esade

EsadeEcPol - Center
for Economic Policy

Open Internet Governance Institute
PAPER SERIES # 2

La soberanía trasatlántica de los datos: cómo conseguir unos flujos de datos entre la UE y EE. UU. que garanticen la protección de la privacidad

Matthias Bauer
Senior Economist en el ECIPE

MARZO 2022

Sobre el autor

Matthias Bauer (PhD)
es Senior Economist en el European Centre
for International Political Economy (ECIPE).

Resumen ejecutivo

→ **El estado del problema.** El Tribunal de Justicia de la Unión Europea (TJUE) dictaminó en julio de 2020 que en EE. UU. no existe un nivel de protección suficiente para los datos personales de los ciudadanos de la UE, anulando así el acuerdo del Escudo de Privacidad entre EE. UU. y la UE de 2016 en el que basaban las transferencias trasatlánticas de datos. Recientemente, la Comisión Europea y el Gobierno de Estados Unidos anunciaron conjuntamente un "acuerdo de principio" para elaborar un nuevo marco para las bajas de datos. Sin embargo, su contenido, sus especificidades y, sobre todo, su plasmación en cambios mejorados serán claves para garantizar que sea más sostenible que su predecesor.

→ **Lo que hay en juego.** Esa resolución, sumada a la respuesta vaga e incierta que las autoridades de protección de datos le dieron y a su errática aplicación por parte de las entidades nacionales, generó una considerable incertidumbre a las empresas (pequeñas y grandes), las organizaciones y los ciudadanos sobre un aspecto central de la gobernanza económica global: durante los últimos 15 años, los datos han permitido que el comercio de servicios digitales entre EE. UU. y Europa se haya duplicado; y ha sido así tanto en los sectores digitales como en los menos digitales, por ejemplo, la manufactura tradicional, que depende fundamentalmente de los datos que circulan entre la UE y EE. UU.

→ **El obstáculo clave.** El TJUE considera que las autoridades estadounidenses que recopilan datos no cuentan, en virtud de las actuales leyes de vigilancia, con opciones reales de reparación para los ciudadanos de la UE, lo que permite a los organismos gubernamentales recopilar información de usuarios extranjeros que se encuentran fuera de su territorio nacional sin que estos tengan los mismos medios que los ciudadanos estadounidenses para defender su privacidad a través de un proceso judicial. La priorización de la seguridad nacional sobre la privacidad (de los ciudadanos extranjeros) se deriva del diferente planteamiento de la privacidad en los dos sistemas legales: en la UE, la protección de los datos personales se considera un derecho fundamental; en consecuencia, el Reglamento General de Protección de Datos europeo (RGPD) impone normas obligatorias acerca de la manera en que las organizaciones y las empresas deben utilizar los datos personales y otorga a las autoridades la capacidad de actuar *ex officio* cuando se infringe esta protección básica de la privacidad. Por el contrario, EE. UU. no cuenta con un equivalente federal al RGPD (ni planes inmediatos o intentos creíbles de crear uno) y se basa en regulaciones estatales de diferente alcance, contenido y cuestiones procesales, que suelen atribuir la responsabilidad de corregir las externalidades negativas a los actores privados y a sus actuaciones específicas.

→ **Un posible camino a seguir.** El objetivo final que deberían fijarse la UE y EE. UU. es «la soberanía trasatlántica de los datos», es decir, las transferencias de datos personales de individuos que respeten la privacidad y se basen en los objetivos y principios comunes y compartidos de los estándares, basados en el valor, utilizados para el comercio internacional y la tecnología en las democracias de mercado orientadas a los derechos y basadas en el Estado de derecho. A pesar de estos puntos en común, convendría adoptar un enfoque pragmático

que reconozca el ámbito limitado del acuerdo y se centre, por lo tanto, en la adecuación, la equivalencia o el reconocimiento mutuo. Para eso, el mínimo de partida deberían ser unas condiciones idénticas para la UE y EE. UU. que reconozcan las opciones de reparación y el control de las capacidades de vigilancia. El gobierno de EE.UU. ha señalado recientemente su voluntad de aplicar un nuevo marco que presenta ambas novedades.

→ **Dentro de EE. UU.,** el principal problema es la articulación del proceso político. Sugerimos tres posibles caminos:

1. El más expeditivo y eficiente sería una orden ejecutiva que limitase las recopilaciones a bulto de datos por parte de las agencias de vigilancia estadounidenses y que proporcionara mecanismos de reparación adicionales para los ciudadanos europeos, por ejemplo una oficina ejecutiva o un tribunal con poder para decidir sobre las reclamaciones y dictar resoluciones vinculantes sobre los servicios de inteligencia estadounidenses. Este parece ser el enfoque preferido por el actual gobierno estadounidense, que se ha comprometido a incluir sus próximos compromisos en una nueva OE. El problema fundamental de esta alternativa es su sostenibilidad a largo plazo, una vez finalice la Administración actual.

2. El más sostenible a largo plazo debería seguir el proceso legislativo convencional: el Congreso de EE. UU. podría modificar la Ley de Vigilancia de la Inteligencia Extranjera (FISA, por sus siglas en inglés) para prohibir la recopilación a bulto de datos de inteligencia y exigir una autorización judicial para cada objeto de vigilancia. Sin embargo, esta ruta podría resultar demasiado lenta para un asunto que es urgente, y además estar sujeta a incertidumbres políticas: la situación política en EE. UU. es compleja, y está caracterizada por un Senado dividido, un marcado partidismo y las próximas elecciones de mitad de mandato.

3. También está sobre la mesa una solución no legal, por ejemplo la modificación del papel de *ombudsperson*, o defensor/a del pueblo, para darle el poder de actuar *ex officio* en nombre de la protección de la privacidad. El problema de esta alternativa, que sería rápida y tal vez políticamente más viable, es la dificultad de evaluar si una opción no legal cumpliría los considerables requisitos europeos en materia de reparación, y si daría lugar a normas estables y fiables.

→ **Dentro de la UE,** los Estados miembros no están sujetos a los mismo estándares que las entidades extranjeras. De hecho, determinados Estados miembros (por ejemplo, Francia) expresaron en el pasado su disposición a excluir por completo a sus agencias de inteligencia del ámbito de la legislación de la UE. Pero, para que un acuerdo sea sostenible, cualquier concesión que haga EE. UU. relacionada con la posibilidad de reparación debería reflejarse en el tratamiento de los datos personales de los ciudadanos estadounidenses por parte de los Estados miembros de la UE. Esto abre la posibilidad de que otros Estados miembros de la UE defiendan un enfoque de la UE que refleje las concesiones estadounidenses en materia de derechos fundamentales de reparación en el contexto de las actividades de vigilancia gubernamentales, subrayando su compromiso con los derechos fundamentales de la UE, la apertura económica y una cooperación transatlántica significativa para resolver el dilema entre privacidad y seguridad.

La soberanía trasatlántica de los datos: cómo conseguir unos flujos de datos entre la UE y EE. UU. que garanticen la protección de la privacidad

Los datos personales de los ciudadanos europeos no se pueden transferir y almacenar sin más en Estados Unidos (EE. UU.), ni se puede acceder a ellos desde allí. Esta es, en términos generales, la consecuencia de un dictamen del Tribunal de Justicia de la Unión Europea (TJUE) de julio de 2020, la llamada sentencia Schrems II. El fallo concluyó que en EE. UU. no existe un nivel de protección para los datos personales de los ciudadanos de la UE (Unión Europea) que sea esencialmente equivalente a la protección que otorga el Reglamento General de Protección de Datos (RGPD) de la UE, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.[1] El TJUE sostiene que las autoridades de vigilancia del Gobierno de EE. UU. no están restringidas, tal como requiere la legislación de la UE, y objeta que los ciudadanos de la UE no cuentan con una manera efectiva de solicitar una reparación. La consecuencia inmediata de esta sentencia, y de su implementación por parte de las autoridades europeas de protección de datos, fue que miles de empresas de la UE y EE. UU., incluidas las pymes, no pudieron seguir basándose en el acuerdo del Escudo de Privacidad entre EE. UU y la UE de 2016 para transferir datos personales a través del Atlántico.

La sentencia Schrems II tiene también una dimensión multilateral. En la actualidad, además de EE. UU., la mayoría de los países que no pertenecen a la UE no cuentan con un nivel equivalente de protección de datos. En consecuencia, los flujos de datos desde la UE hacia esos países, entre ellos países autoritarios como China y Rusia, puede ser considerado ilegal por las autoridades de la UE.[2] Es más, el TJUE indica a las organizaciones (públicas y privadas) que, cuando envíen datos personales bajo cláusulas contractuales tipo (CCT), deben evaluar las protecciones reales "en lo referente a cualquier acceso por parte de las autoridades públicas de ese tercer país a los datos personales transferidos" y "los aspectos pertinentes del sistema jurídico de ese tercer país". A menos que estas protecciones sean "esencialmente equivalentes" a las medidas de la UE, se supone que las empresas deben dejar de hacer transferencias de datos personales.

1 Véase el caso C-311/18, conocido como la resolución "Schrems II".

2 Véase Comisión Europea (2022), "Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection". Disponible en: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Hasta enero de 2022, la Comisión Europea había declarado adecuados a Andorra, Argentina, Canadá (organizaciones comerciales), islas Feroe, Guernsey, Israel, isla de Man, Japón, Jersey, Nueva Zelanda, República de Corea, Suiza y Reino Unido según el RGPD y la Directiva de Aplicación de la Ley (LED, por sus siglas en inglés), y reconocido que Uruguay proporcionaba una protección adecuada.

Con la anulación del acuerdo del Escudo de Privacidad de 2016 a raíz de la resolución Schrems II, una vez más la regulación de los flujos transfronterizos de datos se convirtió en la prioridad del diálogo transatlántico.[3] Aunque al principio muchos observadores creyeron que la UE y EE. UU. pronto se pondrían de acuerdo en un nuevo mecanismo de transferencia de datos personales, y a pesar de las prometedoras declaraciones públicas hechas por la Comisión y EE. UU. a partir de noviembre, que culminó con el anuncio en marzo de 2022 de un "acuerdo de principio" para elaborar un nuevo marco, todavía no hay un texto legal final. Se mantiene una **considerable incertidumbre** sobre si se acordará un nuevo marco, y sobre cuándo se hará. En la actualidad, las **orientaciones** del Comité Europeo de Protección de Datos (CEPD) y de las autoridades nacionales de protección de datos **siguen siendo bastante vagas y generan inseguridad jurídica,** que resulta especialmente gravosa para las pequeñas empresas. Al mismo tiempo, las **erráticas decisiones sobre su aplicación adoptadas por las autoridades nacionales de protección de datos requieren de una actuación oportuna para establecer un mecanismo legal fiable para la transferencia de datos personales** fuera de la UE que proteja la privacidad.[4]

Ya han pasado 20 meses desde la anulación del Escudo de Privacidad. Algunas opiniones públicas sugieren que los representantes de la UE y EE. UU. siguen teniendo diferentes puntos de vista acerca de aspectos clave de la privacidad y la protección de los datos personales, que van desde consideraciones sobre la seguridad nacional a los procedimientos de aplicación. Los siguientes apartados de este *policy brief* se centran en las relaciones políticas y económicas transatlánticas para abordar los **obstáculos decisivos** que impiden la búsqueda de un entorno más armonizado y menos incierto para unos flujos de datos que protejan la privacidad. A continuación, se esbozarán las **posibles medidas políticas** para garantizar la **"soberanía transatlántica de los datos",** definida como las **transferencias de datos personales de individuos entre la UE y EE.UU. en las que se garantiza la protección de la privacidad,** y cómo las políticas complementarias podrían ser aceptadas en otras partes del mundo.

Margen político e impedimentos para la cooperación transatlántica relacionada con la privacidad de los datos

La libre circulación de los datos es muy importante para las relaciones económicas transatlánticas. Si las trasferencias de datos entre la UE y EE. UU. se detuvieran, el comercio y la actividad económica interior, tanto de la UE como de EE. UU., experimentarían pérdidas significativas. Una evaluación de impacto reciente ha hallado que tanto **los sectores digitales como los que son menos digitales,** por ejemplo la manufactura tradicional, **dependen crucialmente de los datos que fluyen entre la UE y EE. UU.,** entre ellos varios tipos y combinaciones de datos personales y no personales.[5] Además, durante los últimos 15 años los datos han

3 El 6 de octubre de 2015, el TJUE dictó una sentencia que declaraba nula la resolución de la Comisión Europea del 26 de julio de 2000 sobre la adecuación jurídica del acuerdo de Puerto Seguro entre la UE y EE. UU. El 12 de julio de 2016, la Comisión Europea emitió un dictamen sobre la adecuación del marco del Escudo de Privacidad entre la UE y EE. UU. Este nuevo marco, que sustituía al programa Puerto Seguro, proporcionaba un mecanismo legal para que las empresas transfirieran datos personales de la UE a los Estados Unidos.

4 Véase, por ejemplo, Noyb (2022), "Austrian DSB: EU-US data transfers to Google Analytics illegal", 13 de enero de 2022. Véase también, Politico (2022), "French privacy regulator rules against use of Google Analytics", 10 de febrero de 2022.

5 Véase ECIPE-Kearney (2021), The economic costs of restricting the cross-border flow of data. Disponible en: <https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625067571000>.

permitido duplicar el comercio de servicios digitales entre EE.UU. y Europa. La libre circulación de datos permite a los consumidores y las empresas de la UE y de EE.UU. aprovecharse de servicios actualizados, como las aplicaciones de comercio electrónico, los servicios en la nube, los servicios sanitarios y un amplio espectro de servicios digitales utilizados para apoyar las operaciones empresariales en todos los sectores.

Así pues, los datos se consideran a menudo la savia del comercio y la inversión, porque apoyan los procesos de producción internacionales y las actividades de investigación y desarrollo. Como tal, su libre circulación contribuye a la resiliencia económica y la "soberanía digital" en todos los sectores, sobre todo en los que hacen un uso intensivo de los datos, como los servicios de información, de telecomunicaciones, financieros y profesionales.[6]

Tanto la UE como EE. UU. se benefician mucho de un mayor acceso a los bienes y servicios y de los puestos de trabajo creados por las inversiones y el comercio digital trasatlánticos. Las estadísticas sobre comercio e inversión revelan que muchos países de la UE están muy expuestos al comercio trasatlántico, lo cual requiere de la libre transferencia de datos personales y de otro tipo. Por ejemplo, se estima que en 2019 los empleos que dependían directamente de filiales de propiedad mayoritariamente estadounidense ascendían en Alemania a los 666.000, en Francia a los 506.000 y en España a los 179.000. Asimismo, los puestos trabajo en EE. UU. creados directamente por empresas de propiedad mayoritariamente de la UE ascendían a 882.000 para Alemania, 799.000 para Francia y 93.000 para España. El comercio transatlántico de servicios, que con frecuencia depende de los datos personales, está bastante equilibrado y ya supone una parte importante del total de las exportaciones de los países de la UE y de sus importaciones de EE. UU.[7] En 2019, las exportaciones de servicios estadounidenses a Alemania ascendieron a 36.600 millones de dólares, mientras que las exportaciones de servicios alemanas a EE. UU. fueron de 34.900 millones de dólares. Las exportaciones de servicios estadounidenses a Francia ascendieron a 22.400 millones de dólares, mientras que las exportaciones de servicios franceses a EE. UU. fueron de 20.400 millones de dólares. Asimismo, las exportaciones de servicios estadounidenses a España ascendieron a 8.700 millones de dólares, mientras que las exportaciones españolas de servicios a EE.UU. fueron de 7.800 millones de dólares.[8]

6 Las nociones de soberanía (o autonomía) digital, tecnológica o industrial siguen siendo ambiguas. Véase un análisis crítico de la concepción de las políticas de la UE sobre el tema en Bauer y Erixon (2021), "Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls", ECIPE Occasional Paper 02/2020.

7 Por ejemplo, en 2019 España exportó servicios por valor de 138.000 millones de dólares. Los principales servicios exportados fueron viajes privados (74.900 millones de dólares), servicios empresariales, profesionales y técnicos (24.800 millones de dólares), transporte (18.700 millones de dólares), viajes de negocios (4.800 millones de dólares) y servicios financieros (3.850 millones de dólares). Véase el Observatorio de la Complejidad Económica (OEC, por sus siglas en inglés). Para una visión general de los modos digitales de suministro/prestación de servicios, véase OCDE (2020), *Handbook on measuring Digital Trade,* publicado conjuntamente por la OCDE, la OMC y el FMI.

8 Para una visión general de las relaciones comerciales y de inversión en la economía transatlántica, véase AmCham (2021), *The Transatlantic Economy in 2021. Annual Survey of Jobs, Trade and Investment between the United States and Europe.*

Tabla 1. Estimación de la magnitud de las inversiones vinculadas a EE. UU. en los principales países europeos

	España	Francia	Alemania
Puestos de trabajo dentro del país en empresas de propiedad estadounidense	179.000	506.000	666.000
Exportaciones de servicios a EE. UU.	$7.800m	$20.400m	$36.600m
Importaciones de servicios de EE. UU.	$8.700m	$22.400m	$34.900m

En general, los Gobiernos son conscientes de la importancia económica que tienen los datos para el comercio y la inversión. Por lo tanto, **la regulación de los flujos de datos y los requisitos para su almacenamiento se han convertido en un aspecto fundamental de la gobernanza económica digital en todo el planeta.**[9] Ocurre igual en la UE y en EE. UU. Desde un punto de vista **económico, a ambas jurisdicciones les convendría establecer un marco regulatorio fiable y que sea válido en el futuro para el intercambio de datos personales e información no personal de un lado a otro del Atlántico.** Pero hay más elementos de los que partir. Si bien existen diferencias en la manera en que la UE y EE. UU. abordan la privacidad y la protección de los datos personales de los ciudadanos, hay importantes puntos en común que pueden tenerse en cuenta en las negociaciones bilaterales y, potencialmente, en los foros multilaterales: en primer lugar, tanto la UE como EE. UU. cuentan con una larga tradición de **respeto a los derechos humanos y al Estado de derecho** y exigen seguridad jurídica para los particulares y las empresas. En segundo lugar, tanto la UE como EE. UU. consideran que la protección de los datos, incluidos los datos electrónicos, es un elemento importante de la **protección del consumidor.** Y en tercer lugar, ambas jurisdicciones comparten **preocupaciones parecidas sobre los derechos humanos (o de los ciudadanos)**, por ejemplo, las relacionadafs con los requisitos ilimitados o desproporcionados que establecen los gobiernos e imponen el acceso a los datos personales en posesión del sector privado.[10] Por último, siguiendo la agenda de la iniciativa transatlántica del Consejo de Comercio y Tecnología (TTC, por sus siglas en inglés), tanto la UE como EE. UU. aspiran a desarrollar conjuntamente unos estándares para el comercio y la tecnología que se "basen en valores" y que deberían aplicarse en países similares a escala global.[11]

La importancia económica de la libre circulación de datos, incluido el flujo seguro de datos personales, junto con una noción compartida de los derechos humanos y el principio del Estado de derecho, **deberían**

9 Véase, por ejemplo, D. Svantesson, (22 de diciembre de 2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", OECD Digital Economy Papers, n.º 301, OECD Publishing, París.

10 Véase, por ejemplo, OCDE (2021), que recoge el trabajo del Comité de Políticas Económicas Digitales de la OCDE, al que pertenecen EE. UU. y los países de la UE. Cabe señalar que los miembros de la OCDE tienen una larga tradición de respeto por los derechos humanos y el Estado de derecho, y además comparten un sólido compromiso con la protección del derecho fundamental a la privacidad cuando los organismos gubernamentales tienen acceso a los datos personales.

11 Véase Comisión Europea (2021), "EU-US launch Trade and Technology Council to lead values-based global digital transformation", comunicado de prensa, 15 de junio de 2021.

proporcionar suficiente margen político para una cooperación significativa que conduzca a enfoques armonizados o, al menos, a **decisiones de equivalencia** (reconocimiento mutuo) en ambos lados. Sin embargo, el diablo está en los detalles. Hoy en día los enfoques legales de la UE y EE. UU. sobre la privacidad de los datos difieren entre sí. Además, la interpretación actual de EE. UU. del alcance de las obligaciones respecto a los derechos humanos difiere de la de la UE, lo que en la práctica limita el margen político para llevar a cabo políticas cuyo resultado sea significativo. A continuación se describen brevemente los enfoques de la UE y EE. UU. acerca de las regulaciones sobre la privacidad de los datos.

La regulación de la privacidad de los datos en la UE

En 2016, la UE adoptó el RGPD, que sustituía a la Directiva de Protección de Datos de 1995, cuyo objetivo era lograr un equilibrio entre la protección de los datos de los individuos y la libre circulación de los datos personales dentro de la UE. La ley estatutaria de la UE sobre la privacidad —el RGPD— es una consecuencia del derecho primario de la UE. **En la UE, la protección de los datos personales se considera un derecho fundamental.** En los Estados miembros, rigen las constituciones nacionales y la Carta de los Derechos Fundamentales de la UE. Los artículos 7 y 8 de la Carta estipulan que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan" y que esos datos "se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley".[12] El artículo 52 permite la limitación de esos derechos solo si se hace "respetando el principio de proporcionalidad" y "cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás". Además, el artículo 47 de Carta concede a cualquier individuo cuyos derechos hayan sido violados "que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley".

El RGPD de la UE impone normas obligatorias para el uso debido de los datos personales en las organizaciones y las empresas.[13] En términos generales, el RGPD tiene por objeto la protección de los datos personales de los ciudadanos de la UE, y reducir la gravedad y la frecuencia de las violaciones de la seguridad de los datos y la posibilidad de que los datos personales en la web se usen o traten incorrectamente. En consecuencia, el RGPD establece varias obligaciones para los responsables y los encargados del tratamiento de los datos y dispone los derechos de los ciudadanos, como el consentimiento para permitir el tratamiento de los datos con un propósito concreto, los derechos relacionados con la transparencia y el derecho al olvido. El RGPD se aplica a los responsables y los encargados del tratamiento de datos que están establecidos en la UE, proporcionan bienes o servicios a personas en la UE o supervisan el comportamiento de individuos dentro de la UE.[14]

12 Véanse el artículo 7 y 8 de la Carta de los Derechos Fundamentales de la UE, 2012/C 326/02.

13 Se consideran datos personales cualquier información que, directa o indirectamente, pueda identificar a una persona viva. Nombre, número de teléfono y dirección del domicilio son ejemplos evidentes de datos personales. Pero los intereses, la información sobre compras realizadas, la salud y el comportamiento online también se consideran datos personales si pueden identificar a una persona.

14 En el RGPD se considera que el responsable es una persona o entidad que determina "los fines y medios" del tratamiento de los datos personales y que un encargado es una persona o entidad que trata los datos en nombre del responsable del tratamiento.

El **RGPD** ya está reconocido como ley en toda la UE. Se trata de un reglamento de la UE que (a diferencia de una directiva de la UE) fue concebido para aplicarse directamente y dar lugar a una armonización entre todos los Estados miembros. Sin embargo, a pesar de ser un reglamento, el RGPD no establece normas sobre la privacidad totalmente idénticas para todos los Estados miembros. Sí aumenta significativamente la coordinación, pero algunos aspectos quedan fuera de su ámbito porque no están dentro de la competencia legislativa de la UE, por ejemplo, la seguridad nacional. Además, algunas normas permiten la discrecionalidad política a escala nacional, por ejemplo, algunas normas específicas para el tratamiento de los datos personales sensibles (datos genéticos, datos sanitarios, datos relacionados con el empleo, datos penales, etc.), normas específicas para el tratamiento de los datos y la imposición de criterios adicionales que deben cumplirse para tratar datos personales con nuevos fines. Asimismo, los Estados miembros de la UE siguen diferentes planteamientos por lo que respecta a las condiciones que permiten el tratamiento de los datos personales relacionados con los antecedentes penales.[15]

El **RGPD,** que se interpreta teniendo en cuenta la Carta de los Derechos Fundamentales de la UE, también regula **las condiciones en las que los exportadores de datos pueden transferir datos personales desde la UE a países extranjeros** (Capítulo V, artículos 44-50). [16] En general, los responsables y los encargados del tratamiento de los datos pueden transferir datos personales a países extranjeros, si la Comisión Europea ha considerado que el país garantiza un **nivel apropiado de protección.** Además, los exportadores de datos pueden servirse de ciertas **garantías adecuadas**: pueden adoptar normas corporativas vinculantes (NCV) que cumplan los requisitos del RGPD o pueden utilizar cláusulas contractuales tipo (CCT), que son términos contractuales específicos aprobados por la Comisión Europea.[17]

15 Véase, por ejemplo, White & Case (2019), "GDPR Guide to National Implementation – A practical guide to national GDPR compliance requirements across the EEA", 13 de noviembre de 2019.

16 Véase el Capítulo V del RGPD.

17 El 4 de junio de 2021, la Comisión Europea dictó unas CCT actualizadas para las transferencias de datos realizadas por responsables y encargados del tratamiento de datos en la EU y el EEE a responsables y encargados del tratamiento de datos establecidos fuera de la EU y el EEE (y no sujetos al RGPD). Cabe señalar que según el artículo 49 del RGPD, el exportador también debe contemplar las "excepciones para situaciones específicas", por ejemplo, que el interesado haya dado explícitamente su consentimiento a la transferencia o en el caso de que la transferencia sea "necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el [interesado y el] responsable del tratamiento".

La perspectiva estadounidense sobre la privacidad y la regulación de los datos

En EE. UU. no existe una ley federal sobre la privacidad de los datos semejante al **RGPD**. Sin embargo, se han implementado algunas leyes nacionales para regular el uso de los datos en sectores específicos de la economía. Entre ellas están:

- **1974:** La Ley de Privacidad de Estados Unidos, que define los derechos y las restricciones relativos a los datos en posesión de las agencias gubernamentales estadounidenses.[18]

- **1996:** La Ley de Responsabilidad y Movilidad del Seguro de Salud (HIPAA, por sus siglas en inglés), que regula la privacidad y la seguridad en el sector sanitario.[19]

- **1999:** La Ley Gramm-Leach-Billey (GLBA, por sus siglas en inglés), que determina la manera en que se obtiene y utiliza la información sobre la privacidad no pública de los consumidores en el sector financiero.[20]

- **2000:** La Ley de Protección de la Privacidad Infantil en Internet (COPPA, por sus siglas en ingles), que supuso un primer paso en la regulación de la información personal obtenida de menores. La ley prohibe a las empresas de internet pedir información de identificación personal a niños menores de doce años, a menos que exista un permiso parental verificable.[21]

Más allá de estas legislaciones, el **Gobierno federal de EE. UU. no ha intentado en serio actualizar las leyes de privacidad mediante la introducción de nuevas aplicaciones para internet, el comercio electrónico y las grandes plataformas *online*.** Algunas regulaciones propuestas, por ejemplo la "Ley Estadounidense de Difusión de Datos", la "Ley de Protección de Datos de los Consumidores" y la "Ley de Diligencia de los Datos" no obtuvieron el apoyo suficiente en el Congreso. Por lo tanto, EE. UU. no dispone aún de reglamentos federales que cubran la privacidad del consumidor y la seguridad de los datos en todos los sectores.[22]

Si bien el Gobierno federal estadounidense no ha desarrollado una versión del RGPD de la UE, **varios estados federales, como California y Washington, han aprobado leyes parecidas de protección de datos.** Esas leyes se parecen al RGPD, pero no son una réplica exacta.[23] **Difieren en alcance, contenido y cuestiones procesales.** Mientras el RGPD de la UE protege a las personas físicas de cualquier nacionalidad y establece requisitos para las empresas, las organizaciones gubernamentales y las que no tienen ánimo de

18 "Ley de Privacidad", 5 U.S.C. § 552a (1974), <https://www.justice.gov/opcl/privacy-act-1974>.

19 "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", CDC, 21 de febrero de 2019, <https://www.cdc.gov/phlp/publications/topic/hipaa.html>.

20 "Gramm-Leach-Billey Act", Comisión Federal de Comercio, consultado el 8 de febrero de 2022, <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>

21 "Children's Online Privacy Protection Rule 'COPPA'", Comisión Federal de Comercio, 25 de julio de 2013, <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

22 "2021 Consumer Data Privacy Legislation", NCSL, consultado el 8 de febrero de 2022, <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx>.

23 Fefer, R. F. y Archick, K., (2022), "EU Data Protection Rules and U.S. Implications".

lucro, la CCPA de California se limita a los residentes en California y a las grandes empresas que operan en su estado. De un modo similar, la Ley de Privacidad de Washington solo incluye a las grandes empresas que llevan a cabo su actividad en el estado de Washington. El RGPD y las leyes federales estadounidenses también se diferencian en las obligaciones impuestas a los recopiladores de datos, como evaluaciones de riesgo, requisitos sobre la minimización de datos y la limitación de los fines. A las empresas les resulta costoso cumplir los distintos requisitos que existen dentro de EE. UU. Además, como no hay un organismo regulador federal que proteja los datos y los derechos de privacidad de los consumidores, los estados federales estadounidenses que aprueban normativas tienen que imponerlas por sí solos. Lo cual hace que el cumplimiento sea confuso e incoherente. Por lo que respecta a su aplicación, el **sistema europeo** se basa en gran medida en organismos especializados de protección de datos que actúan como **protectores *ex officio* de los derechos individuales**, mientras que en **EE. UU.** parece que **las autoridades federales prefieren una estrategia menos intervencionista que aspira a equilibrar los intereses de las empresas y los consumidores.** Las autoridades estadounidenses suelen **atribuir la responsabilidad de corregir las externalidades negativas a los actores privados y sus actuaciones específicas,** normalmente a través del sistema judicial, pero también mediante la Comisión Federal de Comercio en tanto que organismo ejecutivo.

En EE. UU., los estándares de protección de datos más importantes para internet proceden de leyes estatutarias. No se derivan de un compromiso con los derechos humanos. En 1992, EE. UU. ratificó el Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), un tratado de derechos humanos que garantiza los derechos relacionados con la privacidad. El artículo 17 protege a los individuos de injerencias arbitrarias o ilegales "en su vida privada, su familia, su domicilio o su correspondencia".[24] Sin embargo, desde entonces no se ha producido un debate significativo acerca de las leyes de privacidad y su relación con la "privacidad digital" en tanto que derecho fundamental. A diferencia de las europeas, las autoridades estadounidenses (y el sistema legal estadounidense) por el momento no aceptan el principio de "universalidad de los derechos humanos". En la práctica, esto significa que **según EE. UU. el ICCPR es aplicable "solo a individuos que se hallen dentro del territorio de un Estado miembro y estén sujetos a su jurisdicción".**[25] En otras palabras, EE. UU. considera que el ICCPR no se aplica extraterritorialmente. Se trata de un gran impedimento para lograr un acuerdo transatlántico sobre los flujos transfronterizos de datos personales.

En la sentencia Schrems II, el TJUE anuló la resolución de 2016 de la Comisión Europea sobre el Escudo de Privacidad. Por aquel entonces, la Comisión había llegado a la conclusión de que las transferencias de datos personales a EE. UU. de acuerdo con el marco del Escudo de Privacidad acordado proporcionaban un nivel de protección adecuado a los interesados en la UE.[26] Según este acuerdo, los organismos estadounidenses tenían que certificar ellos mismos ante el Departamento de Comercio de EE. UU. que cumplirían unos

24 "Human Rights and Privacy", American Civil Liberties Union, consultado el 8 de febrero de 2022, <http://www.aclu.org/issues/human-rights/human-rights-and-privacy>.

25 Véase Parlamento Europeo (2021), "Exchanges of Personal Data After the Schrems II Judgement", estudio requerido por el comité LIBE, julio de 2021. Véase también, por ejemplo, la declaración de Matthew Waxman, subdirector principal de Planificación de Políticas del Departamento de Estado ante el Comité de Derechos Humanos de la ONU el 17 de julio de 2006.

26 Véase la Decisión de Ejecución (UE) 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 Privacidad UE-EE. UU. (notificada con el número C[2016] 4176).

requisitos similares al RGPD, por ejemplo, requisitos sobre notificaciones, límites de retención de datos, requisitos de seguridad y la limitación de la finalidad del tratamiento de los datos. En 2016, la Comisión también consideró que el acceso del Gobierno estadounidense a los datos personales de los ciudadanos europeos estaba realmente restringido, lo que aseguraba la protección legal efectiva frente a las injerencias de las agencias de inteligencia estadounidenses. La Comisión Europea reconoció que los derechos de reparación de los ciudadanos no estadounidenses estaban limitados, pero al mismo tiempo manifestó que el nuevo mecanismo del ombudsperson garantizaba un nivel de protección suficiente.[27]

Con la sentencia Schrems II, **el TJUE anuló el dictamen y la resolución de la Comisión Europea. Consideró que las autoridades estadounidenses que recopilaban datos en virtud de las leyes de vigilancia existentes carecían de opciones efectivas de reparación para los ciudadanos de la UE.** La sección 702 de la Ley de Vigilancia de la Inteligencia Extranjera (**FISA,** por sus siglas en inglés) **permite a las agencias del Gobierno estadounidense recopilar información de usuarios extranjeros que se encuentran fuera de su territorio nacional, pero sin que estos tengan los mismos medios que los ciudadanos estadounidenses para defender su privacidad a través de un proceso judicial.** Es principalmente esta priorización de la seguridad nacional sobre la privacidad y la protección de los datos personales lo que llevó al TJUE a anular el Escudo de Privacidad.

Opciones políticas

Aunque existen diferencias en el modo en que la UE y EE. UU. abordan la privacidad y la protección de los datos personales de los ciudadanos, hay importantes puntos en común en los que pueden basarse las negociaciones transatlánticas y los foros multilaterales:

1. **tanto la UE como EE.UU. tienen una larga tradición de respeto por los derechos humanos y el Estado de derecho,**

2. **la UE y EE.UU. consideran que la protección de los datos, incluidos los datos electrónicos, es un elemento importante de la protección del consumidor,**

3. **ambas jurisdicciones comparten preocupaciones similares sobre el acceso ilimitado, irrazonable o desproporcionado de los gobiernos a los datos personales en posesión de individuos y organizaciones privadas,**

4. **varios estados federales de Estados Unidos han implementado o están considerando aprobar una legislación parecida al RGPD de la UE, aunque no sea una replica exacta y**

5. **ambas jurisdicciones, en el marco del TTC, renovaron su compromiso de trabajar juntas en unos estándares basados en valores para el comercio internacional y la tecnología que propicien el comercio transfronterizo.**

27 Véase "Privacy Shield agreement ANNEX A: EU-U.S. Privacy Shield Ombudsperson Mechanism".

A pesar de estos puntos en común, **el alcance de una armonización completa de las leyes de privacidad sigue siendo bastante limitado**. Como se ha descrito antes, el RGPD no armoniza plenamente las leyes de protección de datos de los Estados miembros de la UE. Además, una diferencia clave entre las visiones de la privacidad en EE.UU. y la UE es aquello en lo que hacen hincapié. En el pasado, parecía que a las autoridades estadounidenses lo que más les preocupada era la integridad de los datos como activo comercial, mientras que el RGPD antepone firmemente los derechos individuales a los intereses empresariales. Además, la UE y EE.UU. tienen **distintas estrategias para implementar la nueva legislación,** lo cual afecta a qué ley puede ser aprobada. Con el RGPD, la UE se basaba más en un enfoque de arriba abajo que equilibraba las políticas de un Estado miembro con las supranacionales. En cambio, el enfoque de EE.UU. es de abajo arriba y refleja los derechos de los estados federales en la gobernación y puede hacer que iniciativas como los derechos de privacidad sean una legislación difícil de aprobar. **La adecuación, la equivalencia o el reconocimiento mutuo son, por tanto, formas más prometedoras de llegar a una solución significativa y válida para el futuro,** que acabe con la incertidumbre jurídica de los flujos transatlánticos de datos. La adecuación, la equivalencia o el reconocimiento mutuo también superan el uso de las excepciones del artículo 49, que según algunos expertos podrían constituir una base jurídica fiable para las transferencias intraempresariales de datos personales, ya que estas excepciones pueden discriminar a organizaciones que no sean grandes empresas o grupos de empresas.[28]

Sin embargo, un **obstáculo clave** para la adecuación es la **postura actual de EE. UU. respecto a la aplicación de los derechos fundamentales a los ciudadanos no estadounidenses,** que afecta a la posibilidad de que los europeos puedan reclamar una reparación en los tribunales estadounidenses y a la forma de hacerlo. Es poco probable que la Comisión Europea y las autoridades europeas de protección de datos (que, sin embargo, no tienen poder para vetar un acuerdo político) acepten cualquier acuerdo que mantenga la situación actual en EE. UU. y no garantice principios fundamentales como la supervisión y la rendición de cuentas, la transparencia respecto a las solicitudes del Gobierno y unos derechos de reparación efectivos, aunque en la práctica pueda ser muy difícil que los ciudadanos detecten infracciones. Lo mismo ocurre con el TJUE, que es poco probable que dé el visto bueno a cualquier nuevo acuerdo que no cumpla estas excepciones.

No obstante, cabe apuntar que varios observadores señalaron una **cierta desconexión entre los estándares a los que el TJUE somete a los sistemas de vigilancia de EE.UU. y los estándares dentro de la propia UE.** Dentro de la UE, la seguridad es responsabilidad exclusiva de los Estados miembros. El Gobierno de cada Estado miembro es libre de aplicar sus propias políticas de seguridad nacional y equilibrarlas con las obligaciones de privacidad de la UE. "De hecho, el RGPD utiliza como una herramienta la amenaza de retirar el acceso a los datos personales de la UE, con el fin de procurar una reforma de las agencias de seguridad de otros países para que reflejen la noción de proporcionalidad del TJUE, mientras que exime a los Gobiernos de los Estados miembros de expectativas o amenazas similares".[29] Sin embargo, los gobiernos de la UE siguen estando obligados por el Convenio Europeo de Derechos Humanos (CEDH).

---

28 Véase Parlamento Europeo (2021), "Exchanges of Personal Data After the Schrems II Judgement. Study requested by the LIBE committee", julio de 2021. Véase también, por ejemplo, la declaración de Matthew Waxman, subdirector principal de Planificación de Políticas del Departamento de Estado ante el Comité de Derechos Humanos de la ONU el 17 de julio de 2006.

29 Meltzer, J. P. (2020), "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security", 5 de agosto de 2020. Véase también Baker, S. (2020), "Cross-border data, How Can the U.S. Respond to Schrems II?", 21 de julio de 2020.

En su dictamen sobre Schrems II, el abogado general argumentó que **incluso cuando la ley de la UE no se aplique a un Estado miembro, la evaluación de la adecuación de las leyes y las prácticas de vigilancia de un tercer país debería basarse en los estándares del CEDH** que, por lo demás, son vinculantes para los Estados miembros de la UE.[30]

Algunos Estados miembros de la UE, como Francia, expresaron en el pasado su disposición a excluir por completo a sus agencias de inteligencia del ámbito de aplicación de la legislación de la UE.[31] En consecuencia, **cualquier concesión que haga EE. UU. relacionada con la posibilidad de reparación como la sugerida por la Casa Blanca y la Comisión Europea en su comunicado conjunto del 25 de marzo debería reflejarse en el tratamiento de los datos personales de los ciudadanos estadounidenses,** cuyo fin sea de vigilancia y aplicación de la seguridad nacional, **por parte de los Estados miembros de la UE**. Teniendo en cuenta lo anterior, las negociaciones entre la UE y EE. UU. deberían basarse, en general, en el grupo de trabajo de la OCDE sobre el "acceso de los gobiernos a los datos personales en poder del sector privado", y en otras iniciativas como la coalición para la Reforma de la Vigilancia Gubernamental (RGS, por sus siglas en inglés),[32] y la Iniciativa de la Red Global (GNI, por sus siglas en inglés).[33] Algunos Estados miembros de la UE, como España, los países bálticos y los nórdicos, podrían defender un enfoque de la UE que refleje las concesiones de EE. UU. relativas a los derechos de reparación fundamentales en el contexto de las actividades de vigilancia gubernamentales, subrayando su compromiso con los derechos fundamentales de la UE, la apertura económica y una cooperación transatlántica significativa para resolver el dilema entre privacidad y seguridad.

Por lo que respecta a las concesiones de EE.UU., muchas autoridades estadounidenses comparten la preocupación por la situación actual. En diciembre de 2020, la Comisión de Comercio, Ciencia y Transporte del Senado celebró una audiencia sobre la anulación del "Escudo de Privacidad y el futuro de los flujos transatlánticos de datos". Se manifestó preocupación por la necesidad de reformar las actuales leyes de vigilancia estadounidense: "se está de acuerdo en que una ley de privacidad, por sí sola, no es suficiente; EE. UU. debería, más bien, examinar su estrategia de recopilación de inteligencia y plantearse la reforma de la vigilancia, posiblemente para incluir un consenso basado en la recopilación de inteligencia/vigilancia y la protección de los datos con otras grandes democracias".[34]

---

30 Véase "Opinion of Advocate General Saugmandsgaard, delivered on 19 December 2019. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, interveners: The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance, Inc., Digitaleurope".

31 Lawfare (2021), "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States", 8 de marzo de 2021.

32 La RGS pide a los gobiernos de todo el mundo que se adhieran a los siguientes principios cuando lleven a cabo una vigilancia. Los principios clave de la RGS se describen en: <https://www.reformgovernmentsurveillance.com/principles/>.

33 Los miembros de la GNI creen que la libertad de expresión y la privacidad son fundamentales para fomentar la estabilidad, la inclusión y la seguridad. En consecuencia, las actividades de vigilancia llevadas a cabo por un Gobierno deben cumplir los principios del Estado de derecho y la gobernanza democrática, así como con los principios de los derechos humanos, como la legalidad, la necesidad y la proporcionalidad. Véase: <https://globalnetworkinitiative.org/policy-issues/surveillance/>.

34 Véase *National Law Review* (2020), "Senate Commerce Committee Holds Hearing on the Invalidation of the EU-U.S. Privacy Shield and the Future of Transatlantic Data Flows", 21 de diciembre de 2021. Los testimonios pueden consultarse en: <https://www.commerce.senate.gov/2020/12/the-invalidation-of-the-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows>.

Muchos observadores sostienen que la promulgación de un nuevo estatuto jurídico estadounidense para garantizar la reparación tiene importantes ventajas, pero sigue habiendo grandes obstáculos políticos, entre ellos las barreras bipartidistas y constitucionales. Una solución no legal, que no se oponga a la legislación de la UE, podría ser una alternativa. Como han argumentado recientemente Christakis *et al.* (2021), la ley de la UE es "flexible a la hora de interpretar si EE. UU. debe adoptar una nueva ley para cumplir con los requisitos de reparación, sobre todo cuando la cuestión se contempla a través del prisma de la 'equivalencia esencial' de la protección de datos".[35] Esto podría requerir, por ejemplo, modificaciones en el papel del *ombudsperson,* como ha sugerido el Supervisor Europeo de Protección de Datos. El *ombudsperson* debería poder "actuar con independencia, no solo de los servicios de inteligencia, sino de cualquier otra autoridad. En términos prácticos, la posibilidad de responder directamente ante el Congreso podría ser una opción en este sentido".[36]

Los responsables políticos de EE. UU. no están legalmente obligados por las recomendaciones del TJUE, pero es difícil evaluar si una opción no legal cumpliría los considerables requisitos europeos acerca de la reparación y si daría lugar a unas normas estables y fiables. Sin embargo, para proporcionar un nivel de protección adecuado a las personas interesadas de la UE, en particular los derechos de reparación, las autoridades estadounidenses podrían considerar **dos opciones potencialmente más prometedoras (no excluyentes entre sí):**[37]

(1) Una actuación ejecutiva por parte de EE. UU.: Biden, el presidente estadounidense, podría promulgar una **orden ejecutiva** que **limite las recopilaciones a bulto de datos llevadas a cabo por las agencias de vigilancia de EE. UU. y que proporcione mecanismos adicionales de reparación para los ciudadanos europeos,** como una oficina ejecutiva o un tribunal con poder para resolver quejas y dictar decisiones vinculantes sobre los servicios de inteligencia estadounidenses. En este sentido, la declaración de la Casa Blanca tras el anuncio conjunto de la UE y los EE.UU., en la que se hace referencia a la posibilidad de que los individuos de la UE busquen compensación, parece ir en la dirección correcta. Además, la declaración también mencionaba la voluntad de emplear una OE como dispositivo de compromiso jurídicamente vinculante.

(2) Una nueva legislación estadounidense: **el Congreso de EE. UU. podría modificar la FISA para prohibir las recopilaciones de inteligencia a bulto y exigir una autorización judicial para cada objetivo de vigilancia.** Las recientes señales del gobierno estadounidense parecen mostrarlo dispuesto a restringir la recopilación de información "sólo cuando sea necesario para promover intereses nacionales legítimos", como declaró el 25 de marzo la Casa Blanca. La nueva legislación también podría establecer el derecho de los ciudadanos europeos (o, en general, de los ciudadanos no estadounidenses) a presentar reclamaciones ante un tribunal si creen que las agencias de inteligencia han recogido o usado sus datos de forma ilegal.

---

35 Véase Christakis, T., Propp, K. y Swire, P. (2021), "EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an 'Essentially Equivalent' Solution", 21 de enero de 2021.

36 Véase "Opinion 4/2016, Opinion on the EU-U.S. Privacy Shield draft adequacy decision", 30 de mayo de 2016.

37 Véase, por ejemplo, "Congressional Research Services (2021). EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield", 17 de marzo de 2021.

Una nueva acción legislativa podría llevar tiempo. La situación política en EE.UU. es difícil, caracterizada por un Senado dividido, un marcado partidismo y las próximas elecciones de mitad de mandato. En consecuencia, la intención de EE.UU. es que la Comisión utilice su próxima Orden Ejecutiva como base para su necesaria decisión de adecuación. Sin embargo, esta solución diplomática puede ser anulada por el TJUE, o criticada por la JEPD o las autoridades nacionales de protección de datos de Europa por ser incompatible con el RGPD o la Carta de Derechos Fundamentales de la UE. Del mismo modo, un nuevo tratado internacional que prevalezca sobre la Carta de los Derechos Fundamentales se encontraría probablemente con una importante resistencia pública en la UE y, por tanto, sería rechazado por los Estados miembros de la UE.

Teniendo en cuenta las leyes de protección de la privacidad impuestas recientemente por países de todo el mundo y las recientes decisiones de adecuación de la UE, por ejemplo, las decisiones sobre los equivalentes esenciales en las leyes de privacidad de Japón, Corea del Sur o Reino Unido, **cualquier nueva política para la protección de los datos personales en el comercio transfronterizo debería incluir unos derechos de reparación apropiados para los ciudadanos** (los interesados) **en los países receptores, los límites y los derechos de reparación en relación con la inteligencia indiscriminada,** y las autoridades independientes (incluidos los tribunales, pero no solo ellos) que puedan resolver las reclamaciones de los ciudadanos y de los responsables y los encargados del tratamiento de los datos. La mención a un "nuevo mecanismo de reparación de varios niveles que incluya un Tribunal de Revisión de la Protección de Datos independiente" por parte de la Casa Blanca el 25 de marzo parece tomar este camino, pero esto es sólo el principio.

En otras partes del mundo se podrían aceptar unos estándares elevados para las transferencias de datos personales de los individuos, en las que se garantice la privacidad, que sean compartidos e impulsados conjuntamente por la UE y EE. UU.. Si se reconoce el objetivo común de la UE y EE. UU. de defender unos valores comunes, la UE, EE. UU. y los Estados miembros de la UE, a título individual, podrían establecer un exigente estándar global que contuviera la propagación de las normas y prácticas adoptadas por los países autoritarios, por ejemplo, el modelo de soberanía de los datos de China, que se centra en el Estado, y las políticas de mano dura como los requisitos de localización obligatoria de los datos y las autoridades que tienen acceso ilimitado a la información personal de los ciudadanos sin su consentimiento. Una iniciativa conjunta de la UE y EE. UU. en este ámbito contribuiría a que los derechos de los consumidores fueran significativos, a una aplicación internacional de las normas más coherente y a proporcionar la seguridad que las empresas y los ciudadanos necesitan para aprovechar las nuevas oportunidades que ofrecen el comercio digital y el comercio transfronterizo.

esade

EsadeEcPol - Center
for Economic Policy

Open Internet Governance Institute

El Open Internet Governance nace para ayudar a dar forma a los debates sobre Internet, datos y gobernanza digital tanto en España como en toda la Unión Europea, aportando al mismo tiempo a una mejor comprensión de cómo utilizar mejor los nuevos datos y las herramientas relacionadas con la IA para apoyar y mejorar la formulación de políticas.

Pretendemos contribuir de una manera equilibrada y basada en la evidencia, apartándonos de la delimitación de los dilemas pesados para centrarnos en ofrecer soluciones viables. Nuestro objetivo último es apoyar la construcción de un sistema de gobernanza de Internet global y abierto, fomentando el mejor entorno digital posible para la sociedad del futuro.

Con el apoyo de

Meta