechos, las institucionalizan y les otorgan una función constitucional en sentido material. Se revisarán normas que confieren a las tecnológicas diversos roles como mediadoras y guardianas: mediadoras en la formación de la opinión pública y guardianas de las condiciones de ejercicio de los derechos de la libertad y participación, en ambos casos por su condición de gestoras de comunicaciones digitales y custodias de ingentes cantidades de datos de carácter personal. La panorámica no será exhaustiva, ni en detalle, pues se trata de delinear el perfil mínimo de esa posición institucional para empresas que ofrecen servicios de comunicación a cambio de información personal, como concreción dentro del muy amplio conjunto de lo que pueda entenderse como empresa tecnológica[9]. Se esbozarán los elementos básicos de la función de garantía y seguridad atribuida a estos entes de naturaleza privada, teniendo presente la contradicción de que, a la vez que sus garantes, son los principales responsables de la situación de riesgo en la que se encuentran los derechos de privacidad, y participación, de los ciudadanos[10].

III. EMPRESAS TECNOLÓGICAS Y GARANTÍAS DE DERECHOS

Desde los años noventa del siglo xx, el DUE ha estado especialmente concernido por las cuestiones relativas al uso de la tecnología en las relaciones

[9] La clasificación y análisis de proveedores de servicios de Internet incluiría a las redes sociales como actores específicos, sin agotar las posibilidades presentes y futuras de creación de otros modelos de intermediarios en la difusión de contenidos (Barrio Andrés, 2017: 345 y ss.).

[10] La base comercial es precisamente la que pone en riesgo los datos, que se recopilan para negociar con ellos, al tiempo que se analizan y segmentan sobre la base de una tecnología que puede dejarlos al descubierto (Moreno Muñoz, 2018: apdo. 7).

comerciales. Es por ello que, en el ámbito de la Unión, y, por tanto, en lo que a España se refiere, las responsabilidades de las empresas tecnológicas han sido codificadas en diferentes instrumentos normativos y desde muy pronto se aprobaron diversas directivas sobre comercio electrónico, servicios de la sociedad de la información y protección de datos. Esas responsabilidades, unas de cara a la Administración y otras de cara a los usuarios, ofrecen una primera muestra de en qué medida los proveedores de servicios de Internet, las plataformas de difusión de contenidos y otras empresas que operan en la red pueden considerarse agentes interpuestos en cuestiones relativas a la protección de los derechos de particulares. Por su conexión con los arts. 18.3 y 18.4 CE, y en definitiva con las garantías propias de la privacidad, se trata de responsabilidades de las que puede predicarse una relevancia *iusfundamental*.

1. OBLIGACIONES DE CARA A USUARIOS DE LAS REDES: SEGURIDAD, CUSTODIA Y LÍMITES EN EL TRATAMIENTO DE DATOS PERSONALES

En el primer grupo de obligaciones se incluyen algunas de las relacionadas con la seguridad de los datos, aplicables tanto a Internet como a cualquier otro medio que canalice la recogida y el tratamiento de información personal. Al respecto, las disposiciones vigentes de mayor actualidad son las del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. La Ley Orgánica 3/2018, de Protección de datos, es la norma que incorpora al ordenamiento estatal español aquellas disposiciones del antedicho reglamento que requieren adaptación[11].

Las remisiones de la nueva ley orgánica al citado reglamento son la tónica general del título III de la ley, relativo a los derechos de las personas cuyos

[11] La entrada en vigor del Reglamento de Protección de Datos en 2018 supuso la definitiva sustitución de la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Del mismo modo, la Ley Orgánica 3/2018 sustituye a la anterior LO 15/1999, de Protección de datos.

datos son objeto de tratamiento. Son los conocidos derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición y cancelación. Estos derechos van seguidos, algo más adelante, por una cláusula general de seguridad digital, en el art. 82, y precedidos, bien antes, por una obligación de confidencialidad, también general, en el art. 5. Los deberes de información de los responsables del tratamiento, en el art. 11, se incluyen para dar garantía al usuario de que habrá un interlocutor en caso de duda o cambio de criterio sobre los datos en custodia. Por último, junto con otra serie de garantías más específicas, el marco normativo se cierra con un título IX dedicado al régimen sancionador a cargo de la Agencia Española de Protección de Datos. Así se sujeta tanto a responsables y encargados del tratamiento de datos como a sus representantes en el territorio UE, a las entidades de certificación y a las entidades encargadas de la supervisión de los códigos de conducta que establece el Reglamento.

La indagación en otros textos legales relevantes que establecen garantías para los usuarios de Internet remite a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, también en su mayor parte procedente de un mandato de transposición del DUE[12]. Esta ley asigna a los proveedores de redes y plataformas digitales obligaciones de información sobre los riesgos que conlleva la utilización de sus servicios para la seguridad y la privacidad, así como sobre los posibles mecanismos para prevenirlos, en concreto, en el art. 12 bis LSSI.

Por su parte, la Ley 9/2014, nueva ley general de telecomunicaciones, establece en su art. 41 una obligación especial de protección de los datos relativos a las comunicaciones electrónicas, exigiendo una política de seguridad para las mismas que incluye el cifrado y la vigilancia de las propias redes, conforme a los arts. 43 y 44 de la misma ley. El acceso a algunos de estos datos, los que desde cierta perspectiva podrían entenderse en un lugar intermedio entre el derecho al secreto de las comunicaciones y la protección de datos de carácter personal, se considera como verdadero factor de riesgo para la seguridad y la privacidad de los individuos: los conocidos como datos de tráfico, en cuya delimitación jurídica aún no se ha conseguido la precisión deseable (Fernández Rodríguez, 2016: 100 y ss.). Esos potenciales

[12] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. La LSSI española añade una exclusión de responsabilidad no prevista en la norma de la UE: la que se refiere a las actividades de provisión de enlaces y de herramientas de localización de información (art. 17 LSSI) (Peguera Poch, 2007: 4).

riesgos para la seguridad y la privacidad de las personas ponen en evidencia que las tecnologías de la comunicación digital, al crear un espacio-tiempo propio, hacen necesaria la reconceptuación de ciertas categorías *iusfundamentales*, cuando no, como se verá a continuación, el alumbramiento de algunas nuevas. Se trata, en definitiva, de ajustar los mecanismos de garantía a las incertidumbres que la tecnología proyecta sobre los derechos. A la espera se está del efecto que sobre estas cuestiones acabe teniendo, en caso de que se aprobase la propuesta, el futuro Reglamento sobre la privacidad y las comunicaciones electrónicas, *E-Privacy*, por el momento atascado en fase legislativa el Consejo de la Unión[13].

2. OBLIGACIONES DE CARA A TERCEROS: VIGILANCIA, DERECHO AL OLVIDO Y RESPONSABILIDAD OBJETIVA POR CONTENIDOS LESIVOS

Usuarios o no de las redes, los datos y la privacidad de cualquier persona son objeto de protección por parte del sistema normativo y lo son con la inevitable intermediación de empresas tecnológicas. Bien en calidad de responsables del tratamiento de datos, bien en calidad de proveedores de servicios de la sociedad de la información, las empresas tecnológicas responden frente a terceros.

En la nueva LOPD esto se recoge en varios ámbitos. Por una parte, el art. 24 se refiere a la posible implementación de sistemas de denuncias a través de los cuales se pueda poner en conocimiento de una entidad privada la comisión de actos contrarios a la legislación. Por otra parte, se establece un derecho de rectificación propiamente digital, en el art. 85, encomendando a las empresas responsables de redes sociales y equivalentes que implementen mecanismos para hacer viable la aplicación a sus servicios de la Ley Orgánica 2/1984, reguladora del derecho de rectificación. Es una obligación que se traslada también a los medios de comunicación que utilicen soportes digitales, lo cual resulta lógico en la medida en que estos cumplen con la función constitucional de transmisión de información veraz que justifica la existencia del procedimiento. Cuando el derecho de rectificación se proyecta sobre las redes sociales, cuya función no es, en principio, equiparable a la de los medios, se

[13] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM/2017/010 final — 2017/03 (COD).

ahonda en la caracterización de estas plataformas como intermediarios en la formación de la opinión pública[14], al margen de las posibles afectaciones individuales al honor o la intimidad.

A continuación, el art. 86 LOPD crea otro derecho de nuevo corte: el de actualización de la información digital relativa a una persona. Consiste en la posibilidad de pedir que se incluya un aviso de actualización «suficientemente visible» —dice la ley— junto a las noticias que conciernan a una persona cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio. Es decir: se trataría de adaptar el ya consolidado derecho al olvido digital[15], del que la ley se ocupa algo más adelante, a los casos de informaciones relevantes y veraces que, contenidas en las hemerotecas *online* de los medios, hayan quedado muy atrás y superadas por cambios efectivos[16].

Y por fin, en efecto, la LOPD se refiere también al derecho al olvido, que no solo se va a proyectar sobre las indexaciones realizadas por los motores de búsqueda, reflejadas en el art. 93. La nueva ley incorpora una exigencia de olvido específica para las redes sociales en el art. 94, que vincula a estas incluso si hubiere sido uno mismo quien cedió la información. Si la información hubiere sido cedida por otros, el olvido en redes sociales se impondría cuando esa información se probase inadecuada o desfasada.

---

[14] Lo mismo puede decirse en relación con los instrumentos de *soft law* mediante los que la Unión Europea ha activado sendos planes de trabajo, implicando a las empresas tecnológicas en la lucha contra la desinformación: Comunicación conjunta al Parlamento Europeo, al Consejo Europeo, al Consejo, el Comité Económico y Social y al Comité de las Regiones «Plan de acción contra la desinformación», de 5 de diciembre de 2018, JOIN(2018) 36 final (disponible en: https://bit.ly/35bTgVU), y Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones «La lucha contra la desinformación en línea: un enfoque europeo», de 26 de abril de 2018, COM(2018) 236 final (disponible en: https://bit.ly/2rTp5V4).

[15] Derivado de la muy relevante sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014 en el asunto C-131/12, *Google Spain*, EU:C:2014:317, que en su momento supuso una innovación al alumbrar un contenido adicional a la privacidad y al honor desde la normativa de protección de datos (Rallo, 2014: 259).

[16] Véase el fundamento jurídico 8 de la STC 58/2018, de 4 de junio, ES:TC:2018:58, que establece la obligación de desindexar los datos personales de las noticias contenidas en esos archivos periodísticos digitales y sustituirlos por iniciales para proteger los derechos de la personalidad del 18.1 CE y el de autodeterminación informativa del 18.4 CE.

Más allá del ámbito de la ley protección de datos, y abarcando también la de otros bienes jurídicos como la propiedad intelectual, también a las empresas proveedoras de servicios de copia, alojamiento o inserción de cualquier tipo de información se las hace responsables de posibles ilicitudes en estos procedimientos. En efecto, la ley de servicios de la sociedad de la información establece en sus arts. 15, 16 y 17 la responsabilidad de prestadores de servicios de copia temporal de datos, alojamiento o a los que faciliten enlaces a contenidos o instrumentos de búsqueda. En una aproximación sucinta[17], de la ley se desprende que tanto la ausencia de conocimiento efectivo de la ilicitud como la diligente retirada de los contenidos lesivos, cuando se tenga conocimientos de ello, eximen a los prestadores de la responsabilidad que la ley les atribuye. Se da a entender, igualmente, que ese conocimiento efectivo puede presumirse más allá de los supuestos de intervención judicial cuando este se haya adquirido —art. 17.1 *in fine*— en virtud de «procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse». Se sobreentiende, por tanto, una obligación de vigilancia para estos intermediarios que, de desatenderse, desencadenará el mecanismo de atribución de responsabilidad, y ello sin necesidad de que haya un apercibimiento externo sobre la ilicitud de los contenidos. Así lo ha entendido el Tribunal Supremo en la Sentencia 72/2011, de 10 de febrero, caso *Alasbarricadas.com* (Martínez Otero, 2016: 143-144).

Como consecuencia de lo establecido en estas disposiciones, el perjudicado en sus derechos podrá, en cualquiera de estos casos, dirigirse al proveedor de servicios para obtener la reparación correspondiente por los daños. Todo ello constituye no solo una garantía para esos terceros, sino que también es parte de un deber de colaboración con las autoridades públicas para perseguir las ilicitudes y desventajas, incluso lícitas, de la exposición de la privacidad en la red (Plaza Penadés, 2013: 72). Al entenderse que esa responsabilidad frente a terceros se trata de un supuesto de responsabilidad por hecho ajeno, y no por hecho propio sobre contenidos ajenos, se consolida la percepción de la intención preventiva que inspira estos preceptos, encaminados a permitir un mejor funcionamiento de la red. Tal percepción confirmaría que esta responsabilidad por daños es una garantía de doble dimensión, subjetiva y objetiva (*ibid*.: 75-76), sirviendo esta reflexión para abrir la puerta a las cuestiones relativas a la relación entre empresas tecnológicas y seguridad pública.

[17] Puede consultarse un análisis con más detalle en el trabajo de Plaza Penadés (2013: 74 y ss.).

IV. LAS EMPRESAS TECNOLÓGICAS ANTE LA NECESIDAD DE VELAR POR LA SEGURIDAD PÚBLICA

1. CONFIDENCIALIDAD Y SEGURIDAD DE DATOS PERSONALES FRENTE A SEGURIDAD PÚBLICA E INTERÉS GENERAL

Que la protección de la confidencialidad y el secreto de las transacciones de contenidos y datos en la red pueden excepcionarse y matizarse por razones de interés público es algo explícito en el marco legal de las comunicaciones digitales y en el del tratamiento de los datos. Se intuye la gran importancia que puede llegar a tener el acceso a cierta información, incluso información personal, para la organización de la vida del Estado y en especial para la seguridad. Esos mismos registros que son protegidos, por mandato legal, frente a los procesadores de datos y proveedores de servicios pueden ser parcialmente desprotegidos, en razón de similar mandato, siempre y cuando se cumplan una serie de condiciones.

El art. 8 de la LOPD establece cuáles son los requisitos generales para entender que el tratamiento de datos se debe a una obligación legal, la sumisión a un interés público o al ejercicio de poderes públicos. En primer lugar, lo hace estableciendo una reserva de ley, bien de DUE, bien estatal, que prevea las condiciones generales del tratamiento y los tipos de datos que pueden ser objeto del mismo. La ley podrá, en esos casos, imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679. En segundo lugar, y respecto al tratamiento de datos fundado en el interés público o en el ejercicio de poderes públicos, también se exige reserva de ley.

Pero más allá de la reserva formal de ley, y no obstante la ausencia de referencia concreta en el precepto, estarían las exigencias materiales de esa reserva. Se trataría de esos elementos que son consustanciales a cualquier norma restrictiva de derechos y que, en concreto para los derechos de esta clase, tendrían que responder a los parámetros definidos en el asunto *Digital Rights* por el TJUE como elementos de calidad de la ley. En definitiva: las garantías específicas anudadas a la propia reserva de ley y a las que se adiciona el principio de proporcionalidad. En el caso de la conservación de datos, la ley debe diferenciar los datos, los que fueran a ser retenidos, en función de su fuente o de un objetivo dado de protección de la seguridad o investigación criminal. No es válido establecer un mandato de conservación, tratamiento o acceso, generalizada y sin excepciones. Se deben exigir también restricciones y condiciones específicas para el acceso y utilización de esos datos, como un control judicial previo. También es preciso delimitar un arco temporal

definido de conservación de datos para los fines que había establecido la Directiva 2006/24/CE del Parlamento y del Consejo de retención de datos, así como marcar obligaciones más claras a los proveedores de servicios de comunicación para garantizar la seguridad de los datos conservados[18]. Aquí se vuelve a poner el foco en cómo los intermediarios, empresas tecnológicas, tienen que colaborar con los fines de interés público y de seguridad que determinan las leyes, al tiempo que han de seguir siendo garantes de la reserva, o confidencialidad, y protección de los datos.

2. OBLIGACIONES DE RETENCIÓN, CESIÓN DE DATOS Y COLABORACIÓN CON LOS PODERES PÚBLICOS

La invalidez de la Directiva de retención de datos, declarada por el TJUE en su sentencia de 2014, no hizo desparecer la obligación de retención de datos para los operadores de comunicaciones digitales, pues la regulación europea ya había sido transpuesta. Sí que hubo una adaptación de esas normas estatales. En concreto, en el caso español, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, se modificó mediante la disposición adicional cuarta de la Ley 9/2014, de 9 de mayo, un mes después del fallo del TJUE[19].

En la regulación actual, el protagonismo de las empresas tecnológicas de comunicaciones es indiscutible en la implementación de cualquier normativa sobre conservación de información de tráfico. Los sujetos obligados por la ley de retención, en su art. 2, son inequívocos: los operadores que presten servicios

[18] Véanse los párrafos 108 y siguientes de las conclusiones del abogado general Cruz Villalón de 12 de diciembre de 2013 en el asunto *Digital Rights*, C-293/12 y C-594/12, EU:C:2013:845, así como los párrafos 45 a 71 de la sentencia del TJUE de 8 de abril de 2014 en el mismo asunto, EU:C:2014:238. La directiva arrastraba una serie de problemas de constitucionalidad (Lynskey, 2014), motivo por el cual acabó siendo declarada inválida, por contravenir los derechos a la privacidad y a la protección de datos (González Pascual, 2014: 955), en la STJUE de 8 de abril de 2014, asunto *Digital Rights*, C-293/12 y C-594/12, EU:C:2014:238.

[19] Algunas leyes de transposición ya habían sido modificadas con anterioridad a la sentencia *Digital Rights* como consecuencia de fallos de inconstitucionalidad previos por parte de jueces constitucionales estatales (Lynskey, 2014: 1799). En otros supuestos, como los del Reino Unido o Suecia, las adaptaciones del derecho interno llegaron con posterioridad y a través de mandatos de nueva jurisprudencia derivada de cuestiones prejudiciales: asunto *Tele2 Sverige AB*, C-203/15 y C-698/15, acumulados, Sentencia del TJUE, de 21 de diciembre de 2016, EU:C:2016:970.

de comunicaciones electrónicas disponibles al público o los que exploten redes públicas de comunicaciones en los términos de la ley general de telecomunicaciones. Los datos a conservar, y en su caso ceder, vienen definidos en el art. 3 de la ley, todos ellos relativos a las coordenadas de las comunicaciones realizadas, incluso las fallidas. El procedimiento de cesión de datos, mediante resolución judicial previa, motivada y justificada conforme al principio de proporcionalidad, determina el deber de colaboración de los operadores con fuerzas y cuerpos de seguridad del Estado, vigilancia aduanera e inteligencia —arts. 7 y 8 de la ley—. En esos casos, ni la cesión será comunicada al titular de los datos por el operador ni tendrá efecto la solicitud de acceso o cancelación que pudiera efectuar este —art. 9—, pasando los proveedores de servicios a adoptar una función interpuesta, como se viene defendiendo, entre la custodia de datos y el compromiso con las exigencias de la seguridad pública y el interés general.

En otro orden de intereses, la LSSI también establece en su art. 11 la exigencia de contar con la colaboración de los prestadores de servicios de la sociedad de la información. En ese marco regulativo el objetivo es poner fin a las lesiones de bienes jurídicos que se produzcan a través de las redes. En tales circunstancias, los prestadores tendrán que seguir los mandatos del órgano competente que ordene, conforme a derecho, la interrupción de la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos. La orden tendrá que venir avalada por resolución judicial cuando se afecte a derechos y bienes jurídicos respecto a los cuales la Constitución exija intervención judicial.

En el mismo texto legal, en la disposición adicional novena introducida por la reforma de la ley general de telecomunicaciones en 2014, también se exige a estos intermediarios que colaboren en los incidentes de ciberseguridad que afecten a Internet, suministrando a las autoridades competentes la información necesaria para identificar a los responsables de los mismos (Barrio Andrés, 2017: 455). Por otra parte, y volviendo a la LOPD, también la Agencia Española de Protección de Datos podrá recabar la colaboración de los responsables del tratamiento de datos para sus funciones de investigación, conforme a lo dispuesto en el art. 52 de la ley.

3. LA EMPRESA TECNOLÓGICA COMO GARANTE DE LA PRIVACIDAD ANTE LAS CESIONES INTERNACIONALES DE DATOS: EL CASO *MICROSOFT CORP. VS. UNITED STATES*

Dando un salto hacia cuestiones de dimensión internacional, y más allá del DUE, se inicia este apartado final con una consideración que si puede

resultar tardía es porque hasta ahora se ha dado por supuesta. Sin embargo, cobra protagonismo en el momento en el que el análisis se desvía del ámbito de lo estatal, o en concreto del marco normativo español dentro de la Unión Europea. La consideración, o la indiscutible evidencia, recuerda en este punto que Internet es global y las empresas tecnológicas, las más relevantes, también, pero las jurisdicciones de los Estados no lo son (Muñoz Machado, 2000: 65). Esta realidad se impuso bien pronto. A medida que fue incrementando exponencialmente el número de usuarios de Internet, y con ello la litigiosidad en torno a conflictos derivados de su uso, se pudo constatar cómo muchos de ellos acababan siendo resueltos por tribunales de lugares distintos a aquellos en los que se alojaban los contenidos, el lugar físico de los servidores, o se había producido la lesión inicial de bienes jurídicos protegidos[20]. A la larga esto ha implicado que las leyes aplicables a Internet, y en consecuencia a las empresas tecnológicas, varíen de un lugar a otro del planeta[21]. Los Estados miembros de la UE, por razón de su pertenencia al mercado único y al espacio de libertad, seguridad y justicia, son los que han logrado una mayor homogeneidad en algunas de estas cuestiones, si bien las regulaciones comunes se siguen sustentando, en última instancia, en una concepción de soberanía estatal atribuida, eso sí, funcionalmente a la Unión.

El hecho es que las empresas tecnológicas se someten a diferentes regulaciones en función del lugar en el que tengan su sede principal y sus sucursales o de qué nacionalidad sea el proveedor o el servidor del que depende la gestión de los contenidos o datos. Pero su propio objeto de negocio hace que, en muchas ocasiones, necesiten transferir datos de unos puntos geográficos a otros para la prestación de sus servicios o para la obtención de su beneficio. Esas transferencias, sin embargo, no pueden hacerse libremente, desde luego y con carácter general no sin consentimiento del afectado, pero normalmente

[20] También muy a principios de siglo se analizaba en este sentido el asunto *Yahoo*, que enfrentaba a la plataforma del mismo nombre ante la justicia de los tribunales franceses (De la Torre y Cotino, 2002).

[21] Se dice que «a la larga» puesto que, tras un momento inicial en el que algunos estudiosos de la comunicación en la red abogaron abiertamente por dejar que Internet fuera un espacio desregulado y solo controlado por el código (Johnson y Post, 1996; Zittrain, 2008: 173-174; Nunziato, 2009), las visiones regulativas, defensoras de la competencia de los Estados para regular sobre el uso de Internet, se fueron imponiendo. En estas últimas, frente a autores que postulaban a favor de la creación de cooperación entre Estados para resolver cuestiones relativas a Internet (Muñoz Machado, 2000: 65), otros lo hacían a favor de la recuperación del poder soberano de los Estados sobre la red, incluso usando estos la tecnología para controlarla (Reidenberg, 2004).

también están condicionadas por requisitos legales de distinto signo, siempre en función de los lugares de origen y destino de los datos.

En el caso español, en conexión con el DUE, esas transferencias internacionales de datos están determinadas por el Reglamento de protección de datos en sus arts. 44 y siguientes. En líneas generales, son transferencias no permitidas[22], pero sí que se establecen procedimientos, que pasan por instancias europeas y por autoridades estatales de protección de datos, tanto para adoptar las cláusulas contractuales tipo que puedan utilizarse con terceros para tal fin como para aprobar normas corporativas, vinculantes e internas a las empresas o corporaciones que vayan a transferir datos de un país a otro fuera de la Unión. Esto hace posible transferir datos siempre y cuando haya una decisión previa de adecuación, por parte de la Comisión Europea, sobre los niveles de protección de datos del país de destino de estas transferencias. Se trata, sin duda, de una proyección extraterritorial de las garantías ofrecidas por la regulación del DUE. En ausencia de decisión de adecuación, las transferencias internacionales de datos se complican, requiriéndose a veces una autorización previa por parte de las autoridades de control y siempre tras una investigación por parte de esta, teniendo en cuenta las garantías que los afectados van a poder activar en relación con los datos transferidos.

Como puede observarse, el DUE desarrolla un detallado y estricto marco regulativo para las empresas que, tecnológicas o no, sean responsables de los datos personales que les hayan conferido los particulares en territorio de Estados de la Unión y pretendan sacarlos de esa jurisdicción. Además, ese marco regulativo no es susceptible de excepción, salvo lo dispuesto en el art. 49 del Reglamento. Esa disposición recoge varias razones por las cuales se pueden transferir datos al extranjero. Casi todas ellas se remiten al beneficio del interesado. Pero otras lo hacen a razones importantes que lo justifiquen en función del interés público, que también puede ser causa de una excepción según el 49.1. d). La regulación del DUE se abre, así, a entender que las empresas custodias de datos, tecnológicas o no, se transforman en agentes de seguridad también en otros países, cuando las circunstancias así lo requieren.

No obstante, eso no quiere decir que la exigencia de colaboración con la seguridad de un Estado tercero libere datos de procedencia europea sin la debida garantía. Por una parte, el art. 48 del Reglamento estipula que, si se trata de ejecutar un mandato judicial de un país tercero, será necesario un tratado de asistencia jurídica mutua vigente entre ese tercero y la Unión. En defecto del mismo, el último inciso de ese artículo, «sin perjuicio de otros motivos para la

[22] Es un régimen similar al anteriormente dispuesto en la Directiva 95/46/CE, y que se resume en Sánchez Ferro (2018: 89 y ss.).

transferencia al amparo de este capítulo», parece dejar abierta la posibilidad de transferir datos sin consentimiento, y sin beneficio del titular de estos, cuando haya un motivo importante de interés público. Pero la interpretación de este inciso no resulta del todo clara, pues la excepción del art. 49.1.d) parece volver a matizarse en el 49.4, confirmando que el interés público importante será decidido por el DUE o por el del Estado miembro competente, a la vez que el 49.5 permite limitar transferencias de determinados datos cuando estas no se dirijan a un país que goce de una decisión de adecuación.

Toda esta disquisición sobre las condiciones en las que los datos custodiados en territorio de Estados de la UE pueden o no transferirse, y cuáles podrían aportarse, o no, a requerimiento de una instancia judicial de un país tercero, ha tenido una resonancia singular en tiempos recientes por su conexión con el caso *Microsoft Corp. vs. United States* 584 U. S. (2018)[23]. Las circunstancias de este caso aparecen unidas a las vicisitudes por las que han pasado y siguen pasando, en Europa, las decisiones de la Comisión sobre la adecuación de las garantías de la privacidad para la transferencia de datos a Estados Unidos, que son las transferencias de empresa a las que antes se aludía[24]. Ambas, circunstancias y vicisitudes, propician una reflexión sobre las dificultades de articular garantías de privacidad y seguridad en Internet cuando las empresas tecnológicas tienen dimensión transnacional. Si por una parte son precisas garantías para los derechos de los titulares de los datos, que en el caso de *Microsoft Copr. vs. United States* eran datos sobre comunicaciones y contenido de las comunicaciones en sí mismas, por otra parte estas garantías habrían de ser flexibles en situaciones en las que la seguridad pública así lo requiriera. No se olvide que seguridad pública no es solo seguridad dentro del Estado y que muchas amenazas a esa seguridad pública son transnacionales. Alcanzar ese equilibrio ya es trabajoso en el contexto de una jurisdicción estatal, por lo que propiciarlo mínimamente en el contexto del intercambio de datos e información entre jurisdicciones diversas lo es más aún. El caso *Microsoft Corp. vs. United States* lo pone de manifiesto.

---

[23] La información sobre el caso está disponible en https://bit.ly/2KvzQn4.

[24] Teniendo en cuenta que la Decisión 2000/520/CE, conocida como *Safe Harbour* o *Puerto Seguro*, fue invalidada por la Sentencia del Tribunal de Justicia de la UE de 6 de octubre de 2015 en el asunto C-362/14, *Schrems*, EU:C:2015:650, y que la actualmente vigente, la Decisión 2016/1250, conocida como Escudo de Privacidad, revisada anualmente, sigue obteniendo valoraciones altamente críticas por parte del Parlamento Europeo. Véase la Resolución del Parlamento Europeo sobre la adecuación de la protección conferida por el escudo de la privacidad UE-EE. UU. (2018/2645(RSP), disponible en https://bit.ly/2QsUsA8.

Microsoft Corp. vs. United States fue elevado a conocimiento del Tribunal Supremo de los Estados Unidos en 2016. La controversia versaba sobre un conflicto entre la empresa tecnológica y el Gobierno de aquel país a causa de un juicio penal por presunto delito de narcotráfico. La fiscalía había obtenido en 2013 una orden del juez de distrito de Nueva York, mediante la cual se exigía a la empresa aportar unos correos electrónicos que se encontraban alojados en el servidor que *Microsoft* tenía en Dublín, Irlanda. La empresa replicó que la *Stored Communications Act*, proveniente de la *Electronic Communications Privacy Act* de 1986, no facultaba para emitir esa orden judicial por ser extraterritorial. Ese fue el argumento con el que apeló contra la misma. La orden acabó siendo revocada por el tribunal del Segundo Circuito, que admitió que había una aplicación extraterritorial de la *SCA*. El Gobierno de EE. UU., en su turno, apeló al Supremo, alegando de nuevo Microsoft que la ubicación de los correos requeridos los ponía bajo jurisdicción irlandesa, sometida al DUE, y que conforme a ese ordenamiento era necesario un acuerdo de asistencia jurídica mutua. Por más que Microsoft fuera una empresa ubicada en territorio estadounidense, y sometida a aquella jurisdicción, la ley que regulaba la cesión de esos datos, aun por motivos de seguridad o de investigación del delito, no era —o no *exclusivamente*, matiz de importancia en el asunto— la de aquel país.

Como respuesta al conflicto, y antes de que el Tribunal Supremo entrase a resolverlo, el Congreso optó por reformar la *SCA*. Lo hizo en marzo de 2018 a través de la *Clarifying Lawfull Overseas Use of Data Act*. Como consecuencia de la reforma, se emitió una nueva orden y el caso, que quedó sobreseído por irrelevante, fue devuelto al juez de apelación (Daskal, 2018). La reforma legislativa realizada de la *CLOUD Act* estableció, con una claridad que no figuraba en la anterior *SCA*, la obligación de la empresa tecnológica de asistir a la acción de la justicia en territorio estadounidense, facilitando los datos que tuviera alojados en sus servidores independientemente de su ubicación. Por tanto, la dimensión extraterritorial del mandato no solo no se eliminó, sino que, al contrario, se confirmó. No obstante, la ley tampoco ha querido ser ciega a los inconvenientes que planteaban esa eficacia extraterritorial, por lo que permite una cierta ponderación cuando la empresa requerida tenga los servidores señalados por el juez en territorios en los que las condiciones legales supusieran que, para cumplir con la justicia estadounidense, se tuviera que infringir la ley del lugar (*ibid*.).

Esta concesión que hace la *CLOUD Act* revela que el sistema estadounidense, aun insistiendo en que las empresas tecnológicas bajo su jurisdicción tienen deberes de colaboración con la seguridad nacional, también toma en consideración la función de estas como intermediarias en la red global. Pero

del mismo modo significa que solo mediante la articulación de mecanismos de colaboración entre Estados de una y otra parte del globo, entre sí y con las empresas tecnológicas, se podrá alcanzar un estándar común de seguridad y garantías que sea, por un lado, aceptable para los distintos actores implicados como agentes de seguridad, y, por otro, respetuoso con los derechos de los ciudadanos afectados.

IV. REFLEXIÓN FINAL: LA INSTRUMENTALIZACIÓN DE LAS EMPRESAS TECNOLÓGICAS COMO AGENTES DE SEGURIDAD INTERPUESTOS

Las cuestiones que suscita el asunto *Microsoft Corp. vs. United States* hacen ver que, aun cuando las leyes de EE. UU. no confieren a las empresas obligaciones de custodia tan meticulosas como las europeas, al menos en la vertiente de la seguridad sí hay una equiparación en la posición de las mismas como cooperadoras con la acción de la autoridad y a favor del interés público. No obstante, y en la medida en que no hay un nivel de garantía correspondiente al del DUE para los derechos a la privacidad y a la protección de datos, podría afirmarse que en el otro lado del Atlántico las empresas tecnológicas no son agentes interpuestos al mismo nivel que lo son en Europa. Y el problema para estas empresas es que, con sus diferentes patas extendidas en red sobre los respectivos continentes, siguen siendo una misma araña: una cabeza, un cuerpo, diversas localizaciones.

La solución a los problemas que de lo anterior se derivan para el sistema europeo de protección de la intimidad y de los datos personales tiene al menos dos obstáculos: que las grandes tecnológicas son, casi todas ellas, empresas norteamericanas, y que la cuestión que es central para el DUE y se refiere a los requisitos de calidad de la ley funciona de manera diferente con un sistema de protección de la intimidad, como el estadounidense, menos garantista que el del entorno constitucional europeo con la privacidad y sus derechos instrumentales. Los problemas que en su turno se derivan para las empresas tecnológicas están relacionados con las diferentes exigencias que se les dirigen desde cada sistema normativo. Son exigencias que deben cumplir, simultáneamente, sobre la base de soportes de *software* compartidos, y deben hacerlo a la vez que mantienen niveles óptimos de eficiencia de cara a los mercados, en los que compiten y en los que se basa su modelo de negocio.

Es posible que empresas de estos perfiles comerciales no sean las más indicadas para erigirse, o ser erigidas, como garantes interpuestos de bienes constitucionales del calado de todos estos: la privacidad; la protección de datos; la libertad de comunicaciones; los derechos de participación dependientes del

adecuado respeto a los anteriores; las garantías de la opinión pública libre, o la seguridad pública. Pero son esas, las empresas tecnológicas, y sobre todo las grandes plataformas y soportes de *software*, las que verdaderamente están en posición de hacerlo. El edificio en el que alojar todas esas garantías parece estar a medio hacer y no hay otra vía que continuar la construcción. La dimensión transnacional de las empresas tecnológicas es un aspecto fundamental que ha de tenerse en cuenta para perfilar su ascendente posición institucional.

Bibliografía

Allport, F. H. (1937). Toward a science of public opinión. *Public Opinion Quarterly*, 1 (1), 7-23. Disponible en: https://doi.org/10.1086/265034.

Barrio Andrés, M. (2017). *Fundamentos de Derecho de Internet*. Madrid: Centro de Estudios Políticos y Constitucionales.

Berzosa López, D. (2016). *Democracia constitucional y opinión pública*. Cizur Menor: Aranzadi.

Bourdieu, P. (1973). La opinión pública no existe. *Les Temps Modernes*, 318, 1292-1309.

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Standford Law Review Online*, 71-9. Disponible en: https://stanford.io/31zo5By.

De la Torre Forcadell, S. y Cotino Hueso, L. (2002). El caso de los contenidos nazis en Yahoo ante la jurisdicción francesa: un nuevo ejemplo de la problemática de los derechos fundamentales y la territorialidad en internet. *Actas del XV Seminario de Derecho e Informática* (pp. 897-917). Madrid: Aranzadi.

Fernández Rodríguez, J. J. (2004). *Secreto e intervención de las comunicaciones en Internet.* Madrid: Civitas.

—— (2016). Los datos de tráfico de las comunicaciones: en busca de un adecuado régimen jurídico que elimine el riesgo de control permanente. *Revista Española de Derecho Constitucional*, 108, 93-122. Disponible en: http://dx.doi.org/10.18042/cepc/redc.108.03.

González Pascual, M. I. (2014). El TJUE como garante de los derechos de la UE a la luz de la sentencia Digital Rights. *Revista de Derecho Comunitario Europeo*, 49, 943-971. Disponible en: https://bit.ly/35ZV71e.

Habermas, J (1992). *Teoría de la acción comunicativa* (vol. 1). Madrid: Taurus.

—— *Historia y crítica de la opinión pública. La transformación estructural de la vida pública*. Barcelona: Gustavo Gili.

Johnson D. R. y Post, D. G. (1996). Law and borders- The rise of law in Cyberspace. *Stanford Law Review*, 48, 1367-1402. Disponible en: https://doi.org/10.2307/1229390.

Lynskey, O. (2014). The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland. *Common Market Law Review*, 51, 1789-1812.

Martínez Otero, J. M. (2016). Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento. *Revista Española de Derecho Constitucional*, 106, 119-148. Disponible en: http://dx.doi.org/10.18042/cepc/redc.106.03.

Moreno Muñoz, M. (2018). Mediación tecnológica de la interacción social y riesgos de su instrumentalización. El caso de la plataforma Facebook. *Gazeta de Antropología*, 34 (2). Disponible en: https://bit.ly/2W2GIwG.

Muñoz Machado, S. (2000). *La regulación de la red. Poder y Derecho en Internet.* Madrid: Taurus.

Nunziato, D. C. (2009). *Virtual Freedom, Net Neutrality and Free Speech in the Internet Age*. Standford: Standford University Press.

Pauner Chulvi, C. (2018). Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la Red. *Teoría y Realidad Constitucional*, 41, 297-318. Disponible en: https://doi.org/10.5944/trc.41.2018.22123.

Peguera Poch, M. (2007). Solo sé que no sé nada (efectivamente): la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI. *IDP: Revista de Internet, Derecho y Política*, 5. Disponible en: https://bit.ly/361dKld.

Pérez Luño, A. E. (1999). *Derechos humanos, Estado de Derecho y Constitución*. Madrid: Tecnos.

Plaza Penadés, J. (2013). La ley de servicios de la sociedad de la información y comercio electrónico. En J. Plaza Penadés (dir.). *Derecho y nuevas tecnologías de la información y la comunicación* (pp. 43-101). Cizur Menor: Aranzadi.

Pöschl, M. (2015). La garantía de los estándares de derechos humanos y fundamentales ante las nuevas amenazas que generan los particulares y los actores extranjeros. *Teoría y Realidad Constitucional*, 36, 93-130. Disponible en: https://doi.org/10.5944/trc.36.2015.16072.

Rallo, A. (2014). *El derecho al olvido en Internet*, *Google versus España*. Cuadernos y Debates, 233. Madrid: Centro de Estudios Políticos y Constitucionales.

Reidenberg, J. R. (2004). States and internet enforcement. *University of Ottawa Law and Technology Journal*, 1, 213-230.

Rodríguez Ruiz, B. (1998a). *El secreto de las comunicaciones: tecnología e intimidad*. Madrid: McGraw-Hill.

—— (1998b). The right to privacy: a discourse-theoretical approach. *Ratio Juris*, 155-167. Disponible en: https://doi.org/10.1111/1467-9337.00082.

Sánchez Ferro, S. (2018). La alargada sombra del derecho a la protección de datos y otras cuestiones: Reflexiones al hilo del caso Schrems. En A. M. Carmona Contreras (dir.). *Construyendo un estándar europeo de derechos fundamentales* (pp. 87-108). Cizur Menor: Aranzadi.

Solozábal Echevarría, J. J. (1988). Aspectos constitucionales de la libertad de expresión y el derecho a la información. *Revista Española de Derecho Constitucional*, 23, 139-155. Disponible en: https://bit.ly/2oWJ4Bc.

Walton, C. (2010). La opinión pública y la política patológica de la revolución. *Ayer, Revista de Historia Contemporánea*, 80 (4), 21-51. Disponible en: https://bit.ly/35ZW1La.

Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven: Yale University Press.