NOTAS

LA EXTRATERRITORIALIDAD EN LAS COMUNICACIONES DIGITALES Y LAS EMPRESAS TECNOLÓGICAS ANTE EL DERECHO A SU SECRETO: REFLEXIÓN EN TORNO AL CASO *MICROSOFT CORP. VS. UNITED STATES*

Miryam Rodríguez-Izquierdo Serrano
Profesora Titular de Derecho Constitucional
Universidad de Sevilla[1]

Sumario:

I. SECRETO DE LAS COMUNICACIONES E INTERMEDIACIÓN DIGITAL: LA POSICIÓN DE LAS EMPRESAS TECNOLÓGICAS COMO GARANTES DE LA PRIVACIDAD. II. LAS EMPRESAS TECNOLÓGICAS COMO GARANTES DEL SECRETO DE LAS COMUNICACIONES Y EL CASO *MICROSOFT CORP. VS. UNITED STATES*; 2.1. Jurisdicción y protección de información personal en Internet bajo el DUE; 2.2. El caso Microsoft Corp. vs. United States y las garantías del secreto a las comunicaciones digitales ante el juez ordenante. III. REFLEXIÓN FINAL: LAS EMPRESAS TECNOLÓGICAS Y LAS GARANTÍAS DE LA COMUNICACIÓN DIGITAL.

1 El presente trabajo está vinculado al 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 en este trabajo han sido recuperadas en fecha 31-07-2019.

RESUMEN

Las garantías de los derechos relativos a la privacidad en la era de la comunicación digital exigen una coordinación internacional de sistemas normativos territoriales. Las empresas tecnológicas tienen un especial protagonismo en este campo, sobre todo cuando las leyes de diferentes estados funcionan con criterios dispares y sin atender a los efectos de la extraterritorialidad. Es el caso de las garantías del secreto de las comunicaciones en Europa y en Estados Unidos. La problemática se ilustra en este trabajo bajo el pretexto de una revisión del asunto *Microsoft Corp. vs. United States*.

Palabras clave:
Privacidad; secreto de las comunicaciones; Tribunal Supremo de los Estados Unidos; empresas tecnológicas; derecho sobre Internet

ABSTRACT

DIGITAL COMMUNICATIONS EXTRATERRITORIALITY, RIGHT TO PRIVACY AND TECHNOLOGY COMPANIES: A REFLECTION ON MICROSOFT CORP. VS. UNITED STATES

In this Digital-era, privacy rights must be protected through international cooperation, meaning coordination between legal systems. Technology companies are in the middle of this issue, especially when legal rules differ from one state to another disregarding extraterritorial effect. This is the case with confidentiality of communications in the European Union and the United States. This problems is presented in this article through a reflection on the *Microsoft Corp. vs. United States* case.

Key words:
Privacy; confidentiality of communications; USA Supreme Court; technology companies; Internet law.

I. SECRETO DE LAS COMUNICACIONES E INTERMEDIACIÓN DIGITAL: LA POSICIÓN DE LAS EMPRESAS TECNOLÓGICAS COMO GARANTES DE LA PRIVACIDAD.

Cuando se analizan las tensiones que la privacidad y sus derechos instrumentales sufren en la esfera digital, las concepciones que entienden esos derechos como garantías vinculadas a la libre participación política alcanzan una especial relevancia, más allá de la perspectiva individual de los mismos, ligada a la dignidad de toda persona. La intimidad, el derecho nuclear a la vida privada en la terminología del constituyente español, protege el derecho a reservar un ámbito personal del conocimiento ajeno, pero también es una garantía de la libertad general de actuación del ciudadano, incluyendo la libertad para participar en la formación de la voluntad del Estado[2].

La mayor vulnerabilidad de esa garantía, como ocurre en el universo digital, afecta a las condiciones de participación democrática. Las pruebas de ello se encuentran en diversos ejemplos: la preocupación de los gobiernos británico y norteamericano por el filtrado de datos derivado del escándalo de *Cambridge Analytica*[3]; la declaración de nulidad del 58.bis.1 de la reciente reforma de la LOREG por el Tribunal Constitucional español, a instancias del Defensor del Pueblo[4]; o, antes de todo eso, el rechazo de muchos Estados miembros de la Unión Europea a la directiva 2006/24/CE de retención de datos, finalmente invalidada por el TJUE en la sentencia Digital Rights[5]. La privacidad y sus derechos instrumentales son elementos básicos para la libertad individual, subjetiva, y para el mantenimiento de una opinión pública igualmente libre, que se presumen base objetiva para la autonomía política y la participación, de nuevo libre, informada[6].

2 Habría 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". Vid. BLANCA RODRÍGUEZ RUIZ, *El secreto de las comunicaciones: tecnología e intimidad*, McGraw-Hill, Madrid, 1998, p. 26. En el mismo sentido: JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ, *Secreto e intervención de las comunicaciones en Internet*, Civitas, Madrid, 2004, p. 69.

3 Es el nombre de la empresa que se utilizó para obtener datos personales de usuarios de redes sociales y emplearlos para alterar resultados electorales. El asunto llevó al fundador de *Facebook* a comparecer ante el parlamento británico y ante el Congreso de los EEUU. Sobre el escándalo de *Cambridge Analytica* y otros incidentes de filtrado de datos personales en los que *Facebook* se ha visto inmerso, véase el trabajo de MIGUEL MORENO MUÑOZ, "Mediación tecnológica de la interacción social y riesgos de su instrumentalización. El caso de la plataforma *Facebook*", *Gazeta de Antropología*, núm. 34/2, 2018, disponible en http://www.gazeta-antropologia.es/?p=5084.

4 La disposición final tercera de la LOPDyGDD , añadiendo un nuevo artículo 58 bis a la LOREG, quiso permitir a los partidos recabar datos sobre perfiles ideológicos con finalidad electoral. El primer apartado de esa disposición, 58 bis 1, fue recurrido ante el TC, por el Defensor del Pueblo, y declarado inconstitucional y nulo por la STC 76/2019 de 22 de mayo. Las garantías de la ley eran, según el Alto Tribunal, insuficientes teniendo en cuenta el carácter especialmente sensible de los datos personales ideológicos. Subsiste, no obstante, el 58 bis 2 de la LOREG, que permite a los partidos utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral, se entiende que bajo el régimen regular del consentimiento, ya que el Tribunal Constitucional explicó que las tachas formuladas por el Defensor del Pueblo en su recurso se habían limitado al apartado 1 del artículo 58 bis LOREG (FJ 10).

5 Asuntos C-293/12 y C-594/12, *Digital Rights*, STJUE de 8 de abril de 2014. La directiva había sido objeto de controversia e impugnación, directa o indirecta, ante las jurisdicciones constitucionales de diversos Estados miembros: Bulgaria, Alemania, Rumanía, República Checa, Chipre, Polonia, Eslovaquia y Eslovenia. *Cfr.* ORLA LYNSKEY, "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*, núm. 51, 2014, pp. 1789–1812, p. 1799.

6 A pesar de que el modelo de construcción de la opinión pública dominante viene condicionado, desde la segunda mitad del siglo XX, por el predominio en la comunicación pública de la publicidad comercial y de la propaganda, lo cual hace que la libertad que se predica del modelo sea más que discutible. JÜRGEN HABERMAS, *Historia y crítica de la opinión pública. La transformación estructural de la vida pública*, Gustavo Gili, Barcelona, 2002, p. 221. En la era digital, la *viralización* de noticias falsas y la elaboración de perfiles para asegurar el impacto de los mensajes comerciales y propagandísticos acentúan los problemas de libertad, ya en el nuevo modelo. CRISTINA PAUNER CHULVI, "Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la Red", *Teoría y Realidad Constitucional*, núm. 41, 2018, pp. 297-318, p. 302 y ss.

Pero los ejemplos citados dan cuenta de algo más: la especial posición que las empresas tecnológicas, proveedores de servicios, redes sociales, motores de búsqueda y demás[7], ostentan en relación con el tratamiento de datos de carácter personal, con la garantía del secreto de las comunicaciones y, en definitiva, con la dimensión privada de la vida del ciudadano en la era de la comunicación digital. Por una parte esas empresas son garantes de la privacidad del individuo-usuario, pues en la medida en que se nutren de datos sobre sus intereses, gustos, ubicación o preferencias, deben cumplir con las obligaciones de cuidado que les adjudica la legislación, especialmente la de la Unión Europea. Por otra parte, y en la misma medida en que comercian con tales datos, esas corporaciones ponen en constante riesgo los ámbitos de lo privado[8].

Desde el Derecho de la Unión Europea puede afirmarse que esas empresas ostentan una cierta posición institucional y que tal posición bien puede calificarse como ascendente, pues el DUE atribuye a los operadores de servicios obligaciones de custodia y protección de derechos fundamentales. Al mismo tiempo, las autoridades supranacionales las implican, y cada vez con mayor intensidad, en la definición de las políticas públicas y de las regulaciones que atañen a su posición y a sus funciones mediadoras[9].

El deber de cuidado que vincula a las empresas tecnológicas con la información personal que recopilan se explica, al menos, por tres razones distintas: una comercial, otra jurídica y otra política. La primera, comercial, es que han de mantener la confianza de los usuarios, de la que depende su actividad y existencia. La segunda, jurídica, es que deben cumplir con las obligaciones y límites que les imponen las leyes regulatorias, evitando sanciones de diferente coste económico y social. La tercera, política, es realizar la función colaborativa que el mercado y el Estado les otorgan, al no ser capaces estos por sí mismos, ni uno ni otro y mucho menos el segundo, de facilitar y ordenar un flujo de interacción e información personal de tamaño volumen, densidad y valor[10].

Las empresas tecnológicas se han transformado, así, en una suerte de agentes no gubernamentales, mediadores entre ciudadanía, mercado y Estado. Dicho rol intermediario, si bien tiene el coste de anudar a estas empresas al cumplimiento de una regulación, y autorregulación forzosa, cada vez más meticulosa, les sirve para retroalimentar su misión comercial, la originaria, de conseguir usuarios, afiliados, público al fin y al cabo, dispuestos a facilitar sus datos personales y a interactuar, dejando rastros aprovechables para fines estadísticos, propagandísticos y de ventas[11]. Desde esa perspectiva, las tecnológicas serían entes a los que se pone a cargo de garantizar las condiciones de la seguridad en la red y, con ellas, el libre mercado y el ejercicio de los derechos que se proyectan en Internet[12]. Los deberes de garantía serían, pues, una

7 Una clasificación y análisis de proveedores de servicios de Internet, reconociendo no agotar las posibilidades presentes y futuras de creación de otros modelos de intermediarios en la difusión de contenidos, puede consultarse en el trabajo de MOISÉS BARRIO ANDRÉS, *Fundamentos de Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2017, pp. 345 y ss.

8 Las empresas tecnológicas, en relación con el tratamiento de información personal, son percibidas desde hace tiempo como amenazas potenciales para la privacidad. Estas reflexiones se apoyan en las de MAGDALENA PÖSCHL, "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*, núm. 36, 2015, pp. 93-130, p. 94 y pp. 106-107.

9 El ejemplo es cómo se han implicado en el plan de la Comisión Europea contra la desinformación, siendo las redes sociales *Facebook* y *Twitter* y el motor de búsqueda Google las principales invitadas a participar en él. Véase la 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://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation. Los informes de esas empresas en lo relativo al seguimiento del plan de la Comisión se pueden consultar en https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation

10 Explica Magdalena Pöschl 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", vid. MAGDALENA PÖSCHL, "La garantía de los estándares…, *op. cit.*, p. 107.

11 Como ya se ha dicho, 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. Vid. MIGUEL MORENO MUÑOZ, "Mediación tecnológica de la interacción…, *op. cit.*, apartado 7.

12 Situándose 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. Sobre la relación entre protección de la intimidad y garantías constitucionales en el marco de las teorías del discurso, véase el trabajo de BLANCA RODRÍGUEZ RUIZ, "The right to privacy: a discourse-theoretical approach", *Ratio Juris*, 1998, pp. 155-167.

imposición a cuenta de los beneficios que las empresas obtienen, pero también la única manera que los poderes públicos tendrían para asegurar condiciones mínimas de seguridad y libertad, en la red y en relación con la información personal.

II. LAS EMPRESAS TECNOLÓGICAS COMO GARANTES DEL SECRETO DE LAS COMUNICACIONES Y EL CASO MICROSOFT CORP. VS. UNITED STATES

Una vez esbozada, en un plano abstracto, la posición intermediaria de las empresas tecnológicas, esta reflexión se propone partir de ella para escrutar el papel que esas entidades tienen en relación con las garantías del secreto de las comunicaciones. Para ello, y en concreto, la propuesta plantea descender al plano fáctico con el caso *Microsoft Corp. vs. United States* 584 U. S. (2018)[13]. El caso gira en torno a la autorización judicial exigida, en Estados Unidos, para la intervención gubernamental sobre el secreto de comunicaciones efectuadas desde servidores ubicados en Europa. El dilema es cómo deben responder ante una orden judicial, en tales situaciones, las empresas tecnológicas que prestan servicios en distintos puntos del globo. Y la cuestión hace confluir, por tanto, una doble perspectiva: la del alcance de una orden o autorización judicial, estatal, de intervención en las comunicaciones y la de la vinculación a las mismas de los operadores de comunicaciones transnacionales.

2.1. Jurisdicción y protección de información personal en Internet bajo el DUE.

Desde la perspectiva de la garantía judicial, la autorización requerida para la intervención en el secreto de las comunicaciones tiene una dimensión innegablemente formal, pero también una dimensión sustantiva. Esto se comprueba, en Europa, al indagar en los diferentes requisitos materiales que la jurisprudencia del TEDH ha establecido para que las exigencias de la garantía formal queden satisfechas[14]. No obstante, también es cierto que esas exigencias materiales, que se superponen sobre la exigencia formal, que es la existencia de autorización, pueden variar de una jurisdicción estatal a otra. Si bien en el ámbito del Convenio y de la Unión Europea la uniformidad es considerable, los parámetros de adecuación constitucional pueden diferir al confrontarlas con las de otros estados.

Desde la perspectiva de las empresas tecnológicas, las indiscutibles exigencias formales y sustantivas de su posición intermediaria también pueden ser variables en función de la ubicación territorial de los servicios que presten[15]. Esto significa que también las que rodeen a una autorización judicial podrán proyectarse sobre estas entidades comerciales, de manera que puedan ser discutidas por las mismas ante la autoridad judicial, incluso oponiéndose a ellas, en caso de que no respondan a los parámetros de constitucionalidad establecidos.

Pues bien, el caso *Microsoft* plantea, en efecto, esa problemática. Las grandes corporaciones, responsables del alojamiento de datos y contenidos digitales protegidos por la privacidad y el secreto de comunicaciones, se van a enfrentar a ella en la medida en que su estructura empresarial las ponga ante un conflicto de jurisdicciones: en el caso que aquí se estudia una europea, la irlandesa, frente a la remitente de la orden, estadounidense.

Aunque las circunstancias del caso se relatarán más adelante, este breve avance pone de relieve la incidencia de la extraterritorialidad como causa de conflicto. Internet es global. Las empresas tecnológicas más relevantes tienen establecimientos comerciales en muchas partes del planeta. Pero las jurisdicciones

13 La información sobre el caso está disponible en https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html.

14 *Cfr.* BLANCA RODRÍGUEZ RUIZ, *El secreto de las comunicaciones…, op. cit.*, p. 102.

15 El secreto de las comunicaciones "es objeto de estricta protección en el contexto de los servicios que las llevan a cabo" y se aplica frente a estos servicios, sobre todo si se tiene en cuenta la dimensión participativa del derecho. Vid. BLANCA RODRÍGUEZ RUIZ, *El secreto de las comunicaciones…, op. cit.*, pp. 124 y 174.

de los Estados siguen sometidas a una poco permeable dimensión territorial[16]. Con este escenario, y en un primer momento, algunos conflictos planteados ante tribunales de lugares distintos, tanto distintos de aquellos en los que se alojaban los contenidos lesivos como de aquellos en los que se había producido la afectación a bienes jurídicos protegidos[17], hicieron pensar que Internet, dada su configuración tecnológica, acabaría provocando una cierta uniformidad en el entendimiento de los derechos y su ejercicio en su esfera[18]. Sin embargo, tras casi tres décadas de desarrollo de la comunicación digital, lo que ha ocurrido ha sido lo contrario.

Las leyes aplicables a Internet, y en consecuencia a las empresas tecnológicas, varían de un lugar a otro del planeta[19]. La defensa de los derechos fundamentales que se ejercen en la red lo hace, también, en función de las culturas constitucionales de esas distintas jurisdicciones[20]. Podría decirse que los Estados miembros de la Unión Europea son los que, por razón de su pertenencia a esta, comparten un grado alto de homogeneidad y coordinación en estas cuestiones. Lo hacen, no obstante, sin dejar de sostener tal regulación sobre una concepción basada, en última instancia, en clave de soberanía y, en primera instancia, en clave de mercado.

Como consecuencia, y más allá del ámbito de la UE, las empresas tecnológicas se someten a diferentes regulaciones de manera simultánea, 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. En su funcionamiento, sin embargo, hay una sensación, si no una realidad, de ubicuidad y en cualquier caso los operadores necesitan asegurar la fluidez en el intercambio de datos, dándose efectivas transferencias de unos puntos geográficos a otros. Esas transferencias, como es lógico, no son libres y con carácter general han de contar con el consentimiento del afectado, titular de los datos o emisor de los contenidos de la comunicación privada. También vendrán condicionadas por requisitos legales de distinto signo en función de los lugares de origen y destino de los datos y mensajes.

En el DUE, las transferencias internacionales de datos están determinadas por el Reglamento de protección de datos en sus artículos 44 y siguientes. En líneas generales son transferencias no permitidas[21]. Partiendo de tal premisa, el Reglamento habilita procedimientos, en los que intervienen tanto instancias europeas como autoridades estatales de protección de datos, encaminados a la adopción de cláusulas

16 Ya a principios de siglo se planteaba esta cuestión en SANTIAGO MUÑOZ MACHADO, *La regulación de la red. Poder y Derecho en Internet*, Taurus, Madrid, 2000, p. 65.

17 *Cfr.* SONIA DE LA TORRE FORCADELL y LORENZO COTINO HUESO, "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*, Aranzadi, Madrid, 2002, pp. 897-917.

18 En un momento inicial, algunos estudiosos de la comunicación en la red abogaron abiertamente por dejar que Internet fuera un espacio exento de intervención estatal y solo controlado por el código -DAVID R. JOHNSON y DAVID G. POST, "Law and borders- The rise of law in Cyberspace", *Stanford Law Review*, núm. 48, 1996, 1367-1402; JOHNATHAN ZITTRAIN, *The future of the Internet and how to stop it*, Yale University Press, New Haven&London, 2008, pp. 173 y 174; DAWN C. NUNZIATO, *Virtual Freedom, Net Neutrality and Free Speech in the Internet Age*, Standford University Press, Standford, California, 2009.

19 Las visiones regulativas sobre Internet, defensoras de la competencia de los Estados para normar el uso de Internet, se fueron imponiendo frente a autores que postulaban a favor de la creación de cooperación entre Estados para resolver cuestiones relativas a Internet, como Santiago Muñoz Machado, *La regulación de la red… op. cit.* p. 65. A favor de la recuperación del poder soberano de los Estados sobre la red, incluso usando estos la tecnología para controlarla, véase el trabajo de Joel R. Reidenberg, "States and Internet enforcement", *University of Ottawa Law & Technology Journal*, Vol. 1, 2004, pp. 213-230.

20 Significativos fueron los casos en torno a la libertad de expresión, en conflicto con el derecho al honor, juzgados por tribunales británicos cuyas sentencias se negaron a ejecutar los tribunales estadounidenses apelando a la Primera Enmienda de su Constitución. *Cfr.* STEPHEN BATES, "Libel Capital No More? Reforming British Defamation Law", *Hastings Communication & Entertainment Law Journal*, núm. 34, 2012, pp. 233-274, p. 267. En defensa de la Primera Enmienda, y temiendo que Internet amenazase su sistema de libertad de expresión, se aprobó una ley que impedía la ejecución en Estados Unidos de sentencias de tribunales extranjeros que no cumplieran con los estándares de la Primera Enmienda. Se trata de la Securing the protection of our enduring and established constitutional heritage act (Speech Act), PL 111-223, August 10, 2010, 124 Stat 2380.

21 Es un régimen similar al anteriormente dispuesto en la Directiva 95/46/CE, y que se resume en Susana Sánchez Ferro, "La alargada sombra del derecho a la protección de datos y otras cuestiones: Reflexiones al hilo del caso Schrems" en ANA MARÍA CARMONA CONTRERAS (dir.), *Construyendo un estándar europeo de derechos fundamentales*, Aranzadi, Cizur Menor, 2018, pp. 87-108, pp. 89 y ss.

contractuales-tipo. Se trata de cláusulas a utilizar con terceros para que las transferencias de datos sean lícitas. También indica el Reglamento procedimientos, semejantes a las anteriores, de aprobación de normas corporativas, vinculantes e internas a las empresas que vayan a transferir datos fuera de la Unión. Esto hace posible las transferencias 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. Se trata, sin duda, de una proyección extraterritorial de las garantías ofrecidas por la regulación del DUE. En ausencia de decisión de adecuación, sin el visto bueno de la Comisión al fin y al cabo, 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 en relación con las garantías que los afectados van a poder activar sobre los datos transferidos.

Ese detallado y estricto marco regulativo que el DUE establece para las empresas responsables de datos, cuando pretendan sacarlos de su jurisdicción, puede modularse conforme a lo estipulado en el artículo 49 del Reglamento. Esa disposición recoge razones, excepciones, por las cuales se pueden transferir datos al extranjero fuera de ese marco, casi todas considerando lo que pueden ser beneficios para el interesado. Pero el interés público del país tercero, y por lo tanto la colaboración con la justicia de un Estado no miembro de la Unión, es también potencial causa de una excepción según el 49.1. d).

Esto no quiere decir que una petición de colaboración con la seguridad de un Estado tercero libere datos de procedencia europea sin la debida garantía o que esa garantía pueda ser medida conforme a los parámetros del Estado de destino. Así, el artículo 48 del Reglamento estipula que si se trata de ejecutar un mandato judicial exterior a la Unión, será necesario un tratado de asistencia jurídica mutua vigente entre ese país y la UE. En defecto de tratado, el último inciso de ese artículo indica que la transferencia puede hacerse por "otros motivos (…) al amparo de este capítulo", lo que 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 conforme al artículo 49. Pero la interpretación de este inciso no resulta del todo clara, pues la excepción del artículo 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. Se trataría, por tanto, de una vigilancia continua sobre los datos, también los de las comunicaciones, salidos de la Unión hacia un tercer territorio.

2.2. El caso Microsoft Corp. vs. United States y las garantías del secreto a las comunicaciones digitales ante el juez ordenante.

Las condiciones en las que datos custodiados en territorio de Estados de la UE pueden transferirse, y cuáles podrían aportarse, o no, a requerimiento de una instancia judicial de un país tercero, tienen resonancia singular en esta reflexión, pues sitúan normativamente el conflicto de origen en el caso *Microsoft Corp. vs. United States*[22]. Por así decir, este caso evidencia el choque de dos pretensiones de extraterritorialidad contradictorias, la europea y la estadounidense. Con ello, pone en cuestión tanto la eficacia del sistema europeo de garantía de la privacidad y el secreto de las comunicaciones, como la utilidad de los mecanismos estadounidenses de cooperación con la justicia para la persecución del delito.

También propicia una reflexión sobre las dificultades de articular garantías de privacidad y seguridad en Internet. Por una parte son precisas garantías para los derechos de los titulares de los datos y actores de las comunicaciones en red. Por otra parte estas garantías han de ser flexibles en situaciones en las que la

22 Las circunstancias del mismo no dejan de estar conectadas con las decisiones de la Comisión Europea sobre la adecuación de las garantías de la privacidad para la transferencia de datos a Estados Unidos. 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 http://www.europarl.europa.eu/doceo/document/B-8-2018-0305_ES.html.

seguridad pública así lo requiriera. La seguridad pública, en nuestros días, no es solo seguridad dentro del Estado, pues muchas amenazas a esa seguridad pública son transnacionales. Si alcanzar ese equilibrio ya es trabajoso en el contexto de una jurisdicción estatal, propiciarlo mínimamente en el contexto del intercambio de datos e información entre jurisdicciones diversas lo es más aún. Véase a través de la exposición del caso.

Elevado a conocimiento del Tribunal Supremo de los Estados Unidos, *Microsoft Corp. vs. United States* versaba sobre un conflicto entre esa empresa tecnológica y el gobierno de aquel país. La causa del conflicto era un juicio penal, a un usuario de servicios de *Microsoft*, 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 la empresa tenía en Dublín. La empresa replicó que la orden judicial, basada en la *Stored Communications Act*, proveniente de la *Electronic Communications Privacy Act* de 1986, no era óptima y que el juez no era competente para emitir esa orden, por ser extraterritorial.

La empresa apeló contra la orden y esta fue revocada. Fue el tribunal del Segundo Circuito el que admitió que había una aplicación extraterritorial de la SCA, confirmando que la territorialidad superpuesta al volátil universo digital rige sobre el mismo. Tras la decisión del Segundo Circuito, el gobierno de los EEUU apeló al Tribunal Supremo y este se hizo cargo del caso en 2016. Ante el Supremo, Microsoft alegó de nuevo que los correos requeridos estaban bajo jurisdicción irlandesa, pues el servidor allí se ubicaba. Conforme al DUE, sostuvo Microsoft, era necesario un acuerdo de asistencia jurídica mutua, por más que la empresa raíz tuviera su sede en territorio estadounidense y, por tanto, sometida a su jurisdicción. Dicho en otras palabras, la ley que regulaba la cesión de esos datos, aun por motivos de seguridad o de investigación del delito, no era *exclusivamente* la de aquel país.

Antes de que el Tribunal Supremo entrase a resolver el conflicto, el Congreso optó por reformar la *Stored Communications Act* en marzo de 2018. Lo hizo a través de la llamada *CLOUD Act, Clarifying Lawfull Overseas Use of Data Act*. Como consecuencia de la reforma, se emitió una nueva orden y el caso quedó sobreseído, por irrelevante. Finalmente fue devuelto al juez de apelación[23]. Ese fin anticipado tuvo el siguiente fundamento: la reforma derivada de la *CLOUD Act* estableció, con una claridad que no figuraba en la ley a la que sustituía, 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 dónde se encontraran estos.

La dimensión extraterritorial del mandato, por tanto, no se eliminaba. Al contrario, quedaba confirmada. No obstante, la ley estadounidense tampoco fue ciega a los inconvenientes que planteaba su pretendida eficacia extraterritorial. Por ello, su redacción final permitió cierta ponderación, a realizar por el juez, sin mayor especificación, cuando la empresa requerida tuviera los servidores señalados en territorios en los que las condiciones legales supusieran que, para cumplir con la justicia estadounidense, hubiera que infringir la ley de ese otro lugar[24].

Aun insistiendo en que las empresas tecnológicas bajo su jurisdicción tienen deberes de colaboración con la seguridad interna, reafirmando la proyección territorial de la jurisdicción estadounidense sobre el uso de Internet, esa concesión que la *CLOUD Act* hace ante datos alojados en servidores externos demuestra algo importante. El sistema estadounidense es consciente de la necesidad de una colaboración por el bien de los usuarios, por el de los negocios de las empresas tecnológicas y, en última instancia, por el de la seguridad jurídica. Solo mediante la articulación de mecanismos de cooperación entre Estados y empresas tecnológicas se va a poder alcanzar un, necesario, estándar común de seguridad y garantías sustantivas para la privacidad y la comunicación en la red. El problema que se plantea, a partir de ahí, es que ese estándar sea aceptable para los distintos actores implicados, Estados y corporaciones empresariales, y a la vez respetuoso con los derechos de los ciudadanos afectados.

23 Resume el caso en su primera parte el artículo de JENNIFER DASKAL, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0", *Standford Law Review Online*, núm. 71/9, 2018, disponible en https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

24 En la segunda parte del trabajo de JENNIFER DASKAL, "Microsoft Ireland, the CLOUD Act, and.., *op. cit.*

III. REFLEXIÓN FINAL: LAS EMPRESAS TECNOLÓGICAS Y LAS GARANTÍAS DE LA COMUNICACIÓN DIGITAL.

Del asunto *Microsoft Corp. vs. United States* se deduce que las garantías de la comunicación digital exigen una coordinación de sistemas normativos territoriales y que las empresas tecnológicas, aun cuando las leyes de los EEUU no les confieren obligaciones de custodia de la privacidad tan meticulosas como las de la UE, tienen un especial protagonismo en este campo. Si la inicial deslocalización jurisdiccional de Internet dio paso a su progresivo desarrollo territorial estatal, regional en el caso de Europa, de la regulación aplicable a su uso, el momento actual se presenta como el de la necesaria coordinación de sistemas de garantía.

Si esa coordinación no se alcanza, para el sistema europeo de protección de la intimidad digital, datos y comunicaciones, se derivarían dos tipos de problemas: uno relacionado con la efectiva y mayoritaria nacionalidad estadounidense de las tecnológicas más relevantes; otro, en conexión con el anterior, relacionado con la pérdida de eficacia real de garantías tan construidas como la relativa a los requisitos de calidad de la ley restrictiva de derechos de privacidad, como es la de la intervención judicial de las comunicaciones. Si la privacidad se entiende de manera diferente en el orden constitucional estadounidense, menos garantista, cuando las empresas tecnológicas han de responder ante las autoridades estadounidenses y también ante las europeas, y si también las condiciones de los respectivos mercados son distintas, finalmente podría ser que tales condiciones comerciales, y no los derechos, sean las que acaben por fijar las garantías de la intimidad, del secreto de las comunicaciones y de la protección de la información personal. Ese es el riesgo para estos derechos fundamentales.