LA PROTECCIÓN DE TRANSMISIONES DE DATOS TRANSFRONTERIZAS, E. RODRÍGUEZ PINEAU Y E. TORRALBA MENDIOLA (DIRS.),
THOMSON REUTERS ARANZADI, MADRID, 2021,
ISBN: 978-84-1391-290-5,
pp. 33-76.

PROTECCIÓN DE DATOS EN LA ECONOMÍA DIGITAL
UNA APROXIMACIÓN DESDE LA REGULACIÓN DEL COMERCIO INTERNACIONAL

Carmen OTERO GARCÍA-CASTRILLÓN*

I. INTRODUCCIÓN

En la economía digital[1] son cada vez más numerosas las operaciones comerciales que llevan aparejada la transferencia de datos que pueden ser recogidos, procesados y almacenados en distintos países. El peso económico de estas transacciones internacionales se ha incrementado hasta el punto de que, en 2015, el valor del intercambio de datos transfronterizos superó al del comercio de mercancías[2]. Con carácter general, los datos intercambiados pueden encuadrarse en las categorías de *big data* o en la de datos personales. Sin perjuicio de ciertas dificultades de calificación, mientras los primeros no se refieren necesariamente a un individuo específico, los segundos sí[3]. Además de atender a las dificultades para determinar el régimen jurídico aplicable a la protección de los datos personales en el tráfico transfronterizo[4], la seguridad jurídica de

* Catedrática de Derecho internacional privado en la Universidad Complutense de Madrid (cocastri@der.ucm.es).

[1] TAPSCOTT, D., *La Economía Digital: Promesa y peligro en la Era de la Inteligencia en redes*, 1995. La economía digital se entiende como una nueva forma de producción y consumo que resulta de un proceso complejo de cambios en la organización social, económica y política de los países. La economía digital se constituye como un ecosistema en el que convergen la infraestructura de las redes de comunicación, los servicios de procesamiento y las tecnologías web, y los usuarios finales (individuos, empresas, gobierno). El nivel de avance de cada país se define por el grado de desarrollo y complementación de estos componentes, UN.CEPAL *Economía Digital para el cambio estructural y la igualdad*. CEPAL, 2013, p. 9.

[2] MANYIKA, J., LUND, S., BUGHIN, J.,WOETZEL, J., STAMENOV, K. y DHINGRA, D. *Digital globalization: The new era of global flows*, Report, 24.2.2016, McKingsey Digital, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

[3] Los datos generados automáticamente para procesos industriales y no directamente por las personas, con información personal relativa a los mismos o que permita su identificación, forman parte del *big.data*. En todo caso, puede resultar dudosa la consideración de las "huellas" o datos anónimos. Sobre su calificación en la UE, *vid*. FINK, M. y PALLAS, M. "They who must not be identified - distinguishing personal from non-personal data under the GDPR", *International Data Privacy Law*, 2020, vol. 10 núm. 1, pp. 11-36.

[4] OCDE *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 11.7.2013, ("Privacy Guidelines"), revisa la versión original de 1980; para. 22 señala la problemática y recomienda a los Estados que trabajen para resolverla, tanto en lo que concierne a

los operadores económicos e incluso la propia materialización y continuidad de las transacciones internacionales requieren adentrarse en la situación normativa actual en lo que concierne al comercio internacional en el que se ven involucrados estos datos y que, mayoritariamente, se sitúa en la esfera de acción de internet, dentro del llamado comercio digital, que incluye el electrónico[5].

Resulta evidente que la protección de datos y el comercio de bienes y servicios están directamente relacionados. Las empresas recogen, procesan, utilizan, almacenan, transfieren volúmenes de datos personales que sirven para llevar a cabo transacciones y para identificar preferencias, conocer historias y perfiles médicos, financieros etc. de consumidores y de mercados nacionales a los que pretenden acceder o en los que tienen intención de posicionarse. Las transferencias internacionales pueden tener lugar entre distintas empresas o dentro de un mismo grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta[6].

Demasiada protección de estos datos puede restringir excesivamente el comercio transfronterizo en todos los países, incluidos los que se encuentran en desarrollo. No puede perderse de vista que internet está considerado como un instrumento que permite el crecimiento de la riqueza al margen de factores territoriales y promueve el desarrollo sostenible y la emancipación de quienes viven en áreas del planeta menos favorecidas socio-económicamente. Por otra parte, poca protección puede afectar a los derechos fundamentales de los individuos y a la confianza de los consumidores, perjudicando igualmente el comercio internacional. Por lo tanto, debe encontrarse un equilibrio adecuado entre la movilidad internacional de estos datos en el tráfico comercial y su protección.

De entrada, se observa que la existencia de normas internacionales específicas en materia de protección de datos es escasa. No puede perderse de vista que, en sistemas jurídicos de nuestro entorno, los datos personales y su protección se conciben como un derecho fundamental en sí mismo mientras que, en otros, aunque se sitúe en el marco del respeto a la privacidad del individuo como derecho fundamental, se asocia esencialmente a la protección de los consumidores. En esta línea, aunque con distintos alcances, se viene imponiendo el concepto de soberanía digital, de internet o ciber-soberanía (*Digital, Internet o Cyber Sovereignty*), reivindicando así la autoridad de los Estados para regular y mantener estándares propios en sus territorios, conforme a sus concepciones particulares, en lo que concierne a las actuaciones en la red de redes.

Por otro lado, como es sabido, la Organización Mundial del Comercio (OMC) gestiona distintos Acuerdos que, básicamente, liberalizan el comercio internacional de mercancías y de servicios a escala multilateral contando, además, con un sistema propio

---

la competencia judicial internacional como a la ley aplicable. En este sentido, el informe explicativo indica que, dadas las dificultades, se resolvió no proponer soluciones específicas en este instrumento; paras. 74-76,https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum, visitado en julio 2021. No obstante, en relación con la ley aplicable *vid.* notas 28, 111 y para. 51.

[5] El comercio digital abarca las transacciones digitales de bienes y servicios que pueden entregarse de manera digital o física, lo que comprende las transacciones de comercio electrónico, incluyendo los servicios prestados de manera digital, independientemente del medio por el que se soliciten. La comunidad internacional de estadística utiliza actualmente ésta categorización para medir este comercio y la contribución de la transformación digital al producto interior bruto (PIB). *Panorama del comercio electrónico: políticas, tendencias y modelos de negocio*; OCDE, 2019, pp.18 y 25.

[6] Así lo describe expresamente el art. 4.20 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, DOUE L 119 de 4 de mayo de 2016 (en adelante, RGPD).

de solución de diferencias[7]. Con este modelo como referencia, pero a escala bilateral y regional, los Estados Unidos (EE.UU.) y la Unión Europea (UE) encabezan – cuando no lideran- la firma de acuerdos internacionales para la liberalización de intercambios comerciales en los que ha empezado a incorporarse la protección de datos y de la privacidad. Recientemente, esta cuestión se ha incorporado también a las negociaciones comerciales multilaterales.

El debate se polariza entre el proteccionismo y el liberalismo económicos, en el que el reto es encontrar un equilibrio que permita garantizar el respeto a objetivos nacionales de políticas públicas, como la protección de la privacidad, y, al mismo tiempo, preservar los beneficios del comercio digital; de naturaleza abierta y global. En palabras del Reglamento (UE) 2016/679 sobre protección de datos (RGPD); "(L)os flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal"[8].

Este trabajo pretende presentar la situación del régimen jurídico internacional de las transacciones comerciales en este ámbito, tanto desde una perspectiva multilateral como regional, con especial atención a la posición de la UE y sus relaciones con terceros entre los que, desde enero del 2020, se encuentra el Reino Unido[9]. Partiendo de los asuntos *Schrems*, se observará la forma en la que normas internas de protección de datos, en este caso las de la UE (de notoria influencia a escala internacional[10]), se conectan con la regulación del comercio internacional y se apreciará su interacción con el régimen regional y multilateral del comercio internacional, que tratan de abordar la problemática planteada.

II. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y ASUNTOS *SCHREMS*: RESTRICCIONES AL COMERCIO INTERNACIONAL

En el asunto *Schrems II*, el Tribunal de Justicia de la Unión Europea (TJUE)[11] declaró la invalidez, conforme al Derecho de la UE (DUE), de la Decisión de la Comisión 2016/1250 sobre la adecuación de la protección del Escudo de la Privacidad (*privacy shield*) UE – EE.UU.[12], cuyo objeto era permitir la transferencia de datos personales a este tercer país conforme a las exigencias establecidas en la normativa comunitaria en la

[7] https://www.wto.org/. Visitado en julio 2021.

[8] Considerando 101 del RGPD, nota 6.

[9] El período transitorio concluyó el 31.12.2020. Los datos, transmitidos o procesados en el Reino Unido antes de esta fecha relativos a individuos localizados fuera de este país; así como los realizados después sobre la base del Acuerdo de Retirada (art. 7.1), continuaron siendo tratados conforme al Reglamento. *Notice to Stakeholders; Withdrawal of the UK and EU Rules in the Field of Data Protection*, Brussels, 6 July 2020 REV1.

[10] BRADFORD, A. *Brussels Effect,; How the European Union Rules The World*, OUP, 2019.

[11] Sentencia del TJUE de 16 de julio de 2020, *Data Protection Commissioner/Maximillian Schrems y Facebook Ireland; (Schrems II)*, C-311/18, ECLI:EU:C:2020:559. En consecuencia, el 14.12.2020, el TJUE dictó auto de sobreseimiento en el asunto T-738/16, *La cuadrature du net*, ECLI:EU:T:2020:638, en el que se planteaba expresamente su compatibilidad con la CDFUE. En la misma línea, el 8.9.2020, la *Federal Data Protection and Information Commissioner* (FDPIC) suiza, estableció la contrariedad del *Swiss-U.S. Privacy Shield Framework* con la Ley federal suiza de protección de datos (FADP) por no dar un nivel de protección adecuado a las transferencias de datos desde Suiza a EE.UU. https://www.edoeb.admin.ch/edoeb/en/home/latest-news/media/medienmitteilungen.msg-id-80318.html. Visitado en julio 2021.

[12] Decisión de ejecución 2016/1250 de la Comisión, de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU, DO, L 209 de 1.8.2016.

materia, entonces la Directiva 95/46 y, desde el 25 de mayo de 2018, el RGPD[13]. No obstante, la Decisión 2010/87 de la Comisión, relativa a la autorización de dichas transferencias mediante la inclusión de cláusulas contractuales tipo que obligan a los encargados del tratamiento establecidos en terceros países[14], fue declarada conforme con dicha normativa[15].

En síntesis, para las transferencias de datos personales a terceros países, el DUE requiere que éstos garanticen un nivel de protección adecuado (*adequacy finding*); esto es, "sustancialmente equivalente" al que se ofrece en la UE, "interpretado a la luz de la Carta de los Derechos Fundamentales"[16] para evitar así su traslado a países "refugio de datos", con menor nivel de protección (*data havens*). Como es sabido, la protección de datos personales es proclamada como derecho fundamental en la Carta de los Derechos Fundamentales de la UE (CDFUE, art. 8)[17] así como considerada parte del contenido del derecho a la vida privada y familiar en el Convenio Europeo de Derechos Humanos y Libertados Fundamentales (CEDH, art. 8) sobre el que existe una abundante jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH)[18].

---

[13] Título V del RGPD, nota 6, regula el flujo de datos fuera del Espacio Económico Europeo (EEE), que extiende el mercado interior a los países de la Asociación Europea de Libre Comercio (AELC-EFTA); Islandia, Liechtenstein y Noruega. El art. 44 señala como principio general "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

[14] Decisión 2010/87 UE de la Comisión, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, DOUE L 39, 12.2.2010.

[15] La Decisión 2021/914 UE de la Comisión, de 4 de junio de 2021, DOUE L 199, 7.6.2021, deroga la Decisión 2010/87 UE a partir del 27.9.2021, fijando un período transitorio de 15 meses en el que las cláusulas contractuales conforme con la Decisión derogada podrán continuar utilizándose bajo ciertas condiciones (art. 4). El mismo día, la Comisión adoptó la Decisión 2021/915 UE, relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el art.28.7, del RGPD y en el art. 29.7 del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

[16] Sentencia TJUE *Schrems II*, paras. 94 y 105.

[17] Así como en algunas constituciones nacionales, como en el caso de la española (art. 18).

[18] Partiendo de la sentencia del TEDH (Gran Sala) de 4.12.2008, *S. and Marper v. United Kingdom*, en la que se reconoce que "…para determinar si la información personal retenida por las autoridades implica cualquier .. (aspecto) de la vida privada, …, el Tribunal prestará debida atención al contexto específico en el que ha sido grabada y retenida, la naturaleza del expediente, la forma en que se utiliza y se procesa y los resultados que pueden ser obtenidos ...". La doctrina del TEDH ha establecido que el respeto a la vida privada y familiar resulta infringido cuando se accede o se utilizan datos de un individuo sin su consentimiento salvo si este uso está amparado por la ley y, además, resulta necesario y proporcional al objetivo perseguido y se ha garantizado al interesado la oportunidad de obtener revisión judicial de la actuación. Sentencia del TEDH (Sección Quinta) de 8.2.2018, *Ben Faiza v. France*. Recientemente, en *Centrum För Rättvisa v. Sweden* y *Big Brother Watch and Others v. the United Kingdom*, con sentencias (Gran Sala) de 21.06.2021 en las que se estableció la existencia de sendas violaciones del art. 8, el Tribunal ha desarrollado este test en lo que concierne a los sistemas de intercepción masiva de datos: 1.la norma interna debe señalar con suficiente claridad y detalle los casos en los que cabe autorizar la intercepción de los datos y de las comunicaciones; 2.dado el riesgo de abuso y la legitimidad del secreto, la supervisión y de la revisión debe ser mayor; 3.debe tenerse en cuenta el grado de intromisión en los derechos de los individuos durante las distintas fases de intercepción y análisis de los datos, de forma que las necesidad de las salvaguardas va incrementándose progresivamente y, por lo tanto, en cada fase debe hacerse una evaluación de la necesidad y proporcionalidad de la medida; 4.la intercepción de los datos debe estar sujeta

A estos efectos la Comisión Europea puede, bien realizar una constatación de adecuación a la vista de la legislación interna o concertando acuerdos internacionales con el Estado en cuestión (art. 45 RGPD; base para la Decisión sobre el escudo de privacidad con EE.UU), o bien, reconociendo expresamente la importancia que el sector privado tiene en este ámbito, aprobar la suficiencia de cláusulas tipo que habrán de ser incorporadas en los contratos en los que participa el exportador comunitario de datos, siempre que se reconozcan a su titular los derechos y acciones legales para reclamarlos (art. 46.1 y 2.c del RGPD; base para la Decisión sobre cláusulas contractuales). Según indica la Comisión, esta es la herramienta para la trasferencia de datos más utilizada[19]. En su defecto, la normativa establece las condiciones para poder llevar a cabo la transferencia (art. 49 RGPD)[20].

En definitiva, lo que el TJUE viene a confirmar en *Schrems II* es que el régimen de protección de datos personales de EE.UU., en contra de lo estimado por la Comisión al adoptar la Decisión 1250/2016 sobre el escudo de privacidad con EE.UU., no ofrece un nivel equivalente y, por lo tanto, adecuado, para la protección de los datos personales procedentes de la UE. Y ello porque la normativa interna estadounidense permite a sus autoridades acceder y utilizar los datos sin sujeción al principio de proporcionalidad[21] y, además, no reconoce a los interesados derechos exigibles judicialmente frente las autoridades estadounidenses[22]. Esto llueve sobre mojado pues, ya en 2015, el TJUE llegó a la misma conclusión en el asunto *Schrems I* con respecto a la Decisión sobre el Puerto Seguro[23], precedente de la del Escudo de Privacidad. Por lo demás, es razonable concluir que esta línea argumental del TJUE sería igualmente aplicable al resto de las Decisiones adoptadas por la Comisión que concierne a la transferencia de datos a otros países[24] de forma que, en la medida en que las legislaciones nacionales de cada uno de ellos no permitan garantizar el respeto a estos estándares, la sentencia tendría un "efecto dominó".

Abundando en este nivel de protección comunitario cabe destacar que el TJUE se ha pronunciado sobre la compatibilidad los derechos fundamentales con la recogida

---

a autorizaciones previas -cuando el objeto y alcance de la operación se definen- y toda la operación debe quedar sujeta a supervisión y evaluación independientes *ex post*.

[19] Comunicación de la Comisión al Parlamento Europeo y al Consejo de 24 de junio de 2020, *La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos*, COM/2020/264 final, p. 15.

[20] Sobre el régimen de transferencia internacional de datos de la UE *vid*. CORDERO ÁLVAREZ, C.I., "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento Europeo: especial referencia al caso estadounidense y la *Cloud Act*", *Revista Española de Derecho Europeo*, núm. 70, abril-junio 2019, pp. 49-108.

[21] Sentencia TJUE *Schrems II*, para. 183, al menos respecto de algunos programas de vigilancia.

[22] *Ibid.*, para. 187. Además, el mecanismo del Defensor del Pueblo, no proporciona vías de recurso ante un órgano que ofrezca garantías sustancialmente equivalentes a las del DUE, que puedan asegurar su independencia ni su autoridad para adoptar decisiones vinculantes para los servicios de inteligencia estadounidenses, para. 168. En la Sentencia TJUE 15 de junio de 2015, *Shrems c. Comisario de Protección de Datos* (*Schrems I)*, C-362/14, ECLI:EU:C:2015:650, paras. 87-98 (anulación de base jurídica del 2puerto seguro") y 93-95 (normas claras sobre acceso de los gobiernos a los datos y recurso judicial). Esto último también en Dictamen 1/15, paras. 141 y 154.

[23] Sentencia TJUE *Schrems I*, en lo que concierne a la Decisión 2000/520 de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de EE.UU. ("Puerto Seguro"), DOUE 2000, L 215, p. 7.

[24] Otras Decisiones de adecuación adoptadas por la Comisión se refieren a Suiza (26.7.2000); Canadá (20.12.2002); Argentina (3.6.2003); Guernsey (21.11.2003); Isla de Mann (28.4.2004); Jersey (8.5.2008); Islas Feroe (5.3.2010); Andorra (19.10.2010); Israel, (31.1.2011); Uruguay (21.8.2012); Nueva Zelanda (19.12.2012), Japón (23.1.2019) y Reino Unido (28.6.2021).

indiscriminada de datos así como el acceso a los mismos por razones de seguridad en el ámbito intracomunitario en el asunto *Privacy International*[25]. Concretamente, el TJUE ha establecido que el respeto a los derechos fundamentales exige que sólo excepcionalmente, con carácter extraordinario y limitado, la legislación nacional pueda permitir que sus agencias de seguridad e inteligencia requieran que los proveedores de servicios de la sociedad de la información les transferieran datos de manera general e indiscriminada (de tráfico y localización).

En cuanto a las cláusulas contractuales, más allá del análisis de su adecuación, que corresponde realizar a la Comisión y que el Tribunal confirma en este caso, el TJUE señala que no puede dejar de tenerse en cuenta la necesidad de evaluar, junto a la cláusula, las posibilidades de acceso a los datos por parte de las autoridades públicas del Estado al que se han transferido conforme al sistema jurídico de dicho país[26]. El riesgo, bien de que tales autoridades públicas accedan o usen los datos transferidos de manera conforme a su propia normativa pero sin alcanzar el estándar de protección del DUE, o bien de que los contratantes no puedan cumplir los términos de la cláusula contractual, debe ser valorado por las autoridades de control de la UE (protección de datos) y, en caso de existir, habrán de prohibir o suspender dichas transferencias[27].

En síntesis, la regulación en materia de protección de datos en la UE tiene carácter imperativo aplicándose las normas territorialmente[28]. Esto explica que no se regule la "importación" o entrada de datos personales de un país tercero puesto que, naturalmente, su protección quedará sujeta al DUE. Sí se regula en cambio el régimen de "exportación" o salida de los datos a terceros países sometiéndolo a condiciones para que sean protegidos en el extranjero de manera equivalente a la de la Unión. A la vista de la jurisprudencia del TJUE, los mecanismos previstos para velar por el mantenimiento del estándar comunitario en las exportaciones de datos son profundamente garantistas, como cabía esperar dado el carácter de derecho fundamental de su protección en la UE.

Así, desde el momento que la legislación de un tercer país contemple la posibilidad de que sus autoridades públicas puedan acceder a los datos, incluso por razones de interés o seguridad, sin las salvaguardas contempladas por el DUE (y, desde luego, de forma indiscriminada), las Decisiones que la UE haya adoptado respecto de transferencias de datos a terceros países resultarían nulas[29]. Del mismo modo, las operaciones que fueran a realizarse sobre la base de contratos con cláusulas autorizadas deberán ser prohibidas puesto que, por más empeño de adaptación a las exigencias comunitarias que realizaran los operadores económicos, no podrían (no está en su mano) modificar la legislación extranjera que, en la medida que permita a las autoridades públicas el acceso a los datos sin las garantías comunitarias, será considerada como un riesgo para la protección de los datos conforme al DUE. En definitiva, las empresas que pretendan desarrollar su actividad contando con el mercado comunitario se verían abocadas, no sólo a una adaptación al RGPD, sino a no exportar datos y únicamente someterlos a tratamiento y almacenarlos dentro de la UE a través de instalaciones locales.

Por lo tanto, aunque formalmente no se formule así, el efecto de esta situación es, de hecho, que frente a la movilidad de los datos personales ("deslocalización"), parezca necesario, con el fin de garantizar su protección, contar con almacenamiento y tratamiento

---

[25] Sentencia del TJUE de 6.10.2020, en los asuntos *La cuadrature du net*, C-511/18, C-512/18 y C-520/18, ECLI:EU:C:2020:79, para. 118. En la misma fecha y sentido, Sentencia en el asunto *Privacy international*, C-623/17, ECLI:EU:C:2020:790, para. 72.

[26] Sentencia TJUE *Schrems II*, para. 134.

[27] *Ibid.*, para. 135.

[28] Art. 3 RGPD, nota 6, y *Directrices* 3/2018 de la EDPB, relativas al ámbito territorial del RGPD; versión 2.1, 7.1.2020. *Vid.* también, STJUE de 1.10.2015, en el asunto C240/14, *Weltimmo*.

[29] *Vid.* nota 25.

local de los mismos ("localización") en la UE para poder operar con ellos. Sirva como prueba que, en la situación de desconcierto e incertidumbre para todos los operadores generada tras *Schrems II*[30], la reacción del Supervisor Europeo de Protección de Datos (SEPD) fue recomendar vivamente a las instituciones, agencias y oficinas de la UE que, mientras se desarrollaba la estrategia para cumplir con la sentencia, evitaran las transferencias de datos a EE.UU. para nuevas operaciones de procesamiento o nuevos contratos con proveedores de servicios[31].

En definitiva, más allá de lo que señala el texto del RGPD, los casos *Schrems* ilustran cómo, frente a Estados que no cuenten con un régimen normativo equiparable al comunitario, la UE incorpora *de facto* la exigencia de almacenamiento y de tratamiento local de los datos con el fin de garantizar su protección. Más allá de la UE, hay otros sistemas nacionales que, ya sea por razón de protección de la privacidad, para promover la economía nacional o por ciberseguridad[32], imponen por ley o como consecuencia de una serie de medidas, la localización de los datos personales, con carácter general o en determinados sectores (por ejemplo, el sanitario), haciendo imposible su transferencia internacional. No cabe duda de que estas medidas constituyen barreras no arancelarias al comercio que tienen como consecuencia un incremento de costes para los operadores económicos. La cuestión es ¿cómo encaja esta situación con el contexto y regulación jurídico-internacional del comercio?

III. CONTEXTO JURÍDICO INTERNACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES Y DEL COMERCIO DIGITAL

El comercio internacional es un instrumento básico para la difusión de los avances tecnológicos, así como para el desarrollo económico. Internet ha sido percibida como un medio para lograr el crecimiento de la riqueza al margen de factores territoriales, que promueve la emancipación de quienes viven en áreas menos desarrolladas del planeta, en particular a través de los beneficios que la conectividad puede tener para pymes y colectivos como las mujeres. Además, el fomento de su uso se encuentra en línea con varios de los puntos destacados en los objetivos desarrollo sostenible 2030 de las Naciones Unidas[33].

El comercio digital ha llegado para crecer y multiplicarse. Consiste en el intercambio de mercancías y de servicios a través de internet y tecnologías basadas en internet (pedidos, producciones, entregas) que, limitando el impacto de los condicionantes territoriales, reduce costes y conecta a comerciantes (B2B) y

---

[30] A lo que se suma, en el caso de España las demandas presentadas contra distintas empresas; "La RAE, Freepik o eDreams, entre las decenas de entidades denunciadas por permitir las transferencias de datos de sus usuarios a EEUU después de que una sentencia del TJUE las invalidara", *Business Insider*, 18.8.2020, https://www.businessinsider.es/5-empresas-espanolas-denunciadas-enviar-datos-usuarios-eeuu-493151, Visitado en julio 2021.

[31] EDBS, *Strategy for EU institutions to comply with "Schrems II" Ruling*, 29.10.2020, p.2, https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en. Visitado en julio 2020.

[32] En el caso de Rusia, la ley de Protección de Datos de 2015 requiere el almacenamiento local de los datos de los residentes en el país. *Vid.* MIHAYLOVA, I. "Could the Recently Enacted Data Localization Requirements in Russia Backfire?", *JWT*, vol. 50, núm. 2, 2016, pp. 313–334.

[33]En particular, 4 (educación), 5 (igualdad de género), 8 (crecimiento económico), 10 (reducir las desigualdades entre países y dentro de ellos) y 16 (paz y justicia) https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/; tay y como lo reconoce, al plantear los Datos como primera línea temática de actuación en 2020 el *Internet Global Forum* de las UN, https://www.intgovforum.org/multilingual/content/igf-2020-thematic-track . Visitados en octubre 2020

consumidores (B2C), tiene carácter global por naturaleza y se apoya en la circulación de datos[34].

A falta de un concepto internacionalmente aceptado, las transferencias internacionales de datos personales pueden definirse como los flujos transfronterizos que se realizan desde un Estado a otro[35], bien entre responsables de su tratamiento o bien entre un responsable y un encargado de dicho tratamiento[36]. Si los datos personales son simplemente enrutados por países terceros, no existe transferencia sino un mero tránsito[37]. Por lo demás, al menos en la UE, la mera accesibilidad de los datos desde terceros países, no constituye una transferencia cuando los datos han sido insertados y el servidor en el que se almacenan se encuentra localizado en el territorio de referencia[38].

1. Estándares internacionales sobre protección de datos personales

El contexto normativo en el que se desenvuelven las operaciones comerciales digitales transfronterizas se caracteriza por una lógica fragmentación reguladora[39]. Tradicionalmente, dicha fragmentación se ha afrontado, conforme a la convicción sobre las bondades socioeconómicas de la liberalización del comercio internacional, a través de compromisos multilaterales, regionales y bilaterales tendentes a la progresiva eliminación de obstáculos.

Hoy en día la mayoría de los Estados cuentan ya con normas de protección de datos[40]. Sin embargo, a escala internacional general, sólo el Convenio de Estrasburgo para la protección de los individuos establece estándares mínimos (art. 13) para su protección en lo que concierne al procesamiento automático de datos personales (con

---

[34] OECD, *The impact of digitalisation on trade*. https://www.oecd.org/trade/topics/digital-trade/ Visitado en julio 2021.

[35] Art. 44 RGPD, así como las comunicaciones ulteriores desde ese tercer país u organización a otro tercer país. Las que tienen lugar entre Estados miembros de la UE y con respecto a Liechtenstein, Islandia y Noruega (EEE), se denominan transferencias transfronterizas (art. 4.23). En España el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD) define las transferencias internacionales de datos como transmisiones de datos fuera del territorio del EEE, independientemente de si se hacen a otro responsable del tratamiento o a un encargado (art. 5.1).

[36] El Convenio para la protección de los individuos en lo que concierne al procesamiento automático de datos personales; Estrasburgo, 28.01.1981 (en vigor desde 01.10.1985 Tratado núm. 108), modificado el 15.6.1999 (Tratado núm. 108+ "modernizado"; en vigor desde 2001). El 10.10.2018 se adoptó el Protocolo que modifica el convenio (T núm. 223), aún no en vigor; define *controller* y *processor* (art. 2.e y f). En esta línea, el art. 4.7 y 8 del RGPD (Dictamen 1/2010 del GT art. 29 sobre los conceptos de responsable del tratamiento» y «encargado del tratamiento, WP169, 6.2.2019) señala que mientras el responsable determina los fines y los medios relacionados con el tratamiento de los datos personales, el encargado los trata por cuenta del responsable (suele ser un tercero externo o, dentro de grupos de empresa, una de ellas para las demás. Conforme al RGPD (art. 4.2) actividades de tratamiento de datos son el traspaso o la comunicación, entrega, consulta, interconexión, transferencia o "cualquier otra forma de acceso a los datos" …habla también de captura, clasificación, almacenamiento, uso, tratamiento, destrucción. El art. 5.1 RLOPD menciona también la cesión.

[37] En ellos no operan los responsables de la recogida ni del tratamiento de datos; tampoco se almacenan.

[38] En la UE, Sentencia del TJUE de 6.11.2003, *Bodil Lindquvist*, asunto C-101/01, ECLI:EU:C:2003:596, para. 71.

[39] El *UNCTAD Global Cyberlaw Tracker* señala que, de un total de 194, los países que disponen de regulación sobre el comercio en Internet son 158 (82%), de los cuales 68 están en vías de desarrollo o son economías en transición y 30 son países menos desarrollados, Prácticamente todos los europeos (44 de 45), el 91%de los americanos mientras que en África solo 61%. https://unctad.org/page/e-transactions-legislation-worldwide. Visitado en julio 2021.

[40] *Ibid.*, de un total de 194, 132 cuentan con legislación protectoras, África y Asia muestran similares niveles con un 55% de ellos con normas, de los cuales 23 son países de los menos desarrollados.

independencia de la tecnología – "neutralidad tecnológica")[41], sin reconocer expresa y formalmente su carácter de derecho fundamental[42]. A estos efectos, más allá de los ya mencionados CEDH y de la CDFUE, cabe señalar que si bien la Declaración Universal de los Derechos Humanos reconoce el derecho a la protección frente a injerencias en la vida privada de los individuos (art. 12), la precisión de su alcance en lo que concierne a la protección de los datos personales no ha sido internacionalmente establecida.

En síntesis, el Convenio de Estrasburgo reconoce el derecho de los individuos a recibir información sobre la obtención y el tratamiento de sus datos, así como a ser consultados y oponerse a dicho tratamiento, obtener la rectificación y la eliminación de los mismos y contar para todo ello con el respaldo de una autoridad supervisora y con mecanismos judiciales y extrajudiciales (arts. 8, 9 y 12). Además, se contempla la existencia de excepciones a las reglas acordadas cuando estén previstas en la ley y resulten necesarias y proporcionadas "en una sociedad democrática" para proteger los derechos de los individuos y "los derechos y libertades fundamentales de otros; especialmente la libertad de expresión" (art. 11). Actualmente, 55 Estados son parte en el mismo, incluyendo a la UE, pero no EE.UU., que tiene estatuto de observador.

El Convenio establece también normas especiales para el flujo internacional de datos ("exportaciones"[43]) y mecanismos para las consultas y asistencia mutua entre las partes. La propia existencia del Convenio se explicó por la necesidad de evitar que los controles que imponen los Estados para salvaguardar la protección de los derechos en operaciones internacionales interfirieran negativamente en la "libre circulación internacional de información, que es un principio de importancia fundamental para los individuos y para las naciones"[44] y "no debe ser interpretado como un medio para adoptar barreras no arancelarias al comercio internacional"[45]. Así, partiendo del respeto a los estándares comunes acordados en la primera parte del Convenio, lo que supone admitir que ofrecen un nivel de protección considerado adecuado, los Estados parte se comprometen a no prohibir ni sujetar a autorizaciones especiales el flujo de datos entre ellas; salvo que se produzca un riesgo serio de que, con la transferencia, se incumplan las normas del propio acuerdo (art. 14)[46].

En la misma línea pero sin fijar obligaciones internacionales, la OCDE recomienda a sus miembros que se esfuercen en eliminar o evitar la creación de obstáculos injustificados al flujo de datos personales so pretexto de proteger la intimidad

---

[41] *Vid.* nota 34. Los compromisos son aplicables con independencia de la nacionalidad o residencia de los individuos (art. 1.1).

[42] La exposición de motivos del Tratado 108+, nota 36, señala: "*it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data"*. No obstante, también señala que "*the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with <u>other</u> human rights and fundamental freedoms, including freedom of expression*".

[43] *Explanatory Report* – ETS 108, 28.1.1981, nota 36, p. 12, &.66.

[44] *Ibid.* p. 3; &9; viene referido a la libertad de expresión, art. 10 CEDH y 19 de la Declaración Universal de los Derechos Humanos, p.5, &19.

[45] *Ibid.* p. 6; &25.

[46] Art. 14 T 108+ (antiguo 12, modificado), nota 36:"*A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation"*.

de las personas y, a estos efectos, elaboró sus Directrices sobre privacidad[47]. Adoptadas como un estándar mínimo, las Directrices han servido de base para el desarrollo de normas estatales e incluso se referencian en acuerdos internacionales[48]. En lo que concierne al flujo internacional de datos, señalan que los Estados deben: (1) tomar en consideración las implicaciones que puedan tener sus normas nacionales sobre procesado y re-exportación de datos personales a otros países; (2) adoptar todas las medidas razonables y apropiadas para asegurar que el flujo internacional de datos, incluido el tránsito, sean ininterrumpidos y seguros; (3) abstenerse de dificultar los flujos internacionales de datos personales entre ellos *excepto* si no cumplen sustancialmente con las Directrices *o* cuando la re-exportación de los datos incumpliría las normas nacionales para su protección, así como respecto de ciertas categorías de datos que, por razón de su naturaleza, estén sujetos en el Derecho interno a una protección que no se ofrece de manera equivalente en el otro país; y (4) evitar el desarrollo de leyes, políticas y prácticas que, pretextando la protección de la privacidad y las libertades individuales, creen obstáculos al flujo internacional de datos personales que excederían de las exigencias de dicha protección[49].

La cooperación interestatal en esta materia cuenta con la Red Global para la Aplicación de la Ley para la protección de la Privacidad (*Global Privacy and Enforcement Network – GPEN*)[50]. Constituida al albur de la Recomendación homónima de la OCDE[51], reúne a autoridades nacionales de protección de datos para promover el intercambio de información, así como la coordinación y la cooperación en la aplicación de las normas nacionales y el intercambio de las mejores prácticas. Con carácter previo y al margen de dicha organización, un grupo de Estados creó la Red Internacional de Protección del Consumidor y Aplicación de la Ley (*International Consumer Protection and Enforcement Law* - ICPEN) en materia de protección a los consumidores[52], en la que se aborda la protección de su privacidad.

El papel de los operadores económicos también ha sido específicamente reseñado en las iniciativas internacionales. La OCDE cuenta con una Recomendación sobre la protección de los consumidores en el comercio electrónico en la que, además de remitirse a las Directrices sobre privacidad, se refiere al comportamiento de éstos en la materia (B2C) con el fin de que se aseguren de que sus prácticas en la recogida de datos son legales, transparentes y justas, permitiendo a los consumidores participar y elegir y dándoles salvaguardas razonables y seguras[53].

Finalmente, la interacción entre todos los actores interesados, Estados, empresas e incluso la sociedad civil, aparece recogida en otras actuaciones internacionales. Así, las

---

[47] OCDE *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 11.7.2013, ("Privacy Guidelines"), revisa la versión original de 1980. Grupo de trabajo sobre seguridad y privacidad.

[48] A título de ejemplo, baste señalar el CPTPP, notas 98 y 99, o el vigente acuerdo UE- México, nota 103.

[49] Apartados 1, 16, 17 y 18.

[50] Comenzó su actividad en el verano de 2008. https://www.privacyenforcement.net/. Visitado en julio 2021. *Action Plan for the Global Privacy Enforcement Network*, 15.6.2012; Parte E, modificado el 22 de enero de 2013.

[51] OECD *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, adoptada en junio de 2007, http://www.oecd.org/internet/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsprotectingprivacy.htm. Visitado en julio 2021.

[52] En la actualidad, 65 Estados son parte de esta red. https://icpen.org/search?search=personal+data. Visitado en julio 2021.

[53] *Recommendation on Consumer Protection in E-commerce*, adoptada el 9.12.1999 y actualizada en 2016, establece que "*Businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards*"; p. 17, para. 48.

Directrices de las Naciones Unidas para la Protección del Consumidor[54] pretenden atender a la "protección de la privacidad del consumidor y la libre circulación de información a nivel mundial" que catalogan como una necesidad legítima y constituye un principio general de actuación (III.5.k). Para ello establecen que, por una parte, los Estados deben adoptar políticas que fomenten la protección de la privacidad de los consumidores y la protección de sus datos (V.A.14.h) y que, por otro lado, las empresas han de proteger la privacidad de los consumidores mediante mecanismos adecuados en lo relativo a la recopilación u utilización de sus datos personales (IV.11.e).

Naciones Unidas cuenta, además, con un Foro sobre la Gobernanza de Internet (*Internet Governance Forum*), que, con el fin de buscar principios comunes de actuación en los temas relacionados con la red, reúne a gobiernos, empresas, expertos y la sociedad civil. De los cuatro pilares sobre los que se desarrolla su actividad, el primero son los datos, incorporando algunas cuestiones relacionadas con la protección de derechos fundamentales, la privacidad y el impacto que la soberanía digital y la fragmentación de internet tiene en la confianza de los usuarios[55].

Hasta aquí se observa la convicción a escala multilateral de la importancia de encontrar un equilibrio adecuado entre la protección de los datos y de la privacidad, ya sea como derechos fundamentales o como derechos del consumidor, y su flujo transfronterizo en pro de la facilitación del comercio internacional. En este sentido, se reconocen, además de la necesidad de la actuación combinada a escala estatal y privada, la de la existencia de unos estándares de protección de privacidad comunes. Sólo sobre esta última base, se sienta como principio la liberalización del flujo de datos que, no obstante, podrá ser constreñida o excepcionada en función de las necesidades de su tutela valoradas a escala nacional.

Resulta obvio que la existencia de estándares comunes facilita el acceso a los mercados (transparencia, seguridad jurídica). A medida que las tecnologías evolucionan en un mundo interconectado, el desarrollo de una convergencia internacional de estándares se hace más necesario para permitir la continuidad del comercio. En este sentido, no puede dejarse de notar que el Acuerdo sobre Obstáculos Técnicos al Comercio de la OMC se apoya en los estándares internacionales como referente y justificación de las regulaciones nacionales, que no deben crear obstáculos innecesarios al comercio[56]. Al mismo tiempo, crece la motivación de los distintos actores para participar en su elaboración, así como la diversidad de los intereses en presencia; lo que, lógicamente, dificulta la consecución de acuerdos, especialmente a escala multilateral.

En este terreno destaca con carácter general la labor de la Organización Internacional para la Normalización (ISO)[57] y, en el ámbito específico de las telecomunicaciones, la *3rd Generation Partnership Project* (3GPP)[58]; sin que ninguna de ellas haya recogido hasta la fecha disposiciones concretas sobre la protección de datos o

---

[54] *UNCTAD Directrices para la protección del consumidor*, aprobadas por la Asamblea General en su resolución 39/248, de 16.4.1985, ampliadas posteriormente por el Consejo Económico y Social en su resolución 1999/7, de 26 de julio de 1999, y revisadas y aprobadas por la Asamblea General en su resolución 70/186, de 22.12.2015.

[55] https://www.intgovforum.org/multilingual/content/illustrative-policy-questions-data. Visitado en julio 2021.

[56] El Acuerdo sobre Obstáculos Técnicos al Comercio (OTC) de la OMC pretende que la prueba y certificación de las mercancías no creen obstáculos innecesarios al comercio reconociendo. El Acuerdo firmemente a los Miembros que basen sus medidas en normas internacionales (arts. 1.1 y 2).

[57] *International Standarisation Organisation*; https://www.iso.org/home.html visitada en julio 2021.

[58] *The 3rd Generation Partnership Project* (3GPP) reúne a siete organizaciones para el desarrollo de estándares de telecomunicación (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) y facilita un entorno estable para producir informes y especificaciones en las tecnologías; https://www.3gpp.org/about-3gpp/about-3gpp Visitada en julio 2021.

de la privacidad. Esto no puede sorprender puesto que se trata de una cuestión que excede ampliamente la dimensión técnica para abordar consideraciones éticas conectadas con los derechos humanos y su percepción. Más allá de los eventuales intereses económicos nacionales, alcanzar acuerdos en cuestiones que reflejan prioridades culturales nacionales resulta mucho más complejo. En todo caso, el propio Convenio de Estrasburgo, así como las Recomendaciones y Directrices de distintas organizaciones internacionales constituyen trabajos de referencia. Por lo demás, a nivel técnico, dos importantes agencias de estandarización en el ámbito de la creación de protocolos tecnológicos para internet la *Internet Architecture Board* (IAB) y la *Internet Engineering Task Force* (IETF) han incorporado recientemente a su agenda de actuaciones el uso de tecnologías que incrementen el nivel de protección de los datos (*privacy by design*) de forma que se faciliten soluciones técnicas para la protección de los datos con independencia de su localización[59]. Estas soluciones tecnológicas se apoyarían en estándares materiales de protección que contribuirían a alcanzar cierto grado de estandarización, lo que redundaría tanto en la profundización del grado de protección como en su armonización internacional.

En otra línea, en el marco del Acuerdo de Cooperación Económica Asia-Pacífico (APEC)[60] y para facilitar el flujo transfronterizo de datos personales entre los Estados participantes[61], se puso en marcha de manera regional y obligatoria el denominado Sistema de Privacidad de la APEC (*Cross border privacy rules system* - Cbpr)[62]. El Sistema, que combina la actuación de autoridades públicas y del sector privado, se asienta en nueve principios (prevención del daño; información; límites a la recogida de información; usos de la información personal; elección de los particulares; integridad de la información personal; salvaguardas; acceso y corrección y responsabilidad) y establece un sistema de certificación pública de cumplimiento de estándares que permite las transferencias responsables de datos entre ellos. Cuenta, además, con una Guía para ayudar a los todos países APEC a desarrollar aproximaciones nacionales coherentes en la protección de la información personal y la privacidad, de forma que se construyen las bases para una posición regional en la materia.

2. Datos personales en el comercio internacional

Más allá de esta búsqueda de estándares comunes de protección de datos personales que faciliten su tráfico transfronterizo, a la hora de adentrarse en el régimen del comercio internacional multilateral, debe partirse de la calificación de los datos en este contexto. Es bien sabido que la OMC regula el comercio de mercancías (GATT-94 y acuerdos de desarrollo) y de servicios (GATS), además de los aspectos de la propiedad intelectual relacionados con el comercio (ADPIC).

---

[59]World Economic Forum, White Paper, *Exploring International Data Flow Governance Platform for Shaping the Future of Trade and Global Economic Interdependence*, 2019, p. 9. "Privacidad mediante diseño" se diferencia de las tecnologías que incrementan la seguridad en que la primera es un requisito de la arquitectura de un sistema o producto mientras que las segundas se utilizan en un momento posterior, cuando la arquitectura ya se ha desarrollado.

[60] https://www.apec.org/About-Us/About-APEC. Visitado en octubre 2020.

[61] De los 21 Estados miembros, actualmente participan en el sistema EE.UU., México, Japón, Canadá, Singapur, República de Corea, Australia, Taipei Chino, y Filipinas.

[62] *Cross Border Privacy Rules*, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System, visitado en julio 2021. El *APEC Privacy Framework*, que fue adoptado inicialmente el 2005 y actualizado en 2015, se hace eco de la Guía de Privacidad de la OCDE, p.3 &5.

Con carácter general, los datos personales, más allá de la posibilidad de convertirse en un activo susceptible de ser objeto de comercio y de servir de apoyo para las transacciones (físicas o analógicas) en particular, cuando los adquirentes son consumidores[63], son un medio de producción y una herramienta para que las cadenas globales de valor se organicen, así como para la prestación de servicios y para el desarrollo de negocios (la computación en la nube y el internet de las cosas, así como las tecnologías de fabricación aditiva)[64].

Si bien, de entrada, los datos personales podrían ser tratados como una mercancía más, constituyendo el propio objeto de una transacción económica (contratos de compraventa o de cesión), resulta evidente que reúnen cualidades distintas de las mercancías tradicionales que llevan a cuestionar esta calificación[65]. Además, al estar directamente vinculados con aspectos personales de los individuos, su mercantilización con el fin de obtener rendimientos económicos ha dado lugar a hablar de un "capitalismo de vigilancia" (*surveillance capitalism*)[66]. En la UE, el Comité Europeo de Protección de Datos (CEPD) ha señalado expresamente que no pueden ser considerados como mercancía objeto comercio[67]. Sin embargo, en EE.UU., aunque se discuta la caracterización de los datos personales como mercancía[68], quien recogió los datos puede, salvo en algunos ámbitos, disponer de ellos prácticamente como sí de un bien más se tratara[69].

En cuanto a las prestaciones de servicios que involucran *per se* el acceso, tratamiento o utilización de los datos personales, pueden mencionarse, entre otras, desde el acceso a la red y a las publicaciones en webs o blogs desde terceros países, hasta el almacenamiento de archivos de páginas web (servicios de *hosting*) prestados en un tercer

---

[63] Por ejemplo, a través de sistemas de intercambio electrónico de datos; *Electronic Data Interchange* (EDI)

[64] OECD, nota 34.

[65] Mientras que las mercancías, al igual que, los servicios pueden ser producidos, consumidos, comprados y vendidos; los datos, pueden, además, ser duplicados, compartidos y "absorbidos" (saber qué hacer con ellos; interpretarlos y aplicarlos). En esta línea, las Directrices 2/19 del CEPD, sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados- https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf (visitado en julio 2021), para.54 nota a pié, señalan que "el tratamiento de los datos personales difiere de los pagos monetarios desde el punto de vista conceptual. Por ejemplo, el dinero se puede contabilizar, es decir, los precios pueden compararse en un mercado donde rija la libre competencia, y, en general, los pagos monetarios solo pueden realizarse con la participación del interesado. Además, los datos personales pueden ser explotados por varios servicios a la vez. Una vez que una persona pierde el control sobre sus datos personales, es posible que no pueda recuperar dicho control".

[66] ZUBOFF, S. *The Age of Surveillance Capitalism; the fight for the future at the new frontier*, Profile Books, London, 2019.

[67] Directrices 2/2019 del CEPD, nota 67, para. 54 señala que "(H)abida cuenta de que la protección de los datos es un derecho fundamental … y de que uno de los principales objetivos del RGPD es ofrecer a los interesados el control sobre la información que les afecta, los datos personales no pueden considerarse una mercancía. Aunque el interesado pueda prestar su consentimiento al tratamiento sus datos personales, no puede comerciar con sus derechos fundamentales en virtud de dicho acuerdo".

[68] LITMAN, J., "Information Privacy/Information Property", *Standford Law Review*, vol. 52, May 2020, pp.1283-1313, censura el tratamiento de los datos como propiedad y promueve otro basado en la responsabilidad extracontractual (*tort*).

[69] En EE.UU., la privacidad de los datos no se considera como parte del derecho fundamental a la intimidad. La privacidad de los datos se protege en función de las situaciones. En algunos casos la normativa obliga a las a las empresas que recogen datos a introducir medidas de protección y salvaguarda (entre ellos, los sectores sanitarios –HIPAA-, financieros -GLBA y FCR- y comerciales -TCPA, TSR y CAN-SPAM). Fuera de estos casos, no hay normas explícitas para la protección de la privacidad de los datos. La empresa informa a los consumidores de la recogida de datos y del uso que se hará de ellos permitiéndoles no aceptar. Si se continúa navegando, se acepta implícitamente. A partir de ese momento, los datos quedan en manos de la empresa.

país respecto de páginas que contengan datos personales; pasando por los servicios de correo electrónico en la nube (*Gmail; Microsoft Outlook*) con servidores localizados en terceros países (que reciben, almacenan y envían) a los que se transmiten los datos personales de los usuarios; los servicios de mensajería instantánea y video-llamadas (*WhatsApp, Skype*) prestados por empresas localizadas en terceros países (o bien cuando las empresas locales comparten los datos con las empresas del grupo que se encuentran fuera de dicho territorio); así como las redes sociales (*Facebook, Instagram; TickTok*) y las plataformas de marketing (*Mailchimp*) ubicadas en terceros países (que gestionan listas de suscriptores y realizan envíos de publicidad). Y ello en el ámbito de múltiples sectores, tan dispares como los servicios educativos, sanitarios, financieros … etc.

Sobre esta base, resulta pertinente analizar a continuación la existencia de normas en los acuerdos OMC con potencial incidencia en el comercio internacional de mercancías y servicios para los que los datos personales constituyen, si no su propio objeto, sí una herramienta o instrumento fundamental.

IV. LA REGULACIÓN EN EL COMERCIO INTERNACIONAL: LA OMC Y LOS ACUERDOS DE LIBRE COMERCIO

Está claro que las normas de protección de los datos personales y de la privacidad pueden afectar el comercio internacional al fijar condiciones para la transferencia de dichos datos.

1. OMC

Los Acuerdos de la OMC así como los Informes de los Grupos Especiales que resuelven las controversias suscitadas por su aplicación establecen que una medida nacional entra en el ámbito de aplicación de las normas multilaterales de comercio si tiene efectos sobre los compromisos adquiridos en virtud de las disposiciones de los distintos Acuerdos[70], con independencia del entorno comercial en el que se manifiesten tales efectos o se pongan en práctica las medidas (neutralidad tecnológica). Así, las actuaciones estatales en materia de protección de datos personales pueden constituir una medida y, en consecuencia, su conformidad con los compromisos adquiridos puede ser cuestionada en tanto tenga repercusiones sobre el cumplimiento de los mismos.

El comercio de mercancías está regulado por el GATT y los acuerdos que lo desarrollan. Se parte de la progresiva supresión y eliminación de los aranceles (art. II)[71]. Más allá de la obligación de respetar el tratamiento de nación más favorecida (TNMF, art. I), se impone el tratamiento nacional (TN, art. III) y se prohíben las restricciones cuantitativas o medidas de efecto equivalente ya sea a las importaciones o a las

[70] En el caso del GATS, "… *encompasses any measure of a Member to the extent it affects the supply of a service regardless of whether such measure directly governs the supply of a service or whether it regulates other matters but nevertheless affects trade in services*"; Communidades Europeas — Régimen de la importación, venta y distribución de bananos, para. 7.285. En el caso del art. XX GATT, en China – Medidas que afectan a los derechos comerciales y los servicios de distribución respecto de determinadas publicaciones y productos audiovisuales de esparcimiento, WTO/DS363, informe del GE y del OA, adoptados el 19.1.2010, mantuvieron, "*should weigh not only the restrictive impact the measures at issue have on imports of relevant products, but also the restrictive effect they have on those wishing to engage in importing, in particular on their right to trade*" para. 7.788.

[71] En lo que concierne a los aranceles de las transacciones electrónicas, Declaración sobre el comercio electrónico mundial, WT/MIN(98)/DEC/2, de 25.5.1998; sobre la "moratoria". Tras varias prórrogas bienales, la aprobación de una nueva prórroga debía haberse realizado durante la Conferencia Ministerial en junio 2020, pospuesta 2021. *Vid. supra.* nota 123.

exportaciones (art. XI). No obstante, las medidas restrictivas serán permitidas en tanto se enmarquen dentro de las excepciones generales, que incluyen las que resulten necesarias para proteger la moral pública, siempre que no constituyan discriminaciones arbitrarias ni restricciones encubiertas al comercio internacional (art. XX) o las relativas a la seguridad nacional (art. XXI). Asimismo, cabe excepcionar la aplicación del TNMF en lo que concierne a los procesos de integración económica (art. XXIV). Aunque se ha discutido[72], la aplicación de estas normas a las operaciones realizadas a través de internet puede realizarse mediante una interpretación ajustada a este entorno. Así han tenido oportunidad de hacerlo un Grupo Especial y el propio Órgano de Apelación (OA) para productos digitales respecto del TN y a las excepciones generales[73].

1.1 Posibles infracciones

En el caso del tráfico de datos, cabría pensar que medidas estatales que conduzcan al bloqueo parcial o total de las transacciones internacionales, por ejemplo, imponiendo el control de su contenido como exigencia previa para la entrada o para la salida del mercado nacional o condicionando esta entrada o salida a una autorización administrativa, tendrían un efecto equivalente a las restricciones cuantitativas, ya sea a la importación o a la exportación de un producto, y serían, en consecuencia, consideradas infracciones al artículo XI.1[74], sin perjuicio del recurso a alguna excepción.

En el marco de la regulación del comercio de servicios (GATS; art. I.3.b[75]), los Estados gozan de mayor libertad y discrecionalidad, siendo, además, más compleja la identificación de los compromisos de liberalización adquiridos por cada uno de ellos. Esto es así porque, como es sabido, al margen de las limitadas obligaciones generales e incondicionales (TNMF, art. II; transparencia, art. III; regulación, art. VI[76]; y reconocimiento, art. VII[77]) y lo establecido en los Anexos (en particular, los relativos a las telecomunicaciones y a los servicios financieros), los Estados únicamente se obligan a lo fijado en sus respectivas listas de compromisos específicos (art. XV) para cada uno de los 162 sectores y subsectores[78] y en las cuatro modalidades de prestación de servicios (art. I.2)[79] en lo que concierne al tratamiento nacional (art. XVI) y el acceso a los

---

[72] BURRI, M., "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation", *Californa Davis Law Review*; 2017, pp. 93-99, señala que el sistema de la OMC no ha sido capaz de adaptarse a las necesidades del comercio digital y de la protección de datos y defiende la absoluta necesidad de adoptar normas específicas

[73] WTO/DS363, nota 70. El asunto hace referencia a las medidas discriminatorias para la venta, distribución y uso de similares productos audiovisuales extranjeros. El recurso a la excepción general (art. XX) sólo es posible cuando la medida infractora resulta necesaria y proporcionada. El OA recordó que "una medida es necesaria cuando está más cerca de ser "imprescindible" que, simplemente, de "realizar una contribución al" objetivo de que se trate; Corea - Medidas que afectan la importación de carne fresca, refrigerada y congelada, WT/DS161/AB/R, de 11.12.2000, para.161).

[74] RUOTOLO, G.M., "The EU data protection regime and the multilateral trading system: Where dream and day unite"; *QIL Zoom- in*, núm. 51, 2018, pp. 15-16.

[75] El término "servicios" comprende todo servicio de cualquier sector, excepto los suministrados en ejercicio de facultades gubernamentales.

[76] En síntesis, los Estados se obligan a que la aplicación de sus normas relativas al comercio de servicios se realice de forma razonable, objetiva e imparcial.

[77] En síntesis, los Estados se comprometen a facilitar, sin discriminación, un marco adecuado para el reconocimiento de los títulos requeridos para la prestación de servicios.

[78] Lista de clasificación sectorial de servicios de la OMC, MTN.GNS/W/120, de 10 de julio de 1991.

[79] Suministro de un servicio: a) del territorio de un Miembro al territorio de otro (transfronterizo); b) en el territorio de un Miembro a un consumidor de cualquier otro (consumo en el extranjero); c) por un proveedor de servicios de un Miembro mediante presencia comercial en el territorio de otro (presencia comercial); d)

mercados (art. XVII). En todo caso, sobre la base del principio de neutralidad tecnológica, los Estados no pueden diferenciar entre los mecanismos -analógicos o digitales- disponibles para la prestación del servicio[80]. Por lo demás, el GATS también contempla excepciones generales, entre cuyas causas se incluye expresamente la protección de la privacidad de los individuos en lo que concierne al procesamiento y la distribución de sus datos personales y la protección de la confidencialidad de sus informes y cuentas personales siempre que no constituya una discriminación arbitraria ni una restricción encubierta al comercio internacional (art. XIV.c.ii)[81], y por razones de seguridad nacional (art. XIV bis). Asimismo, cabe excepcionar la aplicación del TNMF en lo que concierne a los procesos de integración económica (art. V).

En este marco, las limitaciones a las transferencias internacionales de datos pueden constituir restricciones infractoras del GATS, bien de forma directa o de manera indirecta. Serán restricciones directas cuando el servicio para el que se hayan adquirido compromisos específicos, ya sea de trato nacional o de acceso a los mercados, consista en dicha transmisión de datos (computación en la nube o almacenamiento de datos, por ejemplo). Serán restricciones indirectas cuando obstaculicen la prestación de los servicios para los que, existiendo compromisos de liberalización en la correspondiente lista, los datos sean un elemento imprescindible (por ejemplo, la evaluación de la salud de un paciente)[82]. Como se ha señalado, los compromisos de liberalización relativos al tratamiento nacional y el acceso a los mercados figuran en la lista de compromisos específicos de cada parte.

En cuanto al TN, las infracciones del artículo XVII GATS se producen en la medida en la que se adopta una diferencia de trato. En lo que concierne al acceso a los mercados, el artículo XVI GATS señala una relación de seis barreras prohibidas, mayoritariamente referidas a restricciones cuantitativas (en síntesis, número de proveedores, de operaciones, de empleados, valor de activos o transacciones y de la inversión extranjera). El OSD ha establecido que, existiendo compromisos, las medidas nacionales que tengan como efecto una prohibición total de prestar un servicio en línea a proveedores extranjeros resultan equivalentes a establecer una cuota cero para la

---

por un proveedor de servicios de un Miembro mediante la presencia de personas físicas de un Miembro en el territorio de otro (presencia de personas físicas).

[80] *Programa de Trabajo sobre el Comercio Electrónico - Informe de Situación al Consejo General*, adoptado por el Consejo del Comercio de Servicios el 19.7.1999, S/L/74, 27.7.1999, para. 4: "… la opinión general fue que el AGCS es tecnológicamente neutro, en el sentido de que no contiene ninguna disposición que haga una distinción entre los distintos medios tecnológicos a través de los cuales puede suministrarse un servicio". En este sentido también, WT/DS285 *Estados Unidos — Medidas que afectan al suministro transfronterizo de servicios de juegos de azar y apuestas*; reclamación presentada por Antigua y Barbuda; Informe del Grupo Especial, 10.11.2004, (confirmado por el OA, 7.4.2005), señala que, salvo que se especifique otra cosa en la lista, los compromisos relativos a la prestación de un servicio se aplican a todos los medios; incluido Internet; para. 6.285.

[81] "A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas: A) necesarias para proteger la moral o mantener el orden público (únicamente podrá invocarse cuando se plantee una amenaza verdadera y suficientemente grave para uno de los intereses fundamentales de la sociedad) … C) *necesarias para lograr la observancia de las leyes y los reglamentos que no sean incompatibles con las disposiciones del presente Acuerdo*, con inclusión de los relativos a: i) la prevención de prácticas que induzcan a error y prácticas fraudulentas o los medios de hacer frente a los efectos del incumplimiento de los contratos de servicios; ii) *la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales*; iii) la seguridad. …"

[82] RUOTOLO, G.M., nota 74, p. 20.

provisión del servicio, prohibida por artículo XVI:2.a)[83]. Del mismo modo, si se imponen medidas que provoquen cualquiera del resto de las restricciones cuantitativas descritas en el artículo XVI, se incurriría en infracción del Acuerdo.

1.2 DUE y OMC

Para evaluar la compatibilidad del DUE con este marco regulador tras la jurisprudencia sentada por el TJUE en los asuntos *Schrems*, además de a las obligaciones del GATS, habría que atender fundamentalmente a la lista de compromisos específicos para el comercio de servicios de la UE[84] y, en su caso, a la posibilidad de recurrir a las excepciones. La imposibilidad de llevar a cabo transferencias de datos personales que afecten negativamente la prestación de servicios (restricciones directas) supondrían una infracción del artículo XVI:2.a) en los sectores para los que la UE ha adquirido compromisos específicos. Concretamente, el caso de los servicios de procesamiento de datos (apartado b de los servicios de informática y conexos (B), dentro del grupo 1; servicios prestados a las empresas), la UE se compromete con carácter general a no adoptar medidas que restrinjan el acceso a los mercados en tres modalidades de comercio de servicios (transfronterizo, consumo en el extranjero y presencia comercial)[85] por lo que la infracción de la norma podría llegar a establecerse muy en particular en el comercio transfronterizo. En servicios de telecomunicaciones, sólo se adquieren obligaciones en el comercio transfronterizo y en el consumo en el extranjero[86]. Estas mismas modalidades también están sujetas a compromisos para los servicios financieros (7.a Seguros, B. Bancarios) si bien con muchas particularidades. En todo caso, como se ha indicado, de infringirse las obligaciones adquiridas, siempre se podría tratar de justificar dicho comportamiento recurriendo a las excepciones.

También en este marco, cabría plantear la posibilidad de infracciones del TN (art. XVII) en casos de duplicidad de estándares aplicados a los prestadores de servicios o a la prestación internacional de servicios. En los servicios de procesamiento de datos (B.b), la obligación de TN se recoge para todos los miembros en las mismas tres modalidades[87]. Como en los servicios financieros (7.a Seguros, B. Bancarios), en los servicios de telecomunicaciones (2.C), se adquieren compromisos respecto del comercio transfronterizo y el consumo en el extranjero[88]. En principio, las normas de protección de datos del DUE no parece que den lugar al incumplimiento de esta obligación porque los estándares del RGPD se aplican igualmente a todos. No obstante, más allá de la inexistencia de una discriminación formal, podría llegar a establecerse una diferencia de trato *de facto*, en particular en el caso del comercio transfronterizo, cuando la puesta en práctica de las normas perjudica la posición competitiva de los servicios y prestadores de servicios de otros Estados miembros de la OMC.

En lo que concierne a las obligaciones incondicionales del GATS, se abre la posibilidad de que la sujeción de la transferencia de datos a un examen de adecuación

---

[83] WT/DS285, nota 80, Informe del GE para. 6.331. Confirmando que la prohibición total puede ser el efecto de un conjunto de medidas, y que éstas deben estar debidamente identificadas, Informe del OA, paras. 124-126.

[84] La actual lista de compromisos específicos de la UE, GATS/SC/157, de 7.5.2019, p. 123 servicios de telecomunicaciones; p. 150 y 176 (particularidades de países) y 190, servicios financieros.

[85] Lista de compromisos específicos UE, p. 75. Salvo Eslovaquia, Letonia y Malta.

[86] Lista de compromisos específicos UE, p. 123. Con la excepción de Chipre y Malta en el comercio transfronterizo.

[87] Lista de compromisos específicos UE, p. 75, con excepción de Malta.

[88] Lista de compromisos específicos UE, p. 123. En el caso de las telecomunicaciones, con la excepción de Chipre y Malta en el comercio transfronterizo.

(equivalencia) de trato en el Estado de destino, tal y como prevé el RGPD, de lugar a eventuales discriminaciones entre países, lo que supondría infringir el TNMF (art. II)[89]. Otra cosa es que la diferencia de trato pudiera estar justificada a través de una excepción.

1.3 Vías de excepción

En cuanto a la posibilidad de excepcionar el cumplimiento de las normas (arts. XX GATT y XIV.c.ii) GATS) se requiere acreditar la finalidad de la medida en relación a la protección de datos, así como su necesidad. En este sentido, es preciso demostrar que no existe medida alternativa, razonablemente disponible, menos restrictiva del comercio[90] y que las adoptadas no se aplican de forma que constituyan un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios; esto es, que las excepciones se utilicen de forma razonable, de modo que no frustre los derechos que las disposiciones del GATT y/o GATS confieren a los demás Miembros[91]. Se ha dicho que las infracciones que pretendieran ampararse en esta excepción no podrían estar justificadas ya que el test de necesidad sería difícil de satisfacer puesto que hay "alternativas razonablemente disponibles" para proteger los derechos que resultan menos restrictivas, como las que utiliza Canadá y algunos países de la Comunidad Económica de Asia-Pacífico[92].

De forma paralela al GATT (art. XXI), la excepción de seguridad nacional del GATS (Art. XIVbis I.b) permite a un miembro adoptar "medidas que *estime necesarias* para la protección de los intereses esenciales de su seguridad" en determinados casos relativos a las fuerzas armadas, material sensible o situaciones de guerra o tensión internacional[93], que, constituyendo situaciones extraordinarias relacionadas, además, con cuestiones militares y de seguridad nacional, muy eventualmente estarían vinculadas a las transferencias internacionales de datos personales. A diferencia del examen de necesidad de la excepción general, en esta caso cada miembro decide por sí mismo la necesidad de las medidas siempre que encajen objetivamente en los supuestos contemplados en el precepto[94]. Cabe recordar en esta línea, que hay cuestiones que el sistema de solución de diferencias de la OMC no puede enjuiciar[95]. Dado que el alcance

---

[89] RUOTOLO, G.M., nota 74, p. 26 y IRION, K., YAKOLOEVLA, S. y BARTI, M., *Trade and Privacy: Complicated bedfellows?. How to achieve data protection-proof free trade agreements?*, IVIR, 2016, p.30.

[90] WT/DS285, *supra*, en el ámbito de la protección de la moral y el orden público (art. XIV.a GATS). Mientras que el Informe del Grupo Especial aceptó la existencia de necesidad y consideró suficiente a estos efectos la invitación a celebrar de consultas entre Antigua y EE.UU., el OA, ratificando la existencia de necesidad, no aceptó que esta última constituyera una medida alternativa "porque las consultas, por definición, constituyen un proceso cuyos resultados son inciertos", para. 317 y, no habiéndose propuesto ninguna otra medida alternativa, se cumplió con el requisito de necesidad.

[91] *Ibid.* Mientras el Grupo Especial señaló la existencia de discriminación, el OA, introduciendo correcciones por razón del alcance de la conclusión, confirmó (parcialmente) la existencia de tal discriminación; para. 369.

[92] IRION, K., YAKOLOEVLA, S. y BARTI, M., nota 89, pp. 38-39.

[93] Las medidas deben ser i) relativas al suministro de servicios destinados directa o indirectamente a asegurar el abastecimiento de las fuerzas armadas; ii) relativas a las materias fisionables o fusionables o a aquellas que sirvan para su fabricación; iii) aplicadas en tiempos de guerra o en caso de grave tensión internacional.

[94] *Rusia – medidas relativas al tráfico en tránsito*, WT/DS512/r adoptado el 26.4.2019, paras. 97.108-97.109.

[95] Arts. 3.4 y 7, y 11 del Entendimiento sobre Solución de Diferencias (ESD).

material de esta exclusión no ha interpretado aún[96], resulta difícil pronunciarse en este momento sobre su utilidad en materia de protección de datos personales.

El Anexo sobre Servicios Financieros establece que, sin perjuicio del resto de las disposiciones del GATS, "no se impedirá que un Miembro adopte medidas "por motivos cautelares", entre ellos la protección de inversores, depositantes, tenedores de pólizas o personas con las que un proveedor de servicios financieros tenga contraída una obligación fiduciaria, o para garantizar la integridad y estabilidad del sistema financiero. Cuando esas medidas no sean conformes a las disposiciones del Acuerdo, no se utilizarán como medio de eludir los compromisos u obligaciones contraídos por el Miembro en el marco del Acuerdo" (párrafo 2.a). Dado que los motivos cautelares no se definen y la lista tiene carácter ejemplificador, pueden adoptarse medidas cautelares para proteger los datos personales relativos a la prestación de un servicio financiero. Por lo demás, la norma impide que tales medidas puedan utilizarse para justificar el incumplimiento del GATS, aunque con un lenguaje diferente al del artículo XIV.

Por su parte, el Anexo sobre Telecomunicaciones, centrado en facilitar el acceso y la utilización de las redes a los prestadores de estos servicios, obliga a los miembros a permitir el uso de redes y servicios públicos de transporte de telecomunicaciones para el movimiento y para el acceso a la información contenida en bases de datos o almacenada de otro modo en forma legible por máquina en el territorio de cualquiera de ellos y, en el caso de adoptar medidas que afecten significativamente a esa utilización, habrán de notificarlas y someterlas a consultas (punto 5.c). No obstante, con un lenguaje semejante al del artículo XIV GATS, se les permite adoptar medidas necesarias para garantizar la seguridad y la confidencialidad de los mensajes, siempre que no se apliquen de forma que constituya un medio de discriminación arbitrario o injustificable o una restricción encubierta del comercio de servicios (punto 5.d).

2. ACUERDOS DE LIBRE COMERCIO QUE INCLUYEN LA PROTECCIÓN DE DATOS PERSONALES

No cabe duda de que la protección de los datos personales puede provocar restricciones al comercio a las que debe hacerse frente sin menoscabar la protección de los derechos e intereses de los particulares. Lo acuerdos regionales y bilaterales de libre comercio, cuyo entramado va haciéndose cada vez más complejo, han comenzado a abordar la problemática que, para el comercio digital, plantea el muchas veces necesario e inevitable flujo de datos en general y personales, en particular.

En materia de protección de la información personal, privacidad o datos personales (expresiones que se utilizan en este contexto) EE.UU. y la UE cuentan con acuerdos que incorporan normas ubicadas, bien en capítulos dedicados al comercio electrónico, o bien en los relativos a la prestación de servicios y, de manera especial, en lo que concierne a los servicios financieros. No es extraño que los Estados adquieran compromisos dispares con diferentes países y que la complejidad del entramado de acuerdos pueda llegar a que éstos resulten entre sí contradictorios. En todo caso, las normas que contienen estos acuerdos, no sólo ofrecen ideas, sino que incluso son

[96] En el asunto WT/DS567 (actualmente en apelación), Arabia Saudita — Medidas relativas a la protección de derechos de propiedad intelectual, Informe del GE de 16.6.2020, alegó esta circunstancia, pero la insuficiencia de los fundamentos de la pretensión, en la que se incluían argumentos relativos a la infracción de normas de la OMC, llevó a considerar el asunto como enjuiciable; para. 7.17 y 18. El Informe del GE del GATT (no adoptado), *Estados Unidos - Comercio nicaragüense*, L/6053, 13.10.1986, se negó a formular recomendaciones por no esgrimirse infracción del Acuerdo en una situación de embargo comercial bilateral.

presentadas como propuestas en las negociaciones multilaterales en la materia iniciadas en 2019. Por lo tanto, no resulta ocioso aproximarse a las disposiciones más significativas que se han encontrado en estos acuerdos.

2.1 Esfera EE.UU.

Como se ha señalado, en el marco del APEC y para facilitar el flujo transfronterizo de los datos personales entre los Estados participantes -entre los que se encuentra EE.UU-, se implantó el Sistema de Normas de Privacidad Transfronteriza, cuyo cumplimiento es certificado públicamente[97]. Este modelo no ha sido adoptado aún en otros acuerdos de libre cambio.

Construido sobre el modelo del Acuerdo Transpacífico de Cooperación Económica (TTP; hoy *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* – CPTPP, también llamado TPP-11)[98] -del que formó parte EE.UU hasta 2017[99]-, el Acuerdo de libre comercio entre Canadá, EE.UU. y México (USMCA)[100] cuenta con un capítulo sobre comercio digital que incluye normas para proteger el flujo transfronterizo de datos y evitar "requisitos de localización".

Siguiendo al Convenio de Estrasburgo, el USMCA define la información personal, incluyendo los datos, como la relativa a una persona física identificada o identificable (art. 19.1). A partir de ahí, recoge el compromiso de las partes adoptar o mantener una estructura jurídica para su protección (ya sea con normas generales, para sectores específicos o que prevean el uso de compromisos voluntarios por parte de las empresas) y establece que, para ello, se tomarán en consideración los principios y guías internacionales relevantes, tales como la *APEC Privacy Framework*[101] y la Guía de Privacidad de la OCDE (art. 19.2). Se señala, además, que los principios de actuación en esta materia son: limitar la recogida; elección, calidad de los datos, especificación del propósito, limitación del uso, medidas de seguridad, transparencia, participación individual y responsabilidad (art. 19.3). Las partes "deben aspirar" a adoptar prácticas no discriminatorias para proteger frente a las infracciones de los datos personales (art. 19.4) y, reconociendo que pueden adoptar aproximaciones diversas para esta protección, se comprometen a dar publicidad sobre las mismas (art. 19.5) y a promover la compatibilidad de sus sistemas intercambiando información y explorando vías de actuación entre ellos (art. 19.6 y 19.14.1.a.i), en foros internacionales (art. 19.14.1.b,c y f) y con el sector privado (art. 19.14.1.d).

Además de prohibir "requisitos de localización" (art. 19.12) y de establecer de entrada la libertad de transferencia de información, incluida la personal, para el desarrollo de la actividad negocial (art. 19.11.1), reconocen la importancia de asegurar el cumplimiento de las medidas de protección de datos y que nada impide la adopción de

---

[97] *Vid.* nota 62.

[98] https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text, visitado en julio 2021. El actual *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP), 8.3.2018, del que forman parte Australia, Brunei Darussalam, Canadá, Chile, Japón, Malasia, México, Perú, Nueva Zelanda, Singapur and Vietnam; http://www.sice.oas.org/Trade/TPP/CPTPP/Spanish/CPTPP_Index_s.asp, visitado en julio 2021. Vietnam se unió en enero 2019 y cuenta con un período de 2 años antes de que el capítulo de solución de diferencias en materia de comercio electrónico le sea aplicable.

[99] https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text. Visitado en julio 2021.

[100] https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between Visitado en julio 2021.

[101] http://cbprs.org/ Visitado en julio 2021. *Vid.* también notas 60 a 62.

medidas restrictivas si resultan necesarias para perseguir un objetivo legítimo de interés público, siempre que cumplan los requisitos habituales de necesidad y proporcionalidad (arts. 19.3 y 19.11.2).

De otro lado, el nuevo Acuerdo sobre comercio digital entre EE.UU. y Japón (USJTA), que complementa al de libre comercio,[102] es señalado como el que contiene las disciplinas más fuertes. Aunque parte del patrón del USMCA en cuanto a la información personal (art.1.x.dd), sus normas son más escasas, sucintas y genéricas, llamando especialmente la atención la falta de salvaguardas. Así, se establece la obligación de contar con un régimen de protección transparente (art. 15.1 y 2) a la par que se libera la transferencia de datos (art. 11) y se prohíbe la exigencia del requisito de localización (arts. 12, en general, y 13, para los servicios financieros) sin incorporar mención alguna a las excepciones que pudieran ser necesarias para la protección de los datos personales conforme a los respectivos estándares nacionales (intereses públicos legítimos). No hay mención alguna a los estándares internacionales ni al intercambio de información y experiencias para cooperar en materia de protección información personal, más allá de promover que sus respectivos regímenes sean interoperativos (art. 15.3). Las diferencias con el USMCA resultan evidentes.

2.2 Esfera UE

En cuanto a la UE, algunos de los acuerdos, ya existentes o en negociación, incluyen definiciones sobre datos personales y sobre comercio electrónico. Siguiendo al Convenio de Estrasburgo, son datos personales cualquier información relativa a una persona física identificada o identificable[103]. El comercio electrónico, por su parte, se entiende como el realizado mediante telecomunicaciones, por sí solo o junto con otras tecnologías de la información y la comunicación[104].

El Acuerdo de asociación económica UE-Japón[105] cuenta con un capítulo específico sobre comercio electrónico, comercio de servicios y la liberalización de inversiones (capítulo 8). En cuanto al primero (sección F), se reconoce la importancia de adoptar o mantener medidas conformes con las respectivas legislaciones nacionales para proteger los datos personales de los usuarios del comercio electrónico (art.8.78.3); lo que supone reconocer la libertad de cada uno de ellos para actuar en este ámbito. En el terreno específico del comercio de servicios financieros (sección E.5), tras establecer la libertad de transferencia y procesamiento de información financiera necesaria para el desarrollo del negocio habitual del prestador de servicios, se señala que esto no será óbice para la protección de la privacidad y de los datos personales (art. 8.63). Por lo demás, con carácter

---

[102] *U.S. - Japan Digital Trade Agreement,* 7.10.2019, https://ustr.gov/sites/default/files/files/agreements/japan/Trade_Agreement_between_the_United_States_and_Japan.pdf. Visitado en julio 2021.

[103] Nuevo acuerdo de asociación (partenariado económico) UE-México (que sustituirá al del año 2000); https://trade.ec.europa.eu/doclib/press/index.cfm?id=1833; pendiente de la culminación del proceso de ratificación para su entrada en vigor; Acuerdo UE-Australia, actualmente en negociación, art. 6.4 (capítulo II) https://trade.ec.europa.eu/doclib/press/index.cfm?id=1865., visitados en julio 2021. Sin embargo, el Acuerdo Económico y Comercial Global entre Canadá y la UE y sus EM (CETA), *DO*, L 11, 14.1.2017, no incluye estas definiciones.

[104] Por ejemplo, en el UE-Canadá, art. 16.1, nota 103. En la era digital, los proveedores de servicios de telecomunicación han expandido su actividad alcanzando a los servicios de Internet. De ahí que se haya señalado la conveniencia de revisar y reforzar esta regulación con el fin de asegurar la competencia, FEFER, R.F., *Internet Regimes and WTO E-Commerce Negotiations*, US Congressional Research Service, R.46198, January 2020, p. 4.

[105] Acuerdo de asociación económica UE-Japón, en vigor desde el 1.1.2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684, Visitado en julio 2021.

general (Sección A), las normas de este capítulo pueden excepcionarse, siguiendo el modelo del artículo XX GATT, cuando resulte necesario para asegurar el cumplimiento de normas nacionales relativas a la protección de la privacidad de los individuos en lo que concierne al procesamiento y difusión de sus datos personales y la confidencialidad de sus informes y cuentas (art. 8.3.c.ii)[106]. En esta línea, el capítulo 18 del Acuerdo, destinado a las buenas prácticas y a la cooperación reguladora, salvaguardando el derecho de cada Estado a definir y regular sus propios niveles de protección para la consecución de sus objetivos de interés público en materia de datos personales y ciberseguridad (art. 18.2.h), establece el compromiso de promover las buenas prácticas mediante la transparencia, el debate, la búsqueda de la compatibilidad normativa y cooperando en foros internacionales (art. 18.1). Obviamente, los términos de este acuerdo contrastan con los del existente entre Japón y EE.UU. Por lo demás, no puede dejarse de notar que, la UE autoriza la transferencia de datos personales a Japón sobre la base de una Decisión de la Comisión[107].

Como en el caso de Japón, el Acuerdo de la UE con Singapur[108] también cuenta con un capítulo 8 sobre servicios, establecimiento y comercio electrónico. Las normas sobre transferencia de datos personales para su procesamiento se limitan de nuevo a los servicios financieros (Sección E.6), sentando la libertad de transferencia en el curso normal del desarrollo del negocio, eso sí, sujeta a las salvaguardas adecuadas de privacidad y confidencialidad (art. 8.54.1). En esta línea, cada parte se compromete a adoptar o mantener medidas para proteger la privacidad y los datos personales siempre no se utilicen para incumplir las obligaciones del Acuerdo (art. 8.54.2). Por lo demás, se incorpora también la excepción general en lo que concierne a las medidas para proteger la seguridad, la moral o el orden públicos, así como las que resulten necesarias para asegurar el cumplimiento de leyes y reglamentos conformes con el Acuerdo, incluyendo aquellas relativas a la protección de la privacidad de los individuos en el procesamiento y difusión de sus datos personales y la confidencialidad de sus informes y cuentas personales (art. 8.62. a y e.ii – Sección G).

En el caso del Acuerdo de la UE con Vietnam[109], de nuevo el capítulo 8 se ocupa de liberalización de inversiones, comercio de servicios y comercio electrónico. Sin embargo, más allá de declarar que nada en el Acuerdo restringe el derecho de cada parte a proteger la privacidad y los datos personales en tanto tal derecho no se utilice para incumplir el Acuerdo (art. 8.45.3) y de establecer que cada parte adoptará o mantendrá medidas apropiadas para proteger los datos personales y la privacidad, incluyendo los informes y cuentas individuales (art. 8.45.1); las obligaciones sobre la transferencia de datos, igualmente limitadas al sector financiero, se posponen. Transcurridos dos años de su entrada en vigor, la transferencia de datos habrá de ser posible en dicho sector para que los proveedores de estos servicios puedan llevar a cabo su actividad negocial ordinaria (art. 8.45.2). Además, el acuerdo incorpora la excepción general clásica (art. 8.53).

El Acuerdo entre la UE y Canadá (CETA)[110] contiene un capítulo específico sobre comercio electrónico (16) en el que las partes se comprometen a adoptar o mantener

---

[106] No se hace, sin embargo, referencia al art. XIV GATS. Esta excepción aparece en los mismos términos en el Acuerdo UE-Mercosur, de 28.6.2019, pero ubicada el título sobre comercio de servicios y establecimiento, sección de disposiciones finales y excepciones (4). La sección sobre comercio electrónico (6) no contiene referencias a los datos personales. https://trade.ec.europa.eu/doclib/press/index.cfm?id=2048. Visitado en julio 2021.

[107] *Vid.* nota 24.

[108] Acuerdo de libre comercio y promoción de inversiones, firmado el 19.10.2018, *DO* L 294, 14.11.2019, en vigor desde el 21.11.19.

[109] *DO* L 186/44, 12.6.2020, en vigor desde el 1.8.2020.

[110] *Vid.* nota 103.

nomas para la protección de la información personal de los usuarios tomando en consideración las normas internacionales de protección de datos (art. 16.4) y acuerdan mantener un diálogo sobre la protección de la información personal (art. 16.6.d) que podrá abarcar el intercambio de información así como la puesta en común de experiencias relativas a sus respectivos sistemas jurídicos en la materia (art. 16.6.2). También afirman la importancia de participar en foros internacionales para promover el desarrollo del comercio electrónico (art. 16.6.3). Sólo en el ámbito de los servicios financieros (capítulo 15) se establece expresamente que, además de contar con salvaguardias adecuadas para proteger la privacidad, en particular por lo que respecta a la transferencia de datos personales, las transferencias de información que incorporen este tipo de datos deberán ser conformes con la legislación del Estado parte en la que se hayan originado (art. 13.15)[111]. En el caso de servicios de telecomunicaciones, tras acordar el libre acceso a las redes o servicios públicos de transporte de telecomunicaciones para la circulación y acceso a la información, se establece que las Partes adoptarán medidas para proteger la privacidad de los usuarios pudiendo éstas constituirse en excepciones siempre que resulten necesarias y no constituyan una discriminación arbitraria o injustificada ni restricción encubierta del comercio (art. 15.3.4.b). Por lo demás, aunque no se mencione expresamente, cabría esperar intercambios de información y de experiencias en materia de protección de datos en el marco de la cooperación en materia de reglamentación (capítulo 21), que encaja con la política de transparencia (capítulo 27)[112].

El acuerdo de comercio entre la UE y el Reino Unido[113] cuenta con un título específico sobre comercio digital en el que se establece el compromiso de no obstaculizar el comercio con requisitos que supongan la localización (art.DIGIT 6 - 201). No obstante, se reafirma el legítimo derecho a regular en atención a sus respectivos intereses públicos en lo que concierne a la privacidad y la protección de datos (art.DIGIT 3 - 198) y se reconoce el derecho de los individuos a la protección de ambos, asumiendo que las partes podrán adoptar o mantener las medidas que estimen oportunas a estos efectos -incluyendo las relativas a la transferencia de datos- informándose mutuamente (art.DIGIT 7 - 202). Llama la atención que el compromiso de cooperación regulatoria en esta materia de comercio digital excluya expresamente las normas y salvaguardias para la protección de los datos personales y la privacidad, incluidas las transferencias transfronterizas de datos personales (art.DIGIT 16 - 211). Asimismo, se mantiene la posibilidad de recurrir a la excepción general (arts.DIGIT 4 y 16 y EXC.1 – 199, 211 y 412). La UE ya adoptado una decisión de adecuación en cuanto a la protección de datos en el Reino Unido[114].

En cuanto a algunos de los acuerdos que actualmente negocia la UE, según la información hecha pública, el texto del Acuerdo para modernizar el ya existente entre la UE y México[115] contaría con un capítulo sobre comercio digital que, en materia de protección de datos y de privacidad, se limita a reafirmar la libertad de cada parte de

---

[111] Se trata de la determinación de la ley aplicable a la transferencia de datos personales (*lex originis*). En esta línea, el capítulo 10, sobre entrada temporal establece las partes se facilitan la información sobre entrada temporal de empresarios siempre conforme a sus propias normas en materia de privacidad y protección de datos (art. 10.4.2).

[112] Así, por ejemplo, art. 10.4.1 (para entrada temporal).

[113] Acuerdo de comercio y cooperación UE – Reino Unido, DO L 149, 30.4.21. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX%3A22021A0430%2801%29&from=EN, visitado en julio 2021.

[114] *Vid*. nota 24.

[115] *Vid*. nota 103. https://trade.ec.europa.eu/doclib/press/index.cfm?id=1833. Visitado en julio 2021. El actualmente vigente Acuerdo de asociación económica, *DO* L 276, 28.10.2000, contempla la protección de datos (art. 51) conviniendo establecer un marco de cooperación para "prevenir los obstáculos a los intercambios que requieran la transferencia de datos personales" (arts. 20 y 41) conforme a los estándares internacionales y los marcados por el Derecho de la UE (Anexo V).

regular en sus respectivos territorios con el fin de alcanzar sus objetivos de interés público (art. 1.2)[116]. La posibilidad de acordar la libre circulación de datos se pospone a una negociación que tendría lugar tres años después de la entrada en vigor del Acuerdo (artículo XX).

En el caso de las negociaciones con Australia[117] y con Nueva Zelanda[118], el título sobre comercio digital de las propuestas[119], tras reafirmar el derecho de cada parte a regular en materia de privacidad y de protección de datos (art. 2), reconoce expresamente su carácter de derecho fundamental (art. 6.1) y establece que nada en el Acuerdo afectará su protección conforme a las normas de cada parte, que podrán adoptar y mantener las medidas que estimen apropiadas para su protección, incluyendo las relativas a las transferencias internacionales, con la única obligación de informarse mutuamente sobre las que adopten (art. 6.2 y 3). Así, la protección de datos puede escapar de la acordada liberalización del flujo de datos que resulta de la prohibición de requisitos de localización; norma que se sujetaría a revisión en un plazo de tres años tras la entrada en vigor del Acuerdo (art. 5)[120]. En consonancia con el reconocimiento a la absoluta libertad de las partes en materia de protección de los datos personales y la privacidad, se excluye expresamente esta cuestión -incluso en su dimensión de transferencia de datos- de las disposiciones sobre intercambio de información y cooperación (art. 14.2).

Aunque esté en consonancia con el reconocimiento de la absoluta libertad de las partes en materia de protección de datos, resulta llamativo que se excluya expresamente el intercambio de información y de experiencias en la materia cuando parecería que, al reconocer ambos contratantes el carácter de derecho fundamental de esta protección, comparten un punto esencial de arranque para una más sencilla aproximación de cara a esos intercambios que, tanto la UE como Australia, mantienen, sin embargo, en el marco de acuerdos firmados respectivamente con otros países.

2.3 Visión panorámica

Se observa así cómo, a través de las relaciones bilaterales, tanto la UE como EE.UU. incorporan cuestiones relativa a los datos personales con impacto en el comercio sobre las que plantean sus respectivas aproximaciones y tratan de expandir sus respectivos modelos. De modo paralelo, además de contribuir en cierta medida a un establecimiento y expansión de estándares mínimos internacionales, la diversidad de compromisos puede

---

[116] *Ibid*. En esta línea, el Anexo X-7 sobre comercio transfronterizo en materia de servicios financieros señala expresamente que los datos personales de las informaciones y datos financieros serán tratados conforme a la ley mexicana que los regule. Por lo demás, el Acuerdo excluye ciertos sectores de los compromisos adquiridos en materia de comercio digital (art. 1.4)

[117] *Vid*. nota 103.

[118] https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157581.pdf., visitado en julio 2021. Nueva Zelanda cuenta con la autorización de la Comisión para la transferencia de datos desde la UE, *vid*. nota. 24.

[119] Como en el caso del de México, nota 103, excluyen ciertos sectores de la conclusión de contratos por medios electrónicos (art. 9.2). *Vid.* también el caso de las negociaciones con Australia, nota 103, y Nueva Zelanda, nota 117.

[120] *The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by: a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party; b) requiring the localisation of data in the Party's territory for storage or processing; c) prohibiting storage or processing in the territory of the other Party; d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.*

llegar a colocar a terceros países en situaciones complicadas. Así, con carácter general y más allá de otras consideraciones legales (excepciones al TNMF de los acuerdos de libre comercio tanto en GATT como en GATS), mientras como miembro del USMCA, Canadá está sujeta a la libertad de transferencia de datos, en virtud de sus compromisos con la UE, que ha reconocido la adecuación de su normativa de protección de datos a los efectos de la exportación de los correspondientes a los residentes comunitarios, no podrá facilitar la transmisión de éstos a EE.UU. ni a México.

En todo caso, el pasado 15 de junio de 2021, la UE y EE.UU. han puesto en marcha un Consejo bilateral de Comercio y Tecnología con el fin de buscar enfoques coordinados sobre cuestiones fundamentales en materia de economía, comercio y tecnología sobre la base de "valores democráticos compartidos". En su seno se incluye un grupo de trabajo sobre "Gobernanza de datos y plataformas tecnológicas"[121]. En la línea de intensificar el comercio y la inversión y de evitar obstáculos técnicos al comercio en este terreno, cabe destacar la importancia del objetivo común de facilitar la "cooperación en materia de política reguladora y de ejecución", así como de "cooperar en el desarrollo de normas compatibles e internacionales" que, cabría esperar, aborden en alguna medida la protección de los datos personales y la privacidad.

3. NEGOCIACIONES MULTILATERALES SOBRE COMERCIO ELECTRÓNICO Y PROTECCIÓN DE DATOS EN LA OMC

Como reconoce la OCDE, en particular respecto del comercio de servicios digitales, los beneficios de la digitalización se ponen en peligro por los obstáculos al comercio pues la complejidad del entorno normativo global, que incluye la adopción de medidas legítimas para proteger los datos personales y la privacidad, ha ido creciendo progresivamente; lo que pone más aún de relieve la necesidad de un mayor diálogo y cooperación internacional[122].

1. OMC y comercio digital

Desde la creación de la OMC, el comercio digital constituye un pilar fundamental de su agenda de actuaciones. Si bien es cierto que el foco inicial se centró únicamente en el comercio internacional de productos tecnológicos (ordenadores, equipos de telecomunicación, semiconductores, software, instrumentos científicos etc. y gran parte de sus componentes y accesorios) suprimiendo los aranceles[123], la importancia del comercio electrónico llevó a la organización adoptar una Declaración para establecer un

---

[121] Comunicado de Prensa 15.6.2021, La UE y los Estados Unidos ponen en marcha el Consejo de Comercio y Tecnología para liderar la transformación digital mundial basada en valores, https://ec.europa.eu/commission/presscorner/detail/es/IP_21_2990. Visitado en julio 2021.

[122] FERENCZ, J., *Digital Services Trade Restrictiveness Index* (STRI), OECD Trade Policy Papers, núm. 221, 2019, que identifica, cataloga y cuantifica barreras al comercio digital de servicios de datos en 44 países, entre 2014 y 2018, pp. 6-10.

[123] *Information Technology Agreement* (ITA), Declaración Ministerial sobre Comercio y Productos de las Tecnologías de la Información, WT/MIN(96)/16, 13 de diciembre de 1996. Como resultado de la Conferencia Ministerial de Nairobi, 2015, se amplió el número de productos. Actualmente, 82 miembros de la OMC han suscrito este acuerdo y, desde 2000 (G/IT/19, de 13.11.20009; Programa de trabajo sobre medidas no arancelarias) se debate sobre su extensión a las barreras no arancelarias (declaraciones de conformidad, etiquetado y transparencia). *Vid*, Informe (2019) del Comité de Participantes sobre la Expansión del Comercio de Productos de Tecnología de la Información, G/L/1334, 5.11.2019. La UE ha solicitado la celebración de consultas con India en el marco del procedimiento de arreglo de controversias de la OMC pues comenzó a imponer tarifas a algunos productos de tecnologías de la información y comunicación; WTO/DS582. Otros países se han sumado (EE.UU. y otros cinco más).

Programa de trabajo en la materia, comprometiéndose los Miembros a mantener la práctica acordada en 1998, sucesivamente prorrogada ("moratoria")[124], de no imponer derechos de aduana a las transmisiones electrónicas.

El Programa entiende por comercio electrónico "la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos … incluye también el examen de cuestiones relacionadas con el desarrollo de la infraestructura del comercio electrónico"[125]. Por lo tanto, el comercio electrónico comprende el uso de internet para realizar búsquedas, compras, ventas, entregas de bienes y servicios en línea, lo que supone incorporar a este concepto el acceso a internet y los flujos de datos personales[126].

Concluyendo 2017, distintos Estados parte de la OMC confirmaron su intención de avanzar en esta materia y firmaron la Primera Declaración sobre Comercio Electrónico. En ella, tras reconocer la importancia de la Organización en la promoción de entornos normativos abiertos, transparentes no-discriminatorios y previsibles para facilitarlo, anunciaban su intención de iniciar trabajos exploratorios conjuntos de cara a una futura negociación sobre los aspectos comerciales relacionados con el comercio electrónico[127]. En una segunda Declaración en enero de 2019, confirmaron la "intención de entablar negociaciones en la OMC sobre los aspectos del comercio electrónico relacionados con el comercio" con el objetivo de "alcanzar un resultado de alto nivel que se base en los Acuerdos y marcos de la OMC existentes, con la participación del mayor número posible de Miembros" y reconociendo y teniendo en cuenta "las oportunidades y los desafíos únicos a los que se enfrentan los Miembros, incluidos los países en desarrollo y los menos adelantados (PMA), así como las microempresas y las pequeñas y medianas empresas"[128]. En la actualidad, el número y la diversidad de desarrollo económico de los Estados participantes en las ya iniciadas negociaciones es significativo[129]. Cabe destacar, sin embargo, la ausencia de países como Sudáfrica e India, que parecen querer proteger su flexibilidad y espacio político[130]. Por lo demás, no se entiende la ausencia de Vietnam puesto que, en tanto en sus relaciones con la UE como en el marco del TPP, tiene compromisos en la materia y, en particular, en lo que concierne a la privacidad.

En este marco, las propuestas de distintos Estados, además de tratar de convertir la "moratoria" en una obligación jurídica, se pretende regular algunos aspectos materiales del comercio digital y así como encontrar mecanismos para impedir que los Estados adopten medidas que pudieran suponer restricciones al comercio electrónico, incluso cuando no lo regulen directamente. Las propuestas revelan que los miembros de la OMC son conscientes del carácter central de este tema en general y, dentro del mismo, de la

---

[124] *Vid*. nota 74. Además de algunos países en desarrollo como Indonesia, India y Sudáfrica se oponen a la prórroga. WT/GC/W/747, de 13.7.2018. La situación actual de la moratoria es, cuando menos, dudosa.

[125] WT/L/274, de 30.9.1998. Se encargan de su aplicación: el Consejo del Comercio de Servicios; el Consejo del Comercio de Mercancías; el Consejo de los ADPIC; y el Comité de Comercio y Desarrollo.

[126] WUNSCH-VINCENT, S. *WTO, E-commerce, and Information Technologies: From the Uruguay Round through the Doha Development Agenda, A Report for the UN ICT Task Force*, MCINTOSH, J., Ed. Markle Foundation, 2004, pp. 1-2, agrupa los bienes y servicios tecnológicos en cinco categorías: 1) bienes tecnológicos; 2) servicios de infraestructuras; 3) servicios prestados electrónicamente; y 4) productos digitales.

[127] WT/MIN(17)/60, de 13.12.2017.

[128] WT/L/1056, de 25.1.2019.

[129] Inicialmente, 71. A julio de 2021, son 86, contando los 27 Estados miembros de la UE. A título ilustrativo, participan tanto Guatemala, Colombia, Filipinas, Costa de Marfil, Kenia etc. Los patrocinadores de la negociación son Australia, Japón y Singapur.

[130] India no apoya la continuación de la "moratoria", *vid*. nota 124, y, además, el 14.5.2019, Japón inició contra ella una disputa por imponer aranceles a productos tecnológicos en violación del ITA; WT/DS584.

circulación de datos sin perder de vista la protección de la privacidad, incluso para la propia supervivencia de la propia OMC[131].

Las negociaciones están organizadas en torno a ocho grupos (*focus groups*). El grupo A, en la que los trabajos se encuentran más avanzados, se centra en permitir el comercio digital/*e-commerce* y abarca las cuestiones básicas de confianza tales como los contratos y la firma electrónicas, así como el *spam*. El grupo B se ocupa de la apertura y en el comercio digital/*e-commerce*, abarcando, entre otras, las cuestiones más complejas sobre el flujo de datos, la no discriminación en los contenidos digitales, la responsabilidad y el acceso a Internet y a los datos. El grupo C se ocupa de la confianza, comprendiendo la protección del consumidor, la privacidad y la confianza empresarial. El grupo D se ocupa de las cuestiones trasversales tales como la transparencia, ciberseguridad, creación de capacidad, cooperación, regulación nacional y otros asuntos jurídicos. Finalmente, el grupo E aborda las telecomunicaciones y el F el acceso a los mercados.

No cabe duda de que el tratamiento de la privacidad en el flujo internacional de datos, atribuido a los grupos B y C, constituye uno de los temas más complejos al poner de relieve, no sólo los intereses económicos, sino también las diferentes aproximaciones nacionales a la protección de los datos y de la privacidad y, en consecuencia, los distintos objetivos perseguidos por los negociadores. Se trata de una cuestión trasversal que, como se ha visto, afecta al comercio de mercancías y servicios, pero lo excede y supera ampliamente. En este contexto, tanto la acción política como los discursos se mueven entre la defensa de la protección de la privacidad y los datos y las acusaciones de proteccionismo económico[132].

2. Posiciones negociadoras

Debe tenerse en cuenta que esta negociación se sitúa en un contexto de reivindicaciones nacionales sobre la soberanía de Internet (*Internet Sovereignty*) o ciber-soberanía (*Cyber Sovereignty*) que tiene diferentes alcances para distintos Estados. En China, esta reivindicación responde a un modelo de gobernanza que supone que todos los países deben respetar sus respectivos derechos a elegir el camino para su ciber-desarrollo, su modelo de ciber-regulación y políticas públicas de internet, así como participar en la gobernanza del ciberespacio internacional en términos de igualdad[133]. La UE, por su parte, utiliza la expresión de soberanía digital recordando que su política debe reflejar "los valores de nuestra sociedad, fomente la inclusión y siga siendo compatible con nuestro modo de vida" y, en esta línea, señala el carácter "vital de fomentar la igualdad de condiciones, particularmente en el ámbito del comercio … (lo que) significa garantizar una competencia leal … a escala mundial, fomentar el acceso al mercado, luchar contra las prácticas desleales, las medidas extraterritoriales y los riesgos que para la seguridad plantean terceros países … ".[134] En el caso de EE.UU., el objetivo es mantener una red

[131] Entre otros, JOB/GC/94 US; /97 EU; /98 Brasil; /99 países MIKTA (México, Indonesia, Corea del Sur, Turquía y Australia); /110 China y Pakistán. Por su parte /96 Japón *et al.* y /101/Rev.1, Singapur *et al*., no incorporan referencia alguna a la privacidad.

[132] YAKOVLEVA, S., "Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy", *U. Miami L. Rev.* vol. 74, 2020, p. 416, https://repository.law.miami.edu/umlr/vol74/iss2/5

[133] FEFER, R.F., nota 104, pp. 10-11.

[134] Consejo de la UE, *Una nueva agenda estratégica 2019-2024*, Junio 2019, p.4, https://www.consilium.europa.eu/media/39964/a-new-strategic-agenda-2019-2024-es.pdf, visitada en octubre 2020. "La transformación digital se seguirá acelerando y tendrá repercusiones de gran alcance. Debemos garantizar que Europa … obtenga la parte del beneficio que le corresponde en esta evolución. … Para ello, la UE debe trabajar en todos los aspectos de la revolución digital y la inteligencia artificial:

global abierta, interoperativa, confiable y segura. Por lo tanto, la aproximación al gobierno de internet de la UE es de menor control estatal que la china, que ha sido calificada como de autoritarismo digital (*digital authoritarianism*)[135], pero más reguladora que la estadounidense[136].

EE.UU. concibe las normas que prohíben la transferencia internacional de datos como limitaciones la libertad de circulación de la información; lo que ahoga la competencia y perjudica a las empresas digitales. De ahí que su propuesta negociadora[137] pretenda articular normas comerciales apropiadas que combatan barreras discriminatorias a través de la protección de los movimientos de datos dando entrada a medidas de salvaguarda razonables, como puede ocurrir en caso de necesidad de proteger datos de los consumidores que vayan a ser exportados. Vinculado a este planteamiento, se pretende prohibir la imposición de obligaciones relativas al procesamiento de datos (localización) con el fin de evitar que los Estados fuercen a los proveedores de productos o servicios que se apoyan en la nube para desarrollar su actividad, a crear infraestructuras y centros de datos en cada país en el que operen, pues estas exigencias de localización añaden costes y cargas innecesarias tanto para los propios proveedores como para los consumidores.

China, por su parte, aboga por el respeto a las diferentes políticas de los miembros sobre la protección de la información personal entendiendo las diferencias en cuanto a "las tradiciones históricas y culturales y los sistemas jurídicos de cada Miembro … y el derecho legítimo a adoptar medidas de reglamentación para cumplir objetivos razonables de su política pública" [138], y no incluye obligaciones en relación al procesamiento de datos. Resulta obvia la escasa coincidencia entre las posiciones de EE.UU. y China, lo que ilustra las dificultades para alcanzar resultados significativos en las negociaciones.

La posición negociadora de la UE sobre flujos transfronterizos de datos[139], tras reconocer el compromiso de liberalización estableciendo obligaciones que supriman cualquier exigencia de localización, incide en el carácter de derecho fundamental de la privacidad y de los datos personales y propone una amplia excepción para las restricciones de transferencias internacionales de los mismos. Esta posición permite a la UE hacer compatible su régimen interno de protección de datos con compromisos internacionales.

> *2.7 FLUJOS TRANSFRONTERIZOS DE DATOS*
>
> *1. Los Miembros se comprometen a asegurar el flujo transfronterizo de datos a fin de facilitar el comercio en la economía digital. A tal efecto, los flujos transfronterizos de datos no se restringirán:*
>
> *a) exigiendo el uso de instalaciones informáticas o elementos de la red en el territorio del Miembro para el procesamiento de los datos, en particular imponiendo el uso de instalaciones informáticas o elementos de la red que estén certificados o aprobados en el territorio del Miembro;*
>
> *b) exigiendo la localización de los datos en el territorio del Miembro para su almacenamiento o procesamiento;*

---

infraestructuras, conectividad, servicios, datos, reglamentación e inversión. Ello debe ir acompañado por el desarrollo de la economía de los servicios y por la integración de los servicios digitales"

[135] FEFER, R.F., nota 104, p. 11. Se entiende por autoritarismo digital una forma de controlar a la población nacional; el "gran cortafuegos" (*Great Firewall*), que bloquea o censura páginas web extranjeras.

[136] *Ibid*, p. 9.

[137] United States, *Joint Statement on Electronic Commerce*, WTO/INF/ECOM/23, April 26, 2019. JOB/GC/94, 4 July, 2016.

[138] China, *Declaración conjunta sobre el comercio electrónico*; WTO/INF/ECOM/19, 23.04.2019, paras. 3.9 y 4.1, y WTO/INF/ECOM/40, 23.9.2019 (acceso restringido).

[139] *Propuesta de la UE sobre Disciplinas y Compromisos relativos al comercio electrónico*, INF/ECOM/22, 26.4.2019, paras. 2.7-2.8.

> *c) prohibiendo el almacenamiento o procesamiento en el territorio de otros Miembros;*
>
> *d) supeditando la transferencia transfronteriza de datos al uso de instalaciones informáticas o elementos de la red en el territorio del Miembro o a requisitos de localización en el territorio del Miembro.*
>
> *2.8 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD*
>
> *1. Los Miembros* ***reconocen que la protección de los datos personales y de la privacidad es un derecho fundamental*** *y que las normas estrictas a este respecto contribuyen a generar confianza en la economía digital y a fomentar el comercio.*
>
> *2. Los Miembros* ***podrán adoptar o mantener las salvaguardias que estimen adecuadas para asegurar la protección de los datos personales y de la privacidad,*** *entre otras cosas, mediante la adopción y aplicación de normas para la transferencia transfronteriza de datos personales.*
>
> ***Nada de lo dispuesto en las disciplinas y los compromisos acordados afectará a la protección de los datos personales y la privacidad otorgada por las respectivas salvaguardias de los Miembros****.*
>
> *3. Por datos personales se entiende cualquier información relativa a una persona identificada o identificable.*

Este texto es el mismo que la UE utiliza en las negociaciones bilaterales de acuerdos de libre comercio actualmente en curso[140]. Resulta difícil imaginar la acogida en la OMC del reconocimiento de la protección de datos personales como un derecho fundamental dado que esto no se ha producido a escala internacional general y hay países que no concuerdan con este planteamiento.

Por lo demás, el texto se asemeja a la excepción de seguridad nacional del GATT (art. XXI, o su correspondiente XIVbis I.b GATS) en el sentido de que, quien valora la necesidad y adecuación de la medida es el propio Estado que la adopta[141]. Al colocar la protección de la privacidad y los datos personales al mismo nivel de importancia que la seguridad nacional, la posición negociadora de la UE es diferente de la de EE.UU., cuyo modelo incluye una amplia exigencia de no prohibir o restringir transferencias internacionales de información, incluyendo los datos personales, y una excepción semejante a la general (art. XX GATT o XIV GATS).

Las propuestas de países en desarrollo tienden a mantenerla libertad de los Estados para fijar sus prescripciones reglamentarias sobre transferencia de información que permitirá los flujos de datos en el marco de actividades comerciales sin perjuicio de excepciones justificadas y dejando las cuestiones de privacidad al ámbito de la cooperación reguladora[142]. Los países menos desarrollados adoptan una aproximación más relajada; probablemente para atraer datos y, a través de ellos, inversiones.

Con carácter general, la industria apoya estas negociaciones sobre comercio electrónico como una forma para alcanzar normas vinculantes que ofrezcan seguridad jurídica para el crecimiento del comercio internacional. Por su parte, la llamada sociedad civil parece encontrarse dividida. Frente a quienes se oponen totalmente por considerar que la regulación favorecerá a las grandes compañías tecnológicas a costa de las de los países en desarrollo y sus trabajadores[143]; hay quienes las apoyan siempre que, contando con su participación, se centren en la transparencia y en la protección de los derechos de los consumidores, promoviendo la competencia, asegurando la resolución de disputas y el acceso de los ciudadanos a sus datos en línea, rechazando que la protección de datos y

---

[140] *Vid.* notas 103 y 118, en concreto, Australia y Nueva Zelanda.

[141] *Vid.* nota 96.

[142] *Vid.* por ejemplo, Brasil, *Declaración conjunta sobre el comercio electrónico*, WT/INF/ECOM/27, 30.4.2019, secciones VII y VIII.

[143] *Civil society letter against digital trade rules in the WTO*; 1 April, 2019, https://www.somo.nl/civil-society-letter-against-digital-trade-rules-in-the-world-trade-organization-wto/; visitado en octubre 2020.

la privacidad formen parte de un acuerdo de comercio[144]. Por lo demás, cabe destacar la comunicación que, a través de distinto tipo de reuniones, se establece entre representantes de asociaciones de consumidores y los representantes de los miembros de la OMC cuyo objetivo es promover la transparencia de las negociaciones y el diálogo entre las múltiples partes interesadas[145].

A pesar de las diferentes aproximaciones de la UE y de EE.UU. al tratamiento de la protección de datos personales en general y en el marco de estas negociaciones de la OMC en particular, no puede dejarse de notar que ambos comparten la preocupación sobre el acceso indiscriminado a los datos personales por autoridades públicas extranjeras. En el caso de la UE, así lo prueba la doctrina del TJUE en los asuntos *Schrems*, en particular, respecto de las autoridades estadounidenses por razón de la aplicación del Derecho de este país. En el caso de EE.UU., un Informe al Congreso de EE.UU afirma taxativamente: "*If Chinese companies need to follow domestic Chinese laws and Chinese government directives, U.S. and other officials fear that sensitive data involving their citizens and corporate entities could be exposed to the Chinese government*"[146], mostrando así su preocupación por el acceso de las autoridades chinas a los datos personales de los estadounidenses. No obstante, EE.UU., tiende a tachar proteccionista la política comunitaria en la materia, argumentando que está diseñada para permitir el desarrollo de grandes empresas que puedan competir con las estadounidenses y con las chinas[147].

V. CONCLUSIONES

El tráfico transfronterizo de datos, incluidos los datos personales, es inherente al desarrollo del comercio digital. Mientras que el derecho humano a la privacidad está universalmente reconocido, su alcance en lo que concierne a la protección de datos personales no cuenta con una lectura uniforme pues, si bien en algunos lugares constituye un derecho fundamental, en otros carece de esta consideración. En este contexto, la regulación nacional de la protección de la privacidad y de los datos personales, como la de cualquier objetivo legítimo de interés público nacional, está ligada a los valores constitucionales y éticos que persiguen los diferentes Estados. Sus respectivos ordenamientos internos pueden limitar o condicionar la transferencia o "exportación" de estos datos a terceros países de forma que las restrinjan, o incluso las bloqueen, dando lugar a obstáculos al comercio internacional de bienes y, fundamentalmente, de servicios que, eventualmente, podrían llegar a constituir infracciones de los compromisos adquiridos en virtud de los acuerdos de la OMC o, incluso, de otros acuerdos de libre comercio.

En el caso de la UE, los asuntos *Schrems* ilustran claramente la situación que, por lo demás, ya reconocía y anticipaba el Convenio de Estrasburgo y distintas iniciativas

---

[144] KILIC, B. y AVILA, R. *Opening Spaces for Digital Rights Activism;* report, 30 January 2019, *y Statement de Public citizen digital rights program*, 31 October 2019. Bureau Européen des Unions de Consummateurs (BEUC), *Recommendations on WTO e-Commerce Negotiations*, BEUC/AISBL, 29.3.2019, pp. 6-7.

[145] *Summary of points raised by consumers groups*, https://www.wto.org/english/news_e/news19_e/summary_of_points_raised_trdia_06may19_e.pdf, visitado en julio 2021.

[146] FEFER, R.F., nota 104, p. 13.

[147] En esta línea, servicios de alojamiento en la nube como *Gaia-X*, proyecto franco-alemán (políticos, empresarios y científicos) que cuenta con la participación de otros Estados y la UE; https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html; y *Nextcloud* https://nextcloud.com/about/. Visitados en julio 2021.

desarrolladas en el marco de organizaciones internacionales. Estas actuaciones se centran en el establecimiento de estándares mínimos que, sentando un sustrato común, tienen como objetivo facilitar el tráfico transfronterizo de datos sin sujetarlo, salvo en circunstancias excepcionales, a requisitos o condiciones de localización que limiten u obstruyan el comercio internacional. No obstante, el grado de armonización no acaba con las diferencias normativas y el recurso a las excepciones para la protección de intereses públicos legítimos ofrece márgenes de maniobra, tanto en el Convenio de Estrasburgo como en los acuerdos de la OMC y en los de liberalización comercial/regional del comercio (existentes y en negociación), cada uno en distinta medida.

El inicio de las negociaciones multilaterales sobre comercio electrónico en la OMC con una elevada y diversa participación de Estados miembros –con diferentes niveles de desarrollo económico y tecnológico- así como con la implicación de organizaciones de la sociedad civil, ofrece nuevas perspectivas para abordar la cuestión. Parece obvio que las experiencias e información acumuladas en los distintos acuerdos regionales deben contribuir a facilitar cierta aproximación de manera que se favorezca el acercamiento y la profundización en cuanto a los estándares mínimos de protección de los consumidores, su privacidad y sus datos personales, así como mecanismos para hacer efectivos sus derechos. En este sentido, aunque las propuestas no entren a tratar directamente esta cuestión, no puede dejarse de notar que la aplicación territorial de las normas nacionales no resulta discutida si bien, paralelamente, para el tratamiento de los datos personales de los no residentes el criterio de la *lex originis* parece abrirse camino. Por lo demás, es importante ser conscientes de que la propia tecnología tendrá un papel paralelo y definitivo en la fijación de estándares (*privacy by design*). Asimismo, los mecanismos de certificación y control podrían llegar a constituir una herramienta útil. Todo ello, sin perjuicio de salvaguardias excepcionales, que, en todo caso, cubrirían la principal preocupación común de los Estados; esto es, el acceso indiscriminado y/o injustificado a los datos por las autoridades públicas extranjeras.

Tras *Schrems I* se señaló que, aunque en 2013 el Supervisor europeo de Protección de Datos escribiera que la normativa europea sobre la transferencia internacional de datos se basa "en un grado razonable de pragmatismo con el fin de permitir la interacción con otras partes del mundo", esta regulación no busca un equilibrio razonable entre los estándares propios y los de terceros países sino la afirmación unilateral de los valores de la UE, siendo poco realista esperar soluciones internacionales sin que los Estados estén dispuestos a hacer concesiones[148]. En este sentido, más allá del compromiso de todos los miembros de la OMC con la liberalización del comercio internacional, la expansión tecnológica y de las comunicaciones globales resulta imparable en el día a día de la economía digital. Si no se encuentran soluciones pragmáticas que protejan la privacidad de los consumidores y sus datos, la fuerza de los hechos termina imponiendo esta expansión, debilitando la protección real de los derechos de los particulares. La búsqueda de mecanismos que, sin renunciar a esa protección, no bloquee el desarrollo del comercio digital debe continuar.

[148] KUNER, C. "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal*, vol. 18, núm. 4 2017, p. 917.