CONFERENCIA DE LAS NACIONES UNIDAS SOBRE COMERCIO Y DESARROLLO

UNCTAD

INFORME SOBRE LA ECONOMÍA DIGITAL 2021

Flujos de datos transfronterizos y desarrollo: *Para quién fluyen los datos*

NACIONES UNIDAS

CONFERENCIA DE LAS NACIONES UNIDAS SOBRE COMERCIO Y DESARROLLO

UNCTAD

INFORME SOBRE LA ECONOMÍA DIGITAL 2021

Flujos de datos transfronterizos y desarrollo: *Para quién fluyen los datos*

NACIONES UNIDAS
Ginebra, 2021

United Nations Publications
405 East 42nd Street,
New York, New York 10017
Estados Unidos de América
Correo electrónico: publications@un.org
Sitio web: https://shop.un.org/

Esta publicación ha sido objeto de revisión editorial externa.

Publicación de las Naciones Unidas publicada por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo.

UNCTAD/DER/2021

eISBN: 978-92-1-005827-8

ISSN: 2664-7052

eISSN: 2664-7044

Nota

La Sección de Políticas de TIC de la División de Tecnología y Logística de la UNCTAD desarrolla una labor analítica orientada a las políticas sobre las implicaciones de las tecnologías de la información y las comunicaciones (TIC) y el comercio electrónico en el desarrollo. Se ocupa de la preparación del *Informe sobre la economía digital*, anteriormente conocido como el *Informe sobre la economía de la información*. La Sección también promueve el diálogo internacional sobre cuestiones relacionadas con las TIC que favorecen el desarrollo y contribuye a potenciar las capacidades de los países en desarrollo en materia de medición del comercio electrónico y la economía digital y de diseño e implementación de políticas y marcos jurídicos en ese campo. También se ocupa de gestionar la iniciativa *eTrade for all* (Comercio Electrónico para Todos).

Cuando en el presente Informe se hace referencia a "países" o "economías", el término se aplica también a territorios o zonas, según el caso. Los nombres de los grupos de países utilizados solo tienen por finalidad facilitar el análisis general o estadístico y no implican juicio alguno sobre la etapa de desarrollo alcanzada por un país o una región. Salvo que se indique otra cosa, los grandes grupos de países empleados en el presente Informe siguen la clasificación de la Oficina de Estadística de las Naciones Unidas. Estos son:

Países desarrollados: los países miembros de la Organización de Cooperación y Desarrollo Económicos (OCDE) (con exclusión de Chile, México, la República de Corea y Turquía), a los que se suman los países de la Unión Europea que no son miembros de la OCDE (Bulgaria, Chipre, Croacia, Lituania, Malta y Rumania), además de Andorra, Liechtenstein, Mónaco y San Marino. *Países con economías en transición:* los Estados de Europa Sudoriental y de la Comunidad de Estados Independientes. *Países en desarrollo:* en general, todas las economías no mencionadas más arriba. A efectos estadísticos, en los datos correspondientes a China no se incluyen los de la Región Administrativa Especial de Hong Kong (Hong Kong (China)), los de la Región Administrativa Especial de Macao (Macao (China)) ni los de la Provincia China de Taiwán. Los principales grupos de países utilizados figuran en un archivo de Excel que se puede descargar desde UNCTADstat, en: http://unctadstat.unctad.org/EN/Classifications.html.

Cuando en el texto o en los cuadros se hace referencia a América Latina cabe entender que el término también engloba a los países del Caribe, a menos que se indique otra cosa.

Cuando se hace referencia a África Subsahariana cabe entender que el término también engloba a Sudáfrica, a menos que se indique otra cosa.

Las referencias que se hacen a los Estados Unidos corresponden a los Estados Unidos de América y las que se hacen al Reino Unido corresponden al Reino Unido de Gran Bretaña e Irlanda del Norte.

Por dólares cabe entender dólares de los Estados Unidos de América, salvo que se indique otra cosa.

En los cuadros pueden haberse utilizado los símbolos siguientes:

Dos puntos (..) indican que los datos faltan o no constan por separado.

El que se haya prescindido de una fila indica que no se dispone de datos sobre ninguno de los elementos que la componen.

Una raya (-) indica que la cantidad correspondiente es igual a cero o su valor es despreciable.

Un espacio en blanco indica que los datos correspondientes no son de aplicación, a menos que se indique otra cosa.

La barra (/) entre dos años, por ejemplo 1994/95, indica un ejercicio económico.

Un guion (-) entre dos años, por ejemplo 1994-1995, significa todo el período considerado, incluidos el primer año y el último.

Las tasas anuales de crecimiento y de variación son tasas anuales compuestas, a menos que se indique otra cosa.

Debido al redondeo de las cifras, la suma de los datos parciales y de los porcentajes no siempre coincide con el total indicado.

Prefacio

La pandemia de COVID-19 ha acelerado el proceso de transformación digital y ha hecho más urgente la respuesta de los gobiernos. Un reto clave es la gobernanza y el aprovechamiento del enorme aumento de los datos digitales para el bien global. Se ha estimado que el tráfico mundial de Internet en 2022 superará todo el tráfico de Internet hasta 2016.

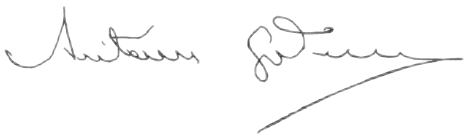
Los datos se han convertido en un activo estratégico clave para la creación de valor tanto privado como social. La forma en que se manejen estos datos afectará en gran medida a nuestra capacidad para lograr los Objetivos de Desarrollo Sostenible. Determinar cuál es el mejor camino será difícil pero necesario. Los datos son multidimensionales y su uso tiene implicaciones no solo para el comercio y el desarrollo económico, sino también para los derechos humanos, la paz y la seguridad. También se necesitan respuestas para mitigar el riesgo del abuso y mal uso de los datos por Estados, agentes no estatales o el sector privado.

Con este telón de fondo, cabe celebrar la publicación del *Informe sobre la economía digital* de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, en el que se examinan las implicaciones de los crecientes flujos de datos transfronterizos, especialmente para los países en desarrollo. En el Informe se propone un replanteamiento y ampliación del debate internacional sobre políticas con vistas a lograr un consenso multilateral.

Es más importante que nunca emprender un nuevo camino para la gobernanza digital y de los datos. El actual y fragmentado panorama de la cuestión de los datos hace que corramos el riesgo de no capturar el valor que podrían acrecentar las tecnologías digitales y puede crear mayores posibilidades de que se produzcan daños sustanciales debido a vulneraciones de la privacidad, ciberataques y otros riesgos.

En el Informe se preconizan enfoques innovadores para la gobernanza de los datos y de los flujos de datos con el fin de garantizar una distribución más equitativa de los beneficios derivados de esos flujos, al tiempo que se abordan los riesgos y los motivos de preocupación. Todo enfoque de las políticas que sea global e integral tiene que reflejar las múltiples e interrelacionadas dimensiones de los datos y encontrar un equilibrio entre los diferentes intereses y necesidades, de manera que pueda apoyarse el desarrollo inclusivo y sostenible con la plena participación de los países más rezagados en lo tocante a la capacidad de preparación digital.

Las Naciones Unidas ofrecen una plataforma natural para hacer avanzar esta agenda con la participación de todas las partes interesadas. El presente Informe proporciona ideas y análisis valiosos, por lo que recomiendo su lectura a un público mundial, especialmente en un momento como el presente en que todos perseguimos el objetivo de colmar la brecha digital y de posibilitar que nadie se quede descolgado en una economía digital impulsada por los datos en rápida evolución.



António Guterres
Secretario General
Naciones Unidas

Prólogo

La rápida digitalización está afectando a todos los aspectos de la vida, incluida la forma en que nos relacionamos, trabajamos, compramos y recibimos servicios, así como la forma en que se crea e intercambia el valor. En este proceso, los datos y los flujos de datos transfronterizos son cada vez más cruciales para el desarrollo.

Como reflejo de las grandes diferencias en la disposición a aprovechar los datos que existen entre los países y dentro de ellos, se suma a la brecha digital convencional, relacionada con la conectividad, lo que puede llamarse una brecha en lo referente a los datos. Los países con capacidades limitadas para convertir los datos en inteligencia digital y oportunidades de negocio y utilizarlos para fomentar el desarrollo económico y social están en clara desventaja.

El presente *Informe sobre la economía digital 2021* señala las complejidades que entraña la gobernanza de los datos y los flujos de datos transfronterizos, de manera que puedan aportar beneficios que favorezcan el desarrollo sostenible. También se subraya que el debate internacional sobre cómo regular los flujos de datos transfronterizos se encuentra en un punto muerto y que las posiciones tienden a polarizarse. El vigente panorama regulatorio es desigual y reflejo de los enfoques muy diferentes adoptados por los distintos países; además está sujeto a las fuertes influencias que ejercen las principales potencias económicas.

Urge, pues, un marco internacional para hacer frente a este problema. Si bien es cierto que en el Informe no se ofrece “la solución”, su análisis exhaustivo y basado en la evidencia pretende replantear y ampliar el debate internacional sobre políticas. Los grandes retos en materia de interconexión e interdependencia de la economía global que plantea la cuestión de los datos exige un abandono de la compartimentación que supone el enfoque de silos y la adopción de un enfoque global más integral y coordinado. A tal efecto, tal vez resulten necesarias nuevas e innovadoras formas de gobernanza mundial, toda vez que las antiguas podrían no ser las adecuadas para responder al nuevo contexto. Asimismo, podría ser necesario crear un nuevo organismo internacional que se centre en la gobernanza de los datos y en el que puedan participar plenamente los países en desarrollo y todas las partes interesadas.

El Informe es reflejo del compromiso de la UNCTAD de informar a los Estados miembros sobre cómo adquirir un mayor protagonismo en los datos y la economía digital y sacarles un mayor rendimiento. También contribuirá al tan necesario diálogo mundial sobre cómo establecer las reglas del juego para que el resultado de la digitalización sea más inclusivo. Albergo la esperanza de que un enfoque integral de la gobernanza global de los datos comporte en última instancia una potenciación del desarrollo sostenible y de la economía digital que redunde en beneficio de las personas y las empresas de todos los países con independencia de cuál sea su grado de desarrollo.

Isabelle Durant
Secretaria General Interina
Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

Agradecimientos

El *Informe sobre la economía digital 2021* fue preparado, bajo la dirección general de Shamika N. Sirimanne, Directora de la División de Tecnología y Logística, por un equipo formado por Torbjörn Fredriksson (jefe de equipo) y Pilar Fajarnés Garcés (autora principal), Laura Cyron, Martine Julsaint Kidane, Woong Joe Ko, Vincent Riegel, Marcin Skrzypczyk y Thomas van Giffen.

Para su preparación ha contado con las inestimables contribuciones de Carolina Aguerre, Shamel Azmeh, Zeynep Engin, Christopher Foster y Neha Mishra, así como del Centre for International Governance Innovation (CIGI). Se recibieron valiosos comentarios de los expertos que asistieron a una reunión virtual de revisión por homólogos celebrada en febrero de 2021 y que fue organizada conjuntamente por la UNCTAD, la Research ICT Africa y el CIGI. Participaron los siguientes expertos: Susan Aaronson, Anna Abramova, Idris Ademuyiwa, Martin Adolph, Carolina Aguerre, Shamira Ahmed, Renata Avila, Shamel Azmeh, Dan Ciuriak, Niccolo Comini, Diane Coyle, Zeynep Engin, Bob Fay, Martina Ferracane, Christopher Foster, Henry Gao, Alison Gillwald, Ebru Gokce, Anita Gurumurthy, Victor Ido, Taisuke Ito, Jonathan Klaaren, Kostantinos Komaitis, Isya Kresnadi, Sophie Kwasny, Patrick Leblond, Stephen MacFeely, Moritz Meier-Ewert, Neha Mishra, Michael Pisa, Lorrayne Porciuncula, Rishab Raturi, Gabriella Razzano, Nivedita Sen, David Souter, Tim Sullivan, Linnet Taylor, Stefaan Verhulst, Dong Wu y Anida Yupari. También se recibieron comentarios por escrito de Jörg Mayer.

La UNCTAD quiere expresar todo su agradecimiento por las aportaciones adicionales de la Comisión Económica para Europa, la Comisión Económica para América Latina y el Caribe, la Comisión Económica y Social para Asia y el Pacífico y la Comisión Económica y Social para Asia Occidental. Además, las siguientes organizaciones brindaron generosamente su muy apreciada aportación, que se basa en la labor que desarrollan actualmente: el Consejo de Europa; la Internet and Jurisdiction Policy Network; la Oficina del Enviado de las Naciones Unidas para la Tecnología; la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional; la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura; la Organización de las Naciones Unidas para el Desarrollo Industrial; y la Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas.

La UNCTAD agradece a la Unión Internacional de Telecomunicaciones su apoyo en el suministro de estadísticas relevantes.

La portada y otros gráficos fueron preparados por Magali Studer y de la maquetación asistida por computadora se encargaron Magali Studer y Carlos Bragunde. La infografía corrió a cargo de Natalia Stepanova, y Michael Gibson se encargó de la corrección editorial del texto inglés para su publicación. Diana Quirós prestó apoyo administrativo.

La UNCTAD agradece con reconocimiento el apoyo financiero del Gobierno de Alemania.

Índice

RECUADROS

CUADROS

FIGURAS

Lista de siglas y acrónimos

ACNUDH	Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos
AGCS	Acuerdo General sobre el Comercio de Servicios
AOD	asistencia oficial para el desarrollo
APEC	Foro de Cooperación Económica de Asia y el Pacífico
ASEAN	Asociación de Naciones de Asia Sudoriental
B2B	entre empresas
B2C	de la empresa al consumidor
BGP	protocolo de puerta de enlace de borde
C2C	de consumidor a consumidor
CAFTA	Tratado de Libre Comercio de Centroamérica
CBPR	Sistema de Normas Transfronterizas de Privacidad
CEI	Comunidad de Estados Independientes
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
DEPA	Acuerdo de Asociación de Economía Digital
FGI	Foro para la Gobernanza de Internet
FMI	Fondo Monetario Internacional
G2C	del gobierno al consumidor
GATT	Acuerdo General sobre Aranceles Aduaneros y Comercio
IA	inteligencia artificial
INB	ingreso nacional bruto
IP	protocolo de Internet
IXP	punto de intercambio de tráfico de Internet
OCDE	Organización de Cooperación y Desarrollo Económicos
OMC	Organización Mundial del Comercio
PIB	producto interno bruto
PMA	países menos adelantados
PSI	proveedor de servicios de Internet
RCEP	Asociación Económica Integral Regional
RGPD	Reglamento General de Protección de Datos
TI	tecnología de la información
TIC	tecnología de la información y las comunicaciones
TIPAT	Tratado Integral y Progresista de Asociación Transpacífico
T-MEC	Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá
TPP	Acuerdo de Asociación Transpacífico
UIT	Unión Internacional de Telecomunicaciones
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
W3C	Consorcio World Wide Web

Panorama general

En el *Informe sobre la economía digital 2021* se profundiza en el desarrollo y las implicaciones políticas de los flujos transfronterizos de datos digitales. Los datos digitales son el núcleo de todas las tecnologías digitales que están emergiendo con suma rapidez, como la analítica de datos, la inteligencia artificial (IA), la tecnología de cadenas de bloques, el Internet de las cosas, la computación en la nube y todos los servicios basados en Internet. El tema es oportuno, por cuanto la expansión de los flujos de datos es importante para la consecución de prácticamente todos los Objetivos de Desarrollo Sostenible. Los países de todo el mundo se esfuerzan por determinar cómo abordarlos desde la perspectiva normativa. El enfoque que al final se elija a nivel nacional e internacional afectará no solo al comercio, la innovación y el progreso económico, sino también a una serie de cuestiones relacionadas con la distribución de las ganancias derivadas de la digitalización, así como con los derechos humanos, la aplicación de la ley y la seguridad nacional.

El presente *Informe* pretende contribuir a una mejor comprensión de estos complejos e interrelacionados factores aportando una mirada nueva e integral de este tipo singular de flujo económico internacional. Su análisis se basa en un examen de los estudios que abordan los flujos de datos transfronterizos desde diversas perspectivas, una revista general de la evolución y las desigualdades globales en una economía digital impulsada por los datos y en un debate sobre la naturaleza fundamental de los datos. En el Informe también se examinan los enfoques de gobernanza aplicados actualmente a nivel nacional, regional y multilateral, prestando un interés especial a los flujos de datos. Concluye propugnando un enfoque más equilibrado de la gobernanza de los datos a nivel global que pueda ayudar a garantizar que los datos puedan fluir a través de las fronteras tan libremente como sea necesario y posible, pero que al mismo tiempo permita lograr una distribución equitativa de los beneficios, tanto dentro de cada país como entre los distintos países, y aborde asimismo la cuestión de los riesgos relacionados con los derechos humanos y la seguridad nacional.

Los flujos de datos son difíciles de medir, pero siguen creciendo rápidamente

Medir el tráfico de datos es difícil, pero, sea cual sea el enfoque que se utilice, la tendencia es marcadamente alcista. Una previsión indica que el tráfico global con el Protocolo de Internet (IP) en 2022 —nacional e internacional— superará todo el tráfico de Internet registrado hasta 2016. La pandemia de COVID-19 tuvo un inmenso impacto en el tráfico de Internet, pues la mayoría de las actividades se realizaron cada vez más en línea. Ante este telón de fondo, el ancho de banda global de Internet se incrementó en un 35 % en 2020, que es el mayor crecimiento en un año desde 2013. Se ha estimado que cerca del 80 % de todo el tráfico de Internet está relacionado con los vídeos, las redes sociales y los juegos. Se prevé que el tráfico global de datos mensual experimente un importante aumento: desde 230 *exabytes* en 2020 a 780 *exabytes* en 2026.

Medir los flujos de datos *transfronterizos* es aún más difícil. En términos de volumen, la medida más utilizada es la capacidad total utilizada del ancho de banda internacional de Internet. Mide la cantidad de datos que fluyen en términos de *bytes*, pero no muestra la dirección de los flujos ni ofrece ninguna indicación sobre la naturaleza y calidad de los datos. La información disponible también indica que el uso del ancho de banda internacional se aceleró durante la pandemia, y que dicho tráfico se concentró geográficamente en dos rutas principales: entre América del Norte y Europa, y entre América del Norte y Asia.

La economía digital impulsada por los datos se caracteriza por grandes desequilibrios...

A la hora de evaluar las implicaciones de los datos y los flujos de datos transfronterizos para el desarrollo, es preciso tener en cuenta algunas brechas y desequilibrios digitales que son de fundamental importancia. Solo el 20 % de los habitantes de los países menos adelantados (PMA) son usuarios de Internet; cuando lo son, tienen que contentarse con velocidades de descarga relativamente bajas y a un precio relativamente

alto. Además, la naturaleza del uso de Internet es diferente. Por ejemplo, mientras que hasta 8 de cada 10 usuarios de Internet compran en línea en varios países desarrollados, esa cifra baja a 1 de cada 10 en muchos PMA. Además, dentro de los países se observan importantes diferencias entre zonas rurales y urbanas, así como entre hombres y mujeres. Las mayores brechas de género se observan en los PMA y en la región africana.

En términos de capacidad para participar en la economía digital impulsada por los datos y rentabilizarla, sobresalen dos países: Estados Unidos y China. Estos dos países juntos representan la mitad de los centros de datos de hiperescala del mundo, las tasas más altas del mundo de adopción de 5G, el 94 % de toda la financiación de las nuevas empresas de IA en los últimos cinco años, el 70 % de los investigadores en IA más competentes del mundo y casi el 90 % de la capitalización bursátil de las mayores plataformas digitales del mundo. Las mayores plataformas de este tipo, como Apple, Microsoft, Amazon, Alphabet (Google), Facebook, Tencent y Alibaba, invierten cada vez más en todos los eslabones de la cadena global de valor de los datos: desde su recopilación hasta los servicios de plataforma de cara al usuario; las transmisiones de datos a través de cables submarinos y satélites; el almacenamiento de datos (centros de datos); y el análisis, procesamiento y uso de datos mediante, por ejemplo, la IA. Estas empresas presentan una ventaja competitiva en lo que a los datos se refiere, que se deriva de su componente de plataforma, pero ya no son solo plataformas digitales. Se han convertido en corporaciones digitales globales de ámbito planetario; han adquirido un enorme poder financiero, tecnológico y de mercado, además de controlar grandes cantidades de datos sobre sus usuarios. Además, durante la pandemia se han visto reforzadas en términos de tamaño, beneficios, valor de mercado y posición dominante, ya que la digitalización se ha acelerado. Por ejemplo, mientras que el índice compuesto de la Bolsa de Nueva York entre octubre de 2019 y enero de 2021 aumentó en un 17 %, las cotizaciones de las principales plataformas experimentaron una subida de entre un 55 % (Facebook) y un 144 % (Apple).

La tradicional brecha digital entre países desarrollados y en desarrollo —entendida en términos de conectividad, acceso y uso de Internet— sigue siendo considerable y es un problema recurrente para el desarrollo. Además, a medida que el papel de los datos como recurso económico, así como el de los flujos de datos transfronterizos, ha adquirido mayor relevancia, han aparecido nuevas dimensiones en la cuestión de la brecha digital, esta vez, en relación con la "cadena de valor de los datos". Este concepto es fundamental para la estimación del valor de los datos. El valor se genera en el proceso de transformación de los datos brutos —desde la recogida de datos, pasando por el análisis y el procesamiento hasta llegar la inteligencia digital— que puede ser monetizada con fines comerciales o utilizada para objetivos sociales. Los datos individuales no tienen valor si no se agregan y procesan. Y viceversa no puede haber inteligencia digital sin los datos brutos. Para la creación y captura de valor, se necesitan tanto los datos en bruto como las capacidades para procesarlos y convertirlos en inteligencia digital. Generar valor añadido en los datos es lo que contribuye a avanzar en el proceso de desarrollo.

Con la evolución de la economía digital impulsada por los datos se ha agravado la brecha relacionada con los datos. En esta nueva configuración, los países en desarrollo pueden encontrarse en posiciones subordinadas, ya que los datos y la captura de su valor asociado se concentran en unas pocas empresas digitales globales y otras empresas multinacionales que controlan los datos. Estos países corren el riesgo de convertirse en meros proveedores de datos en bruto para las plataformas digitales globales y de tener que pagar por la inteligencia digital obtenida a partir de sus datos.

..... y se carece de una comprensión común de lo que son y pueden hacer los datos y sus flujos transfronterizos

A pesar de la importancia de los datos en la evolución de la economía digital, no existe una comprensión universalmente común del concepto de datos, lo que puede llevar a confusión e incrementar la complejidad de los análisis y los debates sobre políticas. Los datos son un recurso especial que presentan unas características particulares que los diferencian de los bienes y servicios. Son intangibles y no rivales, lo que significa que muchas personas pueden utilizar los mismos datos, o bien simultáneamente, o bien a lo largo del tiempo sin agotarlos. Al mismo tiempo, el acceso a los datos puede estar limitado por medios técnicos o legales, lo que da lugar a diversos grados de excluibilidad. Por ejemplo, los datos recogidos

por las principales plataformas globales no están disponibles para que otros los utilicen, lo que brinda a los propietarios de las plataformas una posición de monopolio a la hora de rentabilizar los datos. Además, el valor añadido puede ser a menudo mayor que la suma de los valores individuales, especialmente si se combina con otros datos complementarios. Los datos brutos recopilados también pueden tener un valor "opcional" considerable, por cuanto podrían resultar valiosos si a partir de esos datos se pueden abordar nuevos problemas que anteriormente eran inexistentes. Cuanto más detallados y granulares sean los datos, para más fines podrán utilizarse una vez filtrados, agregados y combinados de diferentes maneras, lo que permite generar diferentes conocimientos.

Además, los datos son de naturaleza multidimensional. Desde el punto de vista económico, pueden aportar no solo un valor privado para quienes recopilan y controlan los datos, sino también un valor social para el conjunto de la economía. Y este último valor no puede ser garantizado solo por los mercados. Asimismo, la distribución de los incrementos de los ingresos privados conseguidos a través de los datos es muy desigual. En consecuencia, es necesario que la formulación de las políticas sirva para apoyar los objetivos de eficiencia y equidad. Sin embargo, también hay que tener en cuenta dimensiones no económicas, ya que los datos están estrechamente relacionados con la privacidad y otros derechos humanos, así como con cuestiones de seguridad nacional, aspectos todos ellos que deben ser abordados.

La comprensión de los datos y sus flujos exige observar la cuestión desde diferentes ángulos. En primer lugar, siempre ha habido *datos e información asociada a las transacciones comerciales* —como los datos de facturación, los datos bancarios, los nombres y las direcciones de entrega— que se brindan principalmente de forma voluntaria y rara vez crean problemas desde el punto de vista de las políticas, siempre y cuando los nuevos actores de la economía digital operen con las mismas reglas que las de la economía convencional. En segundo lugar, los *datos brutos* recopilados a partir de actividades, productos, eventos y comportamientos individuales no tienen valor en sí mismos, pero pueden generar valor una vez agregados, procesados y monetizados, o cuando se utilizan con fines sociales. En tercer lugar, el procesamiento de datos brutos para su transformación en inteligencia digital —en forma de estadísticas, bases de datos, conocimientos, información, etc.— genera *"productos de datos"*, que pueden categorizarse como servicios en las estadísticas comerciales cuando se venden a través de las fronteras.

También existen diferentes taxonomías que clasifican los tipos de datos con arreglo a diversos criterios. Las distinciones importantes responden al hecho de que los datos pueden recopilarse con fines comerciales u oficiales; sean utilizados por empresas o por el sector público; sean instantáneos o históricos; sean sensibles o no sensibles, o sean personales o no. La categorización de los datos es importante, puesto que puede tener implicaciones para el tipo de acceso que sería necesario dar a cada tipo, tanto a nivel nacional como internacional, así como para la forma de manejar los datos y sus flujos transfronterizos desde la perspectiva de las políticas.

Los flujos de datos transfronterizos no son comercio y deben tratarse pues de forma diferente

Las características particulares de los datos sugieren que deben ser tratados de forma diferente a los bienes y servicios convencionales, incluso en sus transferencias internacionales. En el nuevo contexto de la economía digital impulsada por los datos, ya se cuestionan conceptos como propiedad y soberanía. Más que intentar determinar quién es el "propietario" de los datos, lo que importa es quién tiene derecho a acceder, controlar y utilizarlos.

Existen importantes dificultades para compaginar la noción de soberanía nacional, tradicionalmente asociada a los territorios de los países, y la naturaleza no territorial, la globalidad y la apertura del espacio digital en el que fluyen los datos. La soberanía digital a menudo está relacionada con la necesidad de almacenar datos dentro de las fronteras nacionales, pero el vínculo entre el almacenamiento geográfico de los datos y el desarrollo no es evidente. Asignar territorialidad a los flujos de datos transfronterizos también plantea un difícil desafío. Los datos pueden entenderse mejor como compartidos, más que como comercializados o intercambiados.

La gobernanza del comercio internacional se nutre de estadísticas que se basan en los tipos, valores y localizaciones del comercio (incluidos el origen y el destino). Estos enfoques son difíciles, si no imposibles, de adoptar cuando se rastrean flujos de datos transfronterizos sobre los que no existen estadísticas oficiales. Unos enfoques con tanto arraigo como los que se aplican al comercio internacional entre distintos territorios (por ejemplo, las normas de origen) no pueden aplicarse con facilidad a los datos dada la naturaleza de estos. Los flujos de datos brutos que no están vinculados a un intercambio específico de un bien o servicio no se incluyen en el concepto de "comercio digital", según el manual para la medición del comercio digital elaborado por varias organizaciones internacionales.

Más allá de los desafíos técnicos para identificar los flujos de datos transfronterizos, se plantean también desafíos desde el punto de vista de las políticas y retos culturales. En el caso de muchas de las categorizaciones de datos que se pueden esbozar, se echan de menos definiciones convenidas a nivel mundial. Esto hace que a veces sea difícil determinar cómo deben tratarse los flujos de datos. Por ejemplo, las distintas definiciones pueden dar lugar a grandes diferencias en el volumen de flujos de datos categorizados como datos personales. Aunque los datos están fuertemente ligados al comercio, y pueden proporcionar fuertes ventajas competitivas a quienes sean capaces de sacarles partido, los flujos de datos transfronterizos no son en sí mismos ni comercio electrónico ni comercio, y no deberían ser regulados meramente como tales.

El dominio de los datos comporta ventajas de información, que se suman a las fuentes de posibles fallos del mercado en las economías conseguidas basándose en datos, en particular las economías de escala y de alcance, así como efectos de red. La asimetría de la información inherente a la economía de los datos parece irreductible, ya que no existen soluciones de mercado para corregirla. Otras soluciones de compromiso relacionados con la ética de los datos son igualmente importantes, como la relación entre la creación de valor a partir de los datos y la vigilancia de la población, y los vínculos entre el filtrado de datos y la censura. Así pues, la gobernanza de los datos y los flujos de datos resulta crucial. Sin embargo, si bien es cierto que establecer normas adecuadas en materia de flujos de datos fronterizos en su justa medida puede ayudar a garantizar los derechos en materia de datos, reducir los problemas estructurales y apoyar el desarrollo económico, no hay consenso sobre el enfoque que es preciso adoptar en las políticas.

La divergencia de enfoques sobre la gestión de los datos y los flujos de datos transfronterizos genera importantes implicaciones

Los principales actores económicos y geopolíticos de la economía digital, los enfoques de la gobernanza de los flujos de datos —y la economía digital en general— presentan variaciones considerables y, salvo raras excepciones, el consenso a nivel regional e internacional es escaso. A nivel mundial, son tres los principales enfoques de gobernanza que tienen una especial influencia. De manera algo simplificada se podría decir que el enfoque de los Estados Unidos se centra en el control de los datos por parte del sector privado. El modelo chino hace hincapié en el control de los datos por parte del aparato del Estado, mientras que la Unión Europea favorece el control de los datos por las personas sobre la base de derechos y valores fundamentales. El contexto actual es uno de tensión entre estas zonas, especialmente entre los Estados Unidos y China. Además, las empresas digitales globales están tratando de ampliar sus propios ecosistemas de datos.

Se observa una carrera por ocupar el liderazgo en cuanto a las novedades tecnológicas, ya que el líder puede obtener una ventaja tanto económica como estratégica, al controlar los datos y las tecnologías relacionadas, especialmente en lo que respecta a la IA. En este contexto, se corre el riesgo de que el espacio digital y de Internet se fragmente. En general, se corre el riesgo de que surja en el futuro una economía digital impulsada por los datos en compartimentos estancos, lo que va en contra del espíritu original de Internet como red libre, descentralizada y abierta. En términos económicos sería una situación subóptima, ya que es probable que la interoperabilidad brinde mayores ganancias.

La fragmentación de la economía digital impulsada por los datos obstaculizaría el progreso tecnológico, reduciría la competencia y permitiría la aparición de estructuras de mercado oligopólicas en algunos ámbitos, y en otros comportaría una mayor influencia del Estado. Esto podría acarrear importantes

repercusiones negativas para la mayoría de los países en desarrollo. La fragmentación reduciría las oportunidades de negocio, puesto que se complicaría el acceso de los usuarios y las empresas a las cadenas de suministro y se verían restringidos los flujos de datos transfronterizos. También habría más obstáculos para la colaboración entre jurisdicciones.

A pesar del riesgo de fragmentación, hay algunos signos de posible convergencia entre los principales reinos de datos. Por ejemplo, a pesar de poner el foco en el libre mercado, los Estados Unidos han tomado medidas para restringir la entrada en su mercado de algunas empresas extranjeras dedicadas a los datos y prohibir salidas de datos nacionales. Mientras tanto, China muestra indicios de decantarse por cierta apertura a los flujos de datos. El resultado final es difícil de predecir y dependerá de la voluntad de los responsables políticos de todo el mundo para encontrar una solución global que redunde en beneficio de todos.

Puede haber distintas y legítimas razones relacionadas con las políticas públicas para que los países regulen los flujos de datos transfronterizos, como la protección de la privacidad y otros derechos humanos, la seguridad nacional, así como los objetivos de desarrollo económico. Mientras no exista un sistema internacional adecuado que regule estos flujos, es posible que algunos países no tengan más opción que restringir los flujos de datos para conseguir determinados objetivos de sus políticas. Sin embargo, la localización de los datos no genera automáticamente valor añadido en los datos nacionales. La relación entre la localización del almacenamiento de datos y la creación de valor no es obvia, pues hay que tener en cuenta tanto los costos como los beneficios. Un examen de una serie de políticas nacionales indica que estos suelen variar en función de las condiciones tecnológicas, económicas, sociales, políticas, institucionales y culturales de cada país.

Con el protagonismo creciente que están adquiriendo los datos y los flujos de datos transfronterizos en la economía mundial, la necesidad de una gobernanza global resulta cada vez más urgente. Lamentablemente, las opiniones y posiciones divergentes sobre su regulación hacen que actualmente el debate internacional se halle en un punto muerto. A pesar del creciente número de acuerdos comerciales en los que se aborda la cuestión de los flujos de datos, los principales actores de la economía digital aún no han logrado ponerse de acuerdo en determinadas cuestiones. Entre los miembros del G20 se observa una división de opiniones, no solo en cuanto al fondo (por ejemplo, las medidas de localización de datos), sino también en cuanto al proceso.

Entretanto, adoptar posturas extremas sobre los flujos de datos transfronterizos no resulta útil, puesto que ni adoptar una postura estricta en cuanto a la localización ni la libertad total de los flujos de datos pueden satisfacer las necesidades de los países para lograr diversos objetivos de desarrollo. Es necesario replantear la regulación en esta materia y encontrar las bases para una solución intermedia. La nueva normativa deberá tener en cuenta todas las dimensiones de los datos, tanto las económicas como las no económicas. Deberá trascender el ámbito del comercio y abordar los flujos de datos de manera integral, teniendo en cuenta sus posibles repercusiones en los derechos humanos, la seguridad nacional, el comercio, la libre competencia, la fiscalidad y la gobernanza general de Internet. Llegados a este punto, se plantea la cuestión de cuál es el foro internacional adecuado para abordar las políticas en materia de datos que favorezcan el desarrollo.

Hay fundadas razones que abogan en favor de una gobernanza global de los datos y de los flujos de datos transfronterizos

Está más que justificada la instauración de un marco global de gobernanza de datos que complemente otros niveles de gobernanza. De manera resumida, los principales argumentos y razones son los siguientes:

- La gobernanza global de los datos permitiría compartirlos a nivel global y crear bienes públicos que pudiesen ayudar a afrontar los principales retos del desarrollo a nivel mundial, como la pobreza, la salud, el hambre y el cambio climático.
- La coordinación técnica transfronteriza —idealmente a nivel mundial— es esencial para evitar una mayor fragmentación de la infraestructura de Internet y del espacio digital.

- La gobernanza global de los datos adquiere mayor importancia a la luz de la implantación del 5G y el IoT, así como de la aceleración de la digitalización desencadenada por la pandemia de COVID-19. Estas tendencias amplían las posibilidades de recopilación y monetización de datos a nivel global. Sin la base de un marco de gobernanza global que sea coherente y suscite confianza, se podría producir un retroceso en el intercambio de datos. También se intensificarían los motivos de preocupación que ya suscitan la falta de transparencia en la cadena de valor de los datos y la distribución desigual de los beneficios generados por los datos.
- La proliferación de regulaciones nacionales en materia de flujos de datos transfronterizos crea incertidumbre y eleva los costes de cumplimiento, un aspecto que puede ser especialmente pernicioso para las microempresas y las pequeñas empresas, sobre todo las de los países en desarrollo. La naturaleza interconectada y el alto grado de interdependencia global en la economía digital impulsada por los datos significa que las políticas nacionales en este ámbito tienen efectos en otros países.
- En ausencia de una gobernanza global de las plataformas digitales, la autorregulación ha gestado unas estructuras de mercado definidas por las plataformas, en beneficio predominantemente de ellas mismas, lo que comporta diversas implicaciones para las políticas y el desarrollo. El alcance y la influencia cada vez más global de las grandes plataformas dificultan aún más que un solo país pueda hacer frente a los retos políticos que plantea el fenómeno.
- Es preciso preparar una evaluación exhaustiva y coherente de los riesgos, vulnerabilidades y resultados de los modelos de negocio adoptados por las plataformas digitales, en particular de las plataformas de medios sociales, en un contexto de aumento de los daños que se producen en Internet a escala global.
- Es necesario un enfoque global de la gobernanza de los datos para evitar que se amplíen en el espacio digital impulsado por los datos unas desigualdades tan arraigadas desde hace mucho tiempo y contrarias a los intereses de los países en desarrollo. Es esencial garantizar que los conocimientos, necesidades y puntos de vista propios de ellos estén suficientemente representados en los debates globales sobre políticas.
- Dadas las interdependencias y la interconectividad de la arquitectura global de Internet, el futuro de los flujos de datos transfronterizos no debería estar determinado únicamente por un pequeño número de países importantes.

La digitalización impulsada por los datos crea tanto oportunidades como desafíos globales que requieren soluciones también globales para aprovechar los efectos positivos y paliar los negativos. Una gobernanza global y eficaz de los datos es una condición *sine qua non* para que estos sirvan para apoyar la consecución de los objetivos económicos, sociales y medioambientales de la Agenda 2030 para el Desarrollo Sostenible y donde las personas sean el principal centro de interés.

Los esfuerzos para desarrollar un enfoque global de la gobernanza de los datos y de los flujos de datos transfronterizos deben tener en cuenta una serie de áreas y prioridades cruciales de las políticas, entre las que se encuentran las siguientes:

- Fomentar un entendimiento común sobre las definiciones de los conceptos clave relacionados con los datos.
- Establecer las condiciones de acceso a los datos.
- Reforzar la medición del valor de los datos y los flujos de datos transfronterizos.
- Tratar los datos como un bien público (global).
- Explorar formas incipientes de gobernanza de datos.
- Convenir los derechos y principios digitales y en materia de datos.
- Elaborar normas en materia de datos.

- Estrechar la cooperación internacional en el ámbito de la gobernanza de las plataformas, en particular en lo tocante a la política de defensa de la competencia y a la fiscalidad en la economía digital.

Se necesita una nueva configuración institucional para superar el reto de la gobernanza global de los datos

Los marcos institucionales vigentes a nivel internacional no son adecuados para abordar las características y necesidades singulares de la gobernanza global de los datos. Para que sea eficaz, lo más probable es que se necesite un nuevo marco institucional global, además de una conjunción adecuada de implicación multilateral, multipartita y multidisciplinar.

Hasta ahora, la gobernanza global de los datos y las tecnologías digitales ha discurrido por vías diferentes. En primer lugar, la mayoría de las cuestiones relacionadas con la gobernanza de Internet, en cuanto red de comunicaciones, se han tratado en varios foros multipartitos. La comunidad globalizada de Internet está bien organizada y profundamente implicada en la adopción de enfoques para coordinar los recursos de Internet y conseguir que esta red de redes funcione de manera eficiente. Estos procesos se desarrollan normalmente a través de una participación horizontal y en pie de igualdad.

En segundo lugar, y de forma similar, el Convenio 108 del Consejo de Europa brinda un foro en el que los gobiernos nacionales, los reguladores, las partes interesadas del sector privado y los representantes de la sociedad civil pueden recibir información y compartir ideas sobre la promoción y la mejora del Convenio.

En tercer lugar, con la expansión de los flujos de datos transfronterizos, los gobiernos han tratado de integrar su gobernanza en las normas internacionales de comercio. Estos procesos comportan la negociación entre los firmantes de un conjunto de normas, que puede incluir la posibilidad de un mecanismo de resolución de conflictos. En comparación con las otras dos vías mencionadas, los acuerdos comerciales se caracterizan por su escasa transparencia, por cuanto las negociaciones suelen desarrollarse en procesos cerrados y con escasa participación de las partes interesadas no estatales.

Como alternativa a la creación de organizaciones ya existentes, se han hecho llamamientos cada vez más numerosos en favor de la creación de una institución coordinadora centrada en la evaluación y el desarrollo de una gobernanza global del espacio digital y de los datos, y que además tenga las competencias técnicas necesarias para realizar esa labor. Habría que reconocer que las actuales instituciones mundiales se construyeron para un mundo diferente, que el nuevo mundo digital está dominado por los intangibles y que precisamente por ello se necesitan nuevas estructuras de gobernanza.

No será fácil lograr un terreno común de entendimiento ni soluciones globales. De hecho, en esta época de populismo, antiglobalización e intereses creados que compiten entre sí y asociados a la captura de rentas a partir del uso de las tecnologías y los datos digitales, puede parecer contraproducente proponer un nuevo organismo internacional. Sin embargo, todos estos factores hacen que sea más necesario que nunca tomar una nueva senda global en la gobernanza del espacio digital y de los datos.

Reforzar los reinos de datos o una escisión en múltiples esferas provocaría una situación caótica que provocaría aun una mayor confusión. Esto disminuiría sustancialmente el valor que pueden generar estas tecnologías y los datos asociados, además de crear posibilidades para que se produzcan daños sustanciales en la privacidad y la ciberseguridad, así como otros riesgos.

Para que los debates mundiales sobre la gobernanza de los datos y los flujos de datos transfronterizos sean plenamente inclusivos, lo ideal sería que se celebraran bajo los auspicios de las Naciones Unidas, que es el foro internacional más inclusivo en términos de representatividad de los países. En la actualidad, los países en desarrollo tienden a estar poco representados en las iniciativas mundiales y regionales, lo que implica el riesgo de descuidar sus necesidades, sus conocimientos locales y el contexto cultural en los debates políticos mundiales, lo que se traduce en un aumento de la desigualdad. Ya se han puesto en marcha varias iniciativas en las Naciones Unidas que son de una gran importancia para la gobernanza de los datos, como, por ejemplo, las de la Comisión de Ciencia y Tecnología para el Desarrollo de las Naciones Unidas; la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos;

la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional; la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura; el Foro para la Gobernanza de Internet y la Unión Internacional de Telecomunicaciones (UIT). La UNCTAD también contribuye a través de sus tres pilares de trabajo, mediante la investigación, las actividades de búsqueda de consenso y su labor de cooperación técnica. Para que las Naciones Unidas puedan desempeñar su papel en este contexto, será necesario garantizar unos vínculos eficaces con otros procesos e iniciativas puestas en marcha y dirigidas por la sociedad civil, el mundo académico y el sector privado.

Conseguir que fluyan los datos en beneficio de todos exige mayores esfuerzos para colmar las brechas

Cualquier esfuerzo por aprovechar los datos y los flujos de datos transfronterizos requerirá prestar una atención adecuada a las actuales brechas que caracterizan a la economía digital global. No solo se observan entre los países, sino también entre las partes interesadas. Por ejemplo, la falta de competencias adecuadas en la administración pública se refleja directamente en una representación insuficiente de expertos y analistas en los procesos de elaboración de marcos legislativos y regulatorios. Esto, a su vez, limita las posibilidades de que los gobiernos detecten tanto las oportunidades que podrían ofrecer las tecnologías digitales como los posibles riesgos y amenazas que podrían plantear, así como las formas de regularlas. Con ello se corre el riesgo de una mayor dependencia pública del sector privado, motivado únicamente por los beneficios, con lo que los valores democráticos y los derechos humanos individuales se verían significativamente mermados. Los países menos desarrollados también experimentan la pérdida de sus mejores talentos en favor de los países desarrollados, y tienen una menor representación a la hora de establecer las bases del debate político mundial, lo que contribuye a una creciente desigualdad a nivel global.

Cualquier marco internacional de regulación de los flujos de datos transfronterizos debe complementar y ser coherente con las políticas nacionales concebidas para que la economía digital impulsada por los datos favorezca el desarrollo. Será preciso ser flexible para que los países con diferentes niveles de preparación y capacidades para rentabilizar los datos tengan el espacio político necesario para diseñar y aplicar sus estrategias de desarrollo en la economía digital impulsada por los datos. Al mismo tiempo, las políticas o estrategias nacionales destinadas a favorecer el desarrollo en este contexto podrían fracasar si no tienen en cuenta una perspectiva global.

Aunque todos los países tendrán que destinar más recursos internos al fomento de sus capacidades para generar valor a partir de los datos y capturarlo a nivel nacional, en muchos países los recursos financieros, técnicos y de otro tipo pueden tal vez ser insuficientes para satisfacer esas necesidades. Así podría ocurrir muy especialmente en el caso de los PMA. Si bien la pandemia de COVID-19 y su impacto en los ingresos del Estado han reducido aún más la disponibilidad de fondos públicos, también han hecho que los gobiernos y otras partes interesadas sean más conscientes de la necesidad de mejorar su capacidad de preparación para participar en la economía digital impulsada por los datos y aprovechar sus ventajas. Esta posibilidad pone de relieve la necesidad de apoyo internacional.

En un contexto de flujos de datos de carácter transfronterizo, el apoyo internacional puede centrarse en diversas áreas. En primer lugar, puede ayudar a formular los marcos jurídicos y regulatorios pertinentes. Por ejemplo, menos de la mitad de los PMA cuentan con legislación sobre protección de datos y privacidad. En segundo lugar, muchos países tienen que formular estrategias nacionales para tratar los datos y los flujos de datos transfronterizos de una manera que puedan servir para sacar el máximo partido de los avances logrados en su proceso de desarrollo; mientras que al mismo tiempo, deben observar los derechos humanos y ser vigilantes con ciertas cuestiones relacionadas con su seguridad. En tercer lugar, puede ser necesario realizar actividades de capacitación para concienciar sobre los temas relacionados con los datos y sus repercusiones para el desarrollo. Por último, para lograr resultados inclusivos en este ámbito en los diálogos regionales y mundiales, los países en desarrollo deben tener voz, así como los medios necesarios para participar eficazmente en los procesos y reuniones pertinentes.

Los datos digitales y los flujos de datos transfronterizos desempeñan un papel cada vez más importante en la economía mundial, lo que tiene importantes repercusiones en el logro de los Objetivos de Desarrollo Sostenible. Debido a que el tráfico de datos aumenta vertiginosamente tanto en el plano nacional como en el internacional, urge comprender mejor la dinámica de los flujos de datos transfronterizos para que se puedan formular respuestas políticas adecuadas en ambos planos.

En este primer capítulo se sientan las bases del presente Informe, al definirse el concepto de datos y señalarse algunas de las principales características de estos. En el contexto de la cadena mundial de valor de los datos, se examinan las últimas tendencias de las tecnologías digitales de especial relevancia para los datos y los flujos de datos transfronterizos. Se pone de relieve que la economía digital impulsada por los datos se caracteriza por grandes desequilibrios de poder entre países y a escala nacional, que se reflejan en niveles desiguales de preparación de los países para aprovechar los datos —y su circulación a través de las fronteras— con fines de crecimiento y desarrollo.

ULTIMAS TENDENCIAS EN LA ECONOMÍA **DIGITAL** IMPULSADA POR LOS DATOS

I

CAPÍTULO I LA BRECHA DIGITAL DE CONECTIVIDAD A INTERNET Y DE SU USO ES AGRAVADA POR UNA BRECHA RELACIONADA CON LOS DATOS

Los **datos** son un **recurso especial**, diferente de los bienes y los servicios

Para **promover el desarrollo** es fundamental distinguir entre **datos brutos** y **productos de datos** (inteligencia digital)

La economía digital impulsada por los datos está evolucionando rápidamente en un contexto de **enormes diferencias** en cuanto a preparación digital

El **23 %** de la población de los PMA **no tiene acceso** a una red de **telefonía móvil de banda ancha**

Velocidad media de Internet

8x

Economías desarrolladas — PMA

Uso de Internet

90 % En las economías desarrolladas

20 % En los PMA

Dos países sobresalen en el aprovechamiento pionero del valor de los datos: Estados Unidos y China

El **50 %** de los centros de datos de hiperescala del mundo

Las tasas más altas del mundo en cuanto a la adopción de la **5G**

El **94 %** de toda la financiación de las empresas emergentes de IA

El **90 %** de la capitalización bursátil de las mayores plataformas digitales del mundo

Las mayores plataformas digitales controlan cada vez más todas las etapas de la cadena mundial de valor de los datos

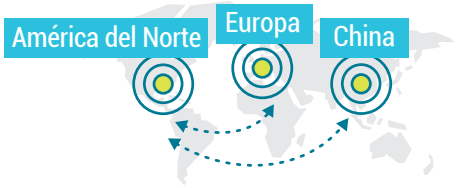
Durante la pandemia se han reforzado sus posiciones dominantes

Recopilación — Transmisión — Almacenamiento — Procesamiento — Uso

El crecimiento de los flujos de datos no ha hecho más que empezar

El tráfico mundial por protocolo de Internet superará en 2022 todo el tráfico registrado hasta 2016

El **uso de ancho de banda internacional** ha aumentado en el último decenio y se concentra geográficamente en **dos rutas principales:**



Los **datos** desempeñan un papel cada vez más importante como recurso económico estratégico, tendencia que se ha visto reforzada por la pandemia de COVID-19, ya que muchas actividades han pasado a realizarse a través de Internet

Los flujos de datos transfronterizos constituyen un nuevo tipo de flujo económico internacional y dan lugar a una nueva forma de interdependencia mundial

La regulación de los flujos de datos a escala internacional es ahora más urgente

A. INTRODUCCIÓN

La creciente digitalización de la economía y la sociedad está cambiando las formas de actuar e interactuar de las personas. Uno de los rasgos distintivos de las diversas transformaciones digitales ha sido el crecimiento exponencial de la información legible por máquinas, o datos digitales, a través de Internet (UNCTAD, 2019a). Esos datos son fundamentales para todas las tecnologías digitales que están creciendo vertiginosamente, como el análisis de datos, la inteligencia artificial (IA), la cadena de bloques, la Internet de las cosas, la computación en la nube y todos los servicios basados en Internet, y se han convertido en un recurso económico primordial. La pandemia de COVID-19 ha acelerado los procesos de digitalización, ya que cada vez más personas utilizan, en la medida de lo posible, canales en línea para realizar sus actividades, por ejemplo, para trabajar, estudiar, comunicarse, vender y comprar o entretenerse (UNCTAD, 2021a).

Los datos y los flujos de datos, ya sean nacionales o internacionales, pueden aportar numerosos beneficios y contribuir a hacer frente a los desafíos de la sociedad, incluidos los relacionados con los Objetivos de Desarrollo Sostenible. Si bien hay que aprovechar esos beneficios, es importante garantizar que se distribuyan de forma equitativa y no sean acaparados por unos pocos, y que resulten útiles para la sociedad. El proceso de digitalización en curso se acompaña de desequilibrios de poder y desigualdades que deben abordarse. Los datos son mucho más que un recurso económico, ya que también están relacionados con la privacidad y otras cuestiones de derechos humanos, así como con la seguridad nacional. Por ello, las políticas relacionadas con los datos deben incorporar un enfoque integrado y holístico.

En *The Age of Digital Interdependence – Report of the UN Secretary-General's High-level Panel on Digital Cooperation* (La era de la interdependencia digital: informe del Panel de Alto Nivel del Secretario General de las Naciones Unidas sobre la Cooperación Digital) (United Nations, 2019) se reconoce la importancia de los datos. Las recomendaciones formuladas en dicho informe dieron lugar a la Hoja de Ruta del Secretario General para la Cooperación Digital (United Nations, 2020a), en la que también se destaca la necesidad de aprovechar los datos para el desarrollo. El Secretario General presentó en 2020 su *Data Strategy for Action by Everyone, Everywhere with Insight, Impact and Integrity (2020–2022)* (Estrategia de datos para la acción de todos, en todas partes, con perspicacia, impacto e integridad), destinada a fomentar la transformación del propio sistema de las Naciones Unidas impulsada por los datos. En ella señaló que "hacer un mejor uso de los datos —con enfoques basados en los valores de las Naciones Unidas y los derechos humanos— es fundamental para nuestro futuro y servicio" (United Nations, 2020b:3).

Aunque la UNCTAD se centraba inicialmente en el comercio y el desarrollo, ha evolucionado de forma natural hacia un enfoque de interdependencia y desarrollo, ya que los dos primeros no pueden separarse de las cuestiones de interdependencia. La UNCTAD se ha convertido así en el centro de coordinación del sistema de las Naciones Unidas en lo que respecta al comercio y el desarrollo, así como a las cuestiones conexas en los ámbitos de la financiación, la tecnología, la inversión y el desarrollo sostenible. Todo ello también tiene que ver con la evolución de la situación de interdependencia entre los países en el marco de las tendencias de la globalización, así como entre los procesos nacionales, regionales e internacionales de formulación de políticas. La economía digital impulsada por los datos ha introducido una nueva forma de interdependencia a través de los flujos de datos transfronterizos.

En el contexto de la economía digital impulsada por los datos, y sobre todo en relación con los flujos de datos transfronterizos, resulta muy adecuada la famosa frase del escritor uruguayo Mario Benedetti: "Cuando creíamos que teníamos todas las respuestas, de pronto, cambiaron todas las preguntas"[1]. Si bien muchos de los principios y parámetros de la economía ordinaria pueden aplicarse fácilmente a la economía digital, también hay muchos conceptos económicos que pueden no ser de la misma utilidad y que deben ajustarse al nuevo espacio digital. Además, a medida que surgen nuevos conceptos y dinámicas, se hace necesario reformular considerablemente la economía. Por consiguiente, es importante comprender mejor el papel de los flujos de datos transfronterizos como nuevo recurso clave en las

[1] Para el origen de esta cita, véase *El País*, 11 de enero de 2016, "Queda inaugurada la nueva política", y https://citas.in/frases/1079317/history.

relaciones económicas internacionales y el desarrollo. Entre las diferentes interrogantes que se plantean se incluyen las siguientes:

- ¿Qué se entiende por datos?
- ¿Qué son los flujos de datos transfronterizos?
- ¿Cuáles son las implicaciones de los flujos de datos transfronterizos para el desarrollo?
- ¿Qué posibles políticas relativas a los flujos de datos transfronterizos pueden aumentar al máximo las oportunidades de desarrollo y abordar los desafíos para reducir al mínimo los riesgos de manera integrada y equitativa?

El objetivo del presente Informe es contribuir a dar respuesta a esas interrogantes. A partir de anteriores estudios de la UNCTAD en el mismo ámbito[2], se analiza en profundidad la cuestión de los flujos transfronterizos de datos digitales y las formas en que los países en desarrollo pueden verse afectados por dichos flujos. Se pretende ofrecer una visión fresca y holística de las implicaciones para el desarrollo de este nuevo tipo de flujo económico internacional.

Las cuestiones relacionadas con la regulación de los flujos de datos transfronterizos ocupan actualmente un lugar destacado en la agenda internacional, sobre todo en el contexto de las negociaciones comerciales. No obstante, como ya se ha mencionado, esos flujos son relevantes no solo en el contexto comercial, sino también en relación con los derechos humanos, la seguridad nacional y la aplicación de la ley. Las opiniones sobre los flujos de datos transfronterizos tienden a estar muy alejadas, y el debate actual está bastante polarizado. Hay quienes defienden a ultranza la libre circulación de los datos, mientras que otros subrayan, en particular, la necesidad de que el lugar de almacenamiento de los datos sea nacional con el fin de alcanzar diversos objetivos del país en cuestión. Se puede decir que en la actualidad el debate sobre los flujos de datos transfronterizos se encuentra en un punto muerto.

Por ello es momento de encontrar formas de lograr un mayor consenso. Con el fin de aprovechar todos los beneficios de Internet y de que la economía digital impulsada por los datos sea beneficiosa para las personas y el planeta, es necesario compartir los datos, en particular a través de las fronteras. Al mismo tiempo, es urgente regular adecuadamente los flujos de datos en el plano internacional, dentro del amplio contexto de la gobernanza global de los datos. Esa regulación debe ser flexible y tener en cuenta la variedad de condiciones y los muy diferentes grados de preparación digital de los países, así como sus objetivos de desarrollo. Como se analizará a lo largo de este Informe, los flujos de datos transfronterizos y la distribución de los beneficios de dichos flujos pueden ser regulados por normativas en distintos ámbitos. Encontrar un enfoque de gobernanza equilibrado no es tarea fácil, ya que las cuestiones que se plantean son complejas, no hay definiciones comúnmente aceptadas y cuantificar el fenómeno es todo un reto. El presente Informe pretende aportar valor en ese contexto contribuyendo a reforzar la base de datos empíricos, a entender mejor la dinámica de los flujos de datos transfronterizos y a estudiar posibles caminos.

Este capítulo sienta las bases del presente Informe, primero definiendo el concepto de datos y destacando algunas de sus principales características. En la sección C se destacan las importantes brechas que siguen existiendo en el acceso a las tecnologías de la información y las comunicaciones (TIC) y su uso. A continuación, se analiza la situación con respecto a determinadas variables relacionadas con los datos que reflejan las nuevas brechas que están surgiendo a medida que se desarrolla la economía digital impulsada por los datos. En la sección D se presenta la evolución mundial de Internet y del tráfico de datos, mientras que en la sección E se trata la forma de estimar el valor de los datos y de los mercados de datos. Las dificultades para cuantificar los flujos de datos transfronterizos se abordan en la sección F.

[2] El *Informe sobre la economía digital 2019* se centró en la creación y captura de valor en la economía digital, y puso de relieve el papel central de los datos, así como las implicaciones para los países en desarrollo (UNCTAD, 2019a); y en el *Informe sobre la economía de la información 2017* se hizo hincapié en la necesidad de examinar las interacciones entre la gobernanza mundial de Internet y el régimen comercial internacional (UNCTAD, 2017). Además, un estudio anterior sobre los flujos de datos se centró en cuestiones de protección de datos (UNCTAD, 2016), y en un estudio reciente se analizó la Iniciativa de Declaración Conjunta sobre el comercio electrónico y las cuestiones relacionadas con los flujos de datos transfronterizos (UNCTAD, 2021b).

Seguidamente se examina la evolución de las variables relacionadas con los datos a lo largo de la cadena mundial de valor de los datos: la recopilación de los datos (sección G), la transmisión y el almacenamiento de los datos (sección H) y el procesamiento y el uso de los datos (sección I). Cada una de esas etapas puede tener lugar en diferentes países, lo que genera flujos de datos transfronterizos. En la sección J se analizan algunos aspectos no económicos de los datos en relación con los derechos humanos, así como cuestiones relativas a la confianza. En la sección K se exponen algunas conclusiones y la estructura del resto del Informe.

B. DEFINICIONES Y CARACTERÍSTICAS DE LOS DATOS

Antes de examinar la evolución de la situación mundial de la economía digital impulsada por los datos, en esta sección se aborda la falta de claridad en la definición del concepto de datos, así como algunas características clave de los datos que los distinguen de los bienes y los servicios. Básicamente, en la economía digital, todo son datos. La digitalización de cualquier producto o actividad (que en general pueden llamarse "fenómenos") implica convertirlo en un lenguaje o código binario de ceros y unos. En consecuencia, todo en Internet son números y, por tanto, datos. Cada cero o cada uno representa un bit de información *legible por máquina*, es decir, la unidad de medida de información más pequeña que se puede leer digitalmente. Puede verse como la representación "virtual" de la vida "real". La conversión de los fenómenos de la vida real en códigos de ceros y unos legibles por máquina se realiza mediante *software*.

Entonces, con distintos tipos de *hardware* (por ejemplo, cables submarinos y centros de datos) se pueden transmitir y almacenar esos fenómenos codificados. Internet es una red de redes; en el momento en que los bits se transmiten de los dispositivos de los usuarios a la red comienzan a fluir los datos. Los flujos de datos consisten en la transferencia de esos fenómenos codificados digitalmente (en ceros y unos) entre dispositivos digitales. Esos flujos de datos no constituyen en sí mismos transacciones comerciales, sino la forma en que la información legible por máquina se transmite a través de la red. El funcionamiento de Internet y de la economía digital se basa fundamentalmente en la forma en que esos datos pueden fluir dentro de cada país y de unos países a otros. Dado que Internet es una red mundial, una gran parte de esos flujos de datos son transfronterizos (véase el capítulo III sobre cómo circulan los datos a través de las fronteras).

Lo que importa en general, y sobre todo a efectos de regulación, es lo que los ceros y los unos representan en la vida real, es decir, la información *"legible por el ser humano"* o lo que puede entender la mente humana. A pesar de la importancia de los datos en la evolución de la economía digital, no existe una interpretación común del concepto de datos, lo que puede llevar a confusión y complicar los análisis y los debates sobre políticas. Lo más frecuente en la literatura al respecto y en los debates sobre políticas es que se dé por hecho que todo el mundo entiende el concepto de datos de la misma manera. Da la impresión de que se considera una entidad en cierto modo homogénea y homotética, como un monolito. Sin embargo, la realidad dista mucho de ser así. De hecho, existe una considerable falta de claridad en cuanto a lo que significa el término.

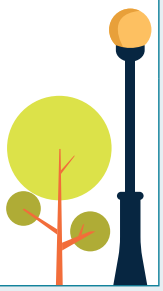
Aunque se han utilizado numerosas metáforas para explicar la naturaleza de los datos —sobre todo se han comparado con el petróleo—, los datos no se parecen a ninguna otra cosa y esas metáforas no resultan útiles para la elaboración de políticas (De La Chapelle y Porciuncula, 2021). Para comprender que los datos tienen una naturaleza diferente a la de los bienes y servicios, así como su valor, es importante reconocer sus características específicas, que se analizan en el recuadro I.1. En ese sentido, aunque los flujos de datos transfronterizos pueden tener implicaciones económicas, son un tipo de flujo "económico" internacional muy diferente de otros flujos económicos internacionales, como el comercio de bienes y servicios o los flujos financieros internacionales, por lo que deben abordarse desde una perspectiva diferente y más amplia.

Los datos son pequeños fragmentos inconexos de información "legible por el ser humano" (puntos de datos), que pueden ser números, pero que también pueden revelar aspectos cualitativos. Mediante la recopilación y el procesamiento de los datos se obtiene información, conocimientos y sabiduría que

Recuadro I.1. Características de los datos

Los datos son bienes intangibles y no rivales, lo que significa que muchas personas pueden utilizar los mismos datos simultáneamente, o a lo largo del tiempo, sin que se agoten. Al mismo tiempo, el acceso a los datos puede limitarse por medios técnicos o legales, lo que da lugar a diversos grados de excluibilidad. En términos técnicos, los datos pueden ser un bien público, un bien privado o un bien de club (cuando el acceso a ellos se concede solo a un grupo de personas). En la figura del recuadro se muestra el lugar que ocupa cada tipo de datos según su rivalidad y excluibilidad.

Figura del recuadro. Los datos en el especto rivalidad-excluibilidad

	EXCLUIBLES	NO EXCLUIBLES
RIVALES	*Bienes privados:* Alimentos, petróleo, ropa y otros productos manufacturados (teléfonos inteligentes), peces en un estanque privado, etc. 	*Bienes comunes:* Bosques, tierras, atmósfera, agua, peces del océano, etc. 
NO RIVALES	*Bienes de blub:* Televisión por satélite, parques privados, cines, *software* privativo, Internet de banda ancha, películas en *streaming* de pago, etc. 	*Bienes públicos:* Defensa nacional, aire, luz del sol, noticias, televisión pública, parques públicos, alumbrado público, faros, etc. 

DATOS

Fuente: UNCTAD, a partir de Schneider (2019) y Liu (2021).

Los datos también suelen conllevar externalidades positivas o negativas. El valor agregado puede ser a menudo mayor que la suma de los valores individuales. Los datos tienen también un valor relacional, es decir, muchos tipos de datos adquieren más valor al combinarse con otros datos complementarios. Además, los datos por sí solos, en principio, no tienen valor, ya que este solo se manifiesta una vez que los datos se agregan, se procesan y se usan; por lo tanto, las fuentes individuales de datos tienen un considerable valor de "opción" o potencial, lo que significa que pueden llegar a ser valiosas si a partir de esos datos se pueden abordar nuevas cuestiones. Cuanto más detallados y elaborados sean los datos, para más fines podrán utilizarse, ya que es posible filtrarlos, agregarlos y combinarlos de distintas maneras para generar diferentes conocimientos. El valor reside en el uso que se haga de ellos, por lo que dependerá en gran medida del contexto (Coyle y otros, 2020).

En general, como se explica en el capítulo III, desde un punto de vista económico, los datos pueden aportar no solo un valor privado a quienes los recopilan y controlan, sino también un valor social a toda la economía, lo que pone de manifiesto los posibles beneficios de ampliar el acceso a los datos, recopilados de forma pública o privada, con fines de interés público. Dado que los mercados no pueden garantizar por sí solos el valor social, es necesario formular políticas por motivos de eficiencia. También se necesitan políticas para asegurar la equidad, ya que la distribución de los incrementos de los ingresos privados es muy desigual.

Los datos pueden compartir algunas características con otros elementos, pero su carácter multidimensional los hace muy singulares e incomparables con esos otros elementos. Desde el punto de vista económico, los datos pueden considerarse un recurso económico, capital, un bien, trabajo e infraestructura. Sin embargo, también hay que tener en cuenta dimensiones no económicas, ya que los datos están estrechamente relacionados con la privacidad y otros derechos humanos, así como con cuestiones de seguridad nacional. En todo caso, los datos no son más que datos que, como se analizará en el capítulo III, deben abordarse desde todas sus dimensiones.

Fuente: UNCTAD.

pueden utilizarse para tomar decisiones más fundamentadas. Los datos pueden ser sobre las personas (como su grupo demográfico, sus comportamientos y sus relaciones), las organizaciones (como sus tipos, actividades y relaciones comerciales), el entorno natural, el entorno construido u objetos manufacturados. Los datos pueden utilizarse para tomar decisiones con repercusiones económicas, ambientales, sanitarias, educativas o sociales en general (Coyle y otros, 2020). Muy a menudo, en los análisis relacionados con los datos, y en los debates sobre políticas en la economía digital, se mezclan los diferentes niveles de procesamiento de los datos, aunque sus implicaciones varían significativamente. En la figura I.1 se ilustra la diferencia entre datos, información, conocimiento y sabiduría. En la pirámide se incluyen buenos usos de los datos. Teniendo en cuenta que las tecnologías no son deterministas —es decir, no son malas o buenas en sí mismas—, sino que, dependiendo del uso que se haga de ellas, el procesamiento de los datos también puede dar lugar a resultados negativos (por ejemplo, la vigilancia) con consecuencias para los procesos democráticos, se necesitan políticas adecuadas para garantizar que los datos se utilicen en beneficio de las personas y del planeta.

En el debate sobre esta cuestión se suele distinguir muy poco entre los distintos tipos de datos y sus usos. Los datos son de diversos tipos y pueden clasificarse según diferentes taxonomías (véase el capítulo III para un análisis más detallado de los tipos de datos). Es importante distinguir entre datos facilitados voluntariamente y datos observados. Por datos *facilitados voluntariamente* se entiende la información proporcionada *motu propio* por el usuario, como los datos personales compartidos en una plataforma de medios sociales o la información de una tarjeta de crédito proporcionada para realizar compras en línea. Por *datos observados* se entiende la información obtenida mediante una aplicación o un *software* de terceros, con o sin el conocimiento o consentimiento del usuario, como su ubicación o sus patrones de uso de Internet. Se extraen de las actividades en la red —por ejemplo, mediante plataformas digitales, aplicaciones, máquinas conectadas y sensores—, la mayoría de las veces de forma gratuita, y abarcan diferentes datos personales de los usuarios, como su ubicación, sus preferencias, sus relaciones y su comportamiento personal. El aumento exponencial de los datos debido a los avances de las tecnologías digitales, sobre todo del análisis de datos, corresponde sobre todo al segundo tipo de datos, por lo que una gran parte de los datos son ahora datos observados.

Es importante también distinguir entre datos estructurados y no estructurados. Los *datos estructurados* son los más fáciles de encontrar y organizar, porque suelen estar contenidos en filas y columnas, y sus

Figura I.1. La pirámide de los datos

Fuente: UNCTAD, a partir de datos de la United States Chamber of Commerce Foundation (2014).

elementos pueden asignarse a campos fijos predefinidos. Los datos estadísticos son un ejemplo de datos estructurados. Los *datos no estructurados* no pueden contenerse en una base de datos de filas y columnas, y no tienen un modelo de datos asociado. Como en el caso de los datos observados, los macrodatos son en su mayoría datos no estructurados. Se estima que el 90 % del total de los datos son datos no estructurados[3]. Conviene señalar que no es que los datos sean grandes o pequeños, sino que se pueden procesar grandes o pequeñas cantidades de ellos[4].

Asimismo, conviene distinguir entre las distintas formas de datos. En primer lugar, los *datos y la información asociados a transacciones comerciales* —como los datos de facturación, los datos bancarios, los nombres y las direcciones de entrega, entre otros— pueden circular de unos países a otros cuando esas transacciones son internacionales. Ya sea en el mundo material o en el digital, esos datos no suelen ser comercializados directamente, sino que se transfieren en el marco de las prácticas comerciales habituales y de los códigos de conducta. Se facilitan principalmente de forma voluntaria y no deberían plantear ningún problema relacionado con las políticas, siempre y cuando los nuevos actores de la economía digital operen con las reglas de la economía ordinaria.

En segundo lugar, los *datos brutos* —obtenidos a partir de actividades, productos, fenómenos o comportamientos individuales— no tienen valor en sí mismos, pero pueden generar valor una vez agregados, procesados y monetizados o cuando se utilizan con fines sociales[5]. Una definición útil del concepto de datos a los efectos del presente Informe es la siguiente: "observaciones convertidas a un formato digital que pueden ser almacenadas, transmitidas o procesadas, y de las que puede extraerse conocimiento" (Statistics Canada, 2019). Los flujos internacionales de *datos brutos*, que son un tipo de flujo diferente de otros flujos económicos internacionales, no están actualmente bien regulados a escala mundial. A falta de un sistema internacional adecuado de regulación de esos flujos de datos, son sobre todo las plataformas digitales globales (o las empresas líderes en las cadenas globales de valor), así como los Gobiernos, los que tienen acceso a los datos, pueden recopilarlos y controlarlos, tienen los recursos y la capacidad para mejorar su calidad y usarlos (o hacer un uso indebido o incorrecto de ellos), y obtienen los correspondientes beneficios. En consecuencia, son los datos brutos (en su mayoría observados y no estructurados) que se están recopilando de forma masiva gracias a los avances de las tecnologías digitales, así como el flujo de esos datos entre los países, los que están añadiendo una nueva dimensión a la labor de formulación de políticas internacionales para hacer frente a los nuevos retos conexos. Los datos brutos se sitúan en la base de la pirámide de la figura I.1.

En tercer lugar, el procesamiento de datos brutos para su transformación en inteligencia digital —en forma de estadísticas, bases de datos, conocimientos, información, etc.— genera *productos de datos*. Estos productos de datos corresponden a los niveles de información, conocimiento y sabiduría de la pirámide de la figura I.1. Pueden categorizarse como servicios y, por tanto, sus flujos transfronterizos (cuando se pagan) se incluyen en las estadísticas y normativas comerciales. No obstante, la evolución de las tecnologías relacionadas con los datos y la consiguiente expansión del comercio de nuevos productos/servicios de datos se basan principalmente en el procesamiento de datos brutos. Por consiguiente, es probable que el crecimiento de los flujos de datos transfronterizos requiera adaptaciones de las normas existentes sobre el comercio de servicios.

[3] Véase *Forbes*, 18 de octubre de 2019, "What's The Difference Between Structured, Semi-Structured And Unstructured Data?"; y *Forbes*, 16 de octubre de 2019, "What Is Unstructured Data And Why Is It So Important To Businesses? An Easy Explanation For Anyone".

[4] Parece haber cierta confusión en la literatura y en los debates al respecto con el término "revolución de los datos", que a veces se refiere a la necesidad de mejorar los datos estadísticos y reforzar las capacidades estadísticas, y otras veces se entiende como la revolución tecnológica digital asociada a los "macrodatos" o "inteligencia de datos" y al análisis de datos.

[5] Algunos observadores consideran que todos los datos son producto de un determinado contexto o mecanismo social, y que por ello no pueden calificarse realmente de brutos. Si bien se reconoce esa dimensión sociológica, en el presente Informe se entiende por "dato bruto" un dato que no se ha procesado, en el sentido de que no se le ha añadido ningún valor económico (véase, por ejemplo, Cattaruzza (2019)).

C. LA BRECHA DIGITAL EN EL ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y EN SU USO

Un breve repaso de la situación actual —sumamente desigual— de la economía digital impulsada por los datos es un buen punto de partida para comprender mejor los posibles efectos de los flujos de datos transfronterizos en el desarrollo. Con el fin de participar en dicha economía y beneficiarse de ella, los países necesitan poder acceder a las tecnologías de las comunicaciones necesarias para la transmisión de datos. También han de tener los medios para hacer un uso productivo de dicho acceso. Todavía existen importantes diferencias, entre países y a escala nacional, en cuanto a la capacidad de conexión a Internet y de utilizarla. Tratar de acabar con esas diferencias en la economía digital es fundamental para el desarrollo. En esta sección se analizan las distintas tendencias en cuanto a la conectividad móvil, el tipo de conexión, la adopción de teléfonos inteligentes, la asequibilidad y el uso de Internet. No obstante, la brecha digital es consecuencia de una situación más amplia de diferencias de ingresos entre países y a escala nacional. Por consiguiente, no bastará con actuar únicamente en el terreno de las infraestructuras de las TIC; también es importante abordar el problema de la desigualdad global mediante las políticas económicas.

1. Telefonía y acceso de banda ancha

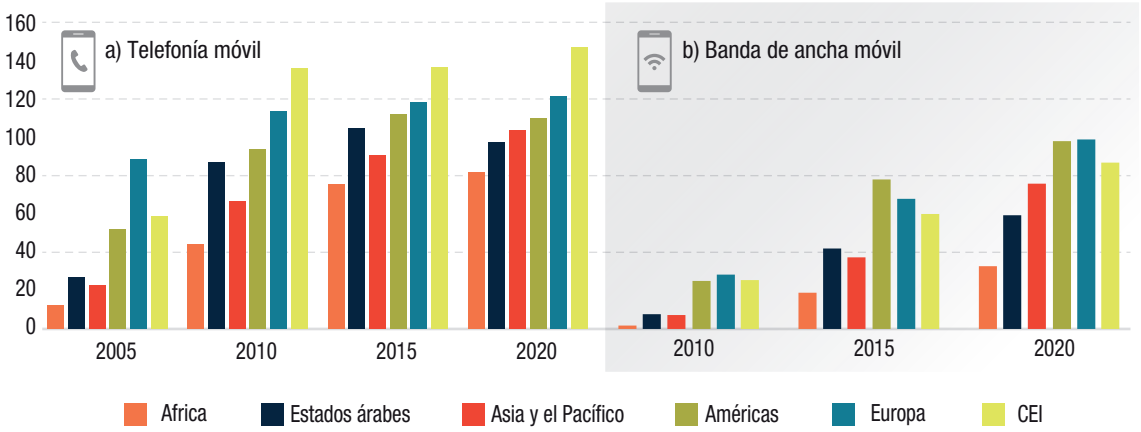
La telefonía fija ha disminuido en los últimos 15 años tanto en las economías desarrolladas como en las economías en desarrollo, mientras que en los países menos adelantados (PMA) nunca ha llegado a ser una tecnología de uso generalizado. En cuanto a las suscripciones de banda ancha fija, la tasa de penetración ha aumentado en las economías desarrolladas y en los países en desarrollo. En los PMA, sin embargo, el número medio de suscripciones por cada 100 personas fue prácticamente nulo en el período 2005-2020, ya que esos países han pasado directamente a tener una conectividad móvil cada vez más eficiente y accesible. Aunque las tasas de penetración de la telefonía móvil en 2020 seguían siendo más altas en los países desarrollados que en los países en desarrollo, sobre todo los PMA, el segundo grupo experimentó un mayor crecimiento en el período referido, lo que contribuyó a reducir la diferencia. En el plano regional, en 2020 la mayor tasa de suscripciones de telefonía móvil se registró en las economías en transición, seguidas de Europa y las Américas. Las tasas de penetración fueron más bajas en Asia y el Pacífico, los Estados árabes y África. Sin embargo, estas últimas regiones, en las que se concentra la mayoría de los países en desarrollo y PMA, registraron los aumentos más espectaculares en el período 2005-2020 (figura I.2a)[6].

Desde 2010, las tasas de penetración de la banda ancha móvil han aumentado considerablemente en todos los grupos de países clasificados por grado de desarrollo. No obstante, más de un decenio después siguen existiendo grandes diferencias: la tasa de penetración en los países desarrollados duplica la de los países en desarrollo, y cuadruplica la de los PMA. A escala regional, el número de suscripciones de banda ancha móvil es inferior al de las de telefonía móvil (figura I.2b). El crecimiento más significativo de la tasa de suscripciones de banda ancha móvil se produjo en África, Asia y el Pacífico y los Estados árabes, ya que todas esas regiones partían de unos valores muy bajos en 2010. En el caso de África, la tasa de penetración de la banda ancha móvil en 2020 era casi 20 veces mayor que en 2010. Si bien esto redujo las diferencias entre los países en desarrollo y los más avanzados en relación con la banda ancha móvil, sigue existiendo una importante brecha en esa tecnología. En Europa y las Américas (incluidos el Canadá y los Estados Unidos), las tasas de penetración en 2020 llegaron a casi 100 suscripciones por cada 100 personas. En las economías en transición de la Comunidad de Estados Independientes (CEI) se alcanzaron valores relativamente similares, pero las tasas de penetración de la banda ancha móvil en Asia y el Pacífico, los Estados árabes y África representaron, respectivamente, tres cuartas partes, menos de dos tercios y solo un tercio de las americanas y europeas. En 2019, la tasa de penetración de la banda ancha móvil en América Latina se estimó en un 73 % (ECLAC, 2021)[7].

[6] Todos los datos de las bases de datos estadísticos en línea utilizados en las figuras y cuadros de este capítulo se actualizaron por última vez en junio de 2021, a menos que se indique otra cosa.

[7] Se indican las estimaciones de la CEPAL solamente para América Latina, ya que en los datos de la UIT se incluye a América Latina en la región de las Américas, junto con el Canadá y los Estados Unidos.

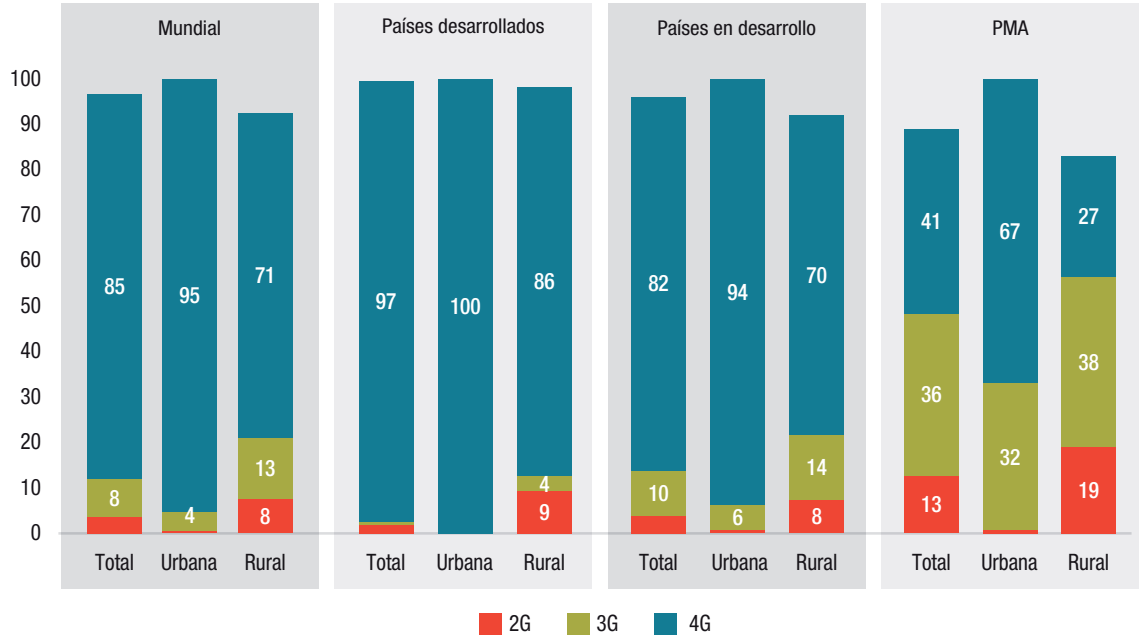
Figura I.2. Suscripciones de telefonía móvil y banda ancha móvil, por región, en años seleccionados
(Por cada 100 personas)



Fuente: UNCTAD, a partir de la base de datos estadísticos de la UIT, que puede consultarse en https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
Notas: Los grupos de países son los establecidos por la fuente. Los datos relativos a 2020 son estimaciones de la UIT.

La brecha existente en el acceso a la banda ancha móvil se debe a, entre otras cosas, las diferencias en las tecnologías de conexión de banda ancha móvil (3G, 4G y ahora 5G) y la adopción de teléfonos inteligentes, así como la asequibilidad de los teléfonos con acceso a Internet y de los planes de datos móviles. En 2020 el 93 % de la población mundial tenía como mínimo cobertura de red de banda ancha móvil 3G (figura I.3). La red 5G no se empezó a implementar de forma efectiva hasta 2020. Como se

Figura I.3. Distribución de la cobertura de cada tipo de red móvil, en zonas rurales y urbanas, por grado de desarrollo, 2020
(Porcentaje de la población)



Fuente: UNCTAD, cálculos a partir de la base de datos estadísticos de la UIT, que puede consultarse en https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
Notas: El valor correspondiente a las redes 2G y 3G indica el porcentaje incremental de la población que no está cubierta por una red de tecnología más avanzada (ejemplo: en el caso de los PMA (total), el 41+36+13=90 % de la población está cubierta por una red 2G, el 41+36=77 % está cubierta por una red 3G y el 41 % está cubierta por una red 4G). Los grupos de países son los establecidos por la fuente. Los datos son estimaciones de la UIT.

explica más adelante, se espera que las conexiones 5G ocupen un lugar central en la economía digital impulsada por los datos, a medida que se disponga de más y más datos. En 2020, el porcentaje de la población que tenía como mínimo cobertura de red 3G era del 98 % en los países desarrollados, mientras que en los países en desarrollo y en los PMA era del 92 % y el 77 %, respectivamente. Por consiguiente, en los PMA, el 23 % de la población no tenía acceso a una red de banda ancha móvil en 2020, lo que queda muy lejos de la meta 9.c de los Objetivos de Desarrollo Sostenible de las Naciones Unidas de aumentar el acceso a las TIC y esforzarse por proporcionar acceso universal y asequible a Internet en los PMA de aquí a 2020 (indicador 9.c.1: Proporción de la población con cobertura de red móvil, desglosada por tecnología). Como se ha señalado anteriormente, el porcentaje de la población con una suscripción de banda ancha móvil es aún menor, sobre todo en África, donde están la mayoría de los PMA.

La brecha tecnológica también se observa entre la población urbana y la población rural de cada grupo de países. Es más acentuada en los PMA, donde el 16 % de la población rural no tenía acceso a ninguna red móvil y el 35 % no podía conectarse a Internet con un dispositivo móvil (figura I.3)[8]. Con todo, esas cifras ilustran una mejora significativa desde 2015, cuando hasta el 63 % de la población rural de los PMA carecía de acceso a Internet a través de un dispositivo móvil.

2. Adopción de teléfonos inteligentes y asequibilidad del acceso móvil a Internet

a) Adopción de teléfonos inteligentes

Los teléfonos inteligentes son una herramienta clave para acceder a Internet y transferir datos, especialmente en la mayoría de los países en desarrollo, donde la conexión de banda ancha fija y el uso de computadoras están menos extendidos. Las tasas de adopción de teléfonos inteligentes, entendidas como la proporción de teléfonos inteligentes con cualquiera de las conexiones móviles, aumentaron en todas las regiones en el período 2016-2019 (figura I.4). No obstante, en 2019 seguían existiendo diferencias entre las regiones. América del Norte y Europa registraron las mayores tasas de adopción de teléfonos inteligentes, por delante de China. África Subsahariana fue la región con la menor tasa de adopción de teléfonos inteligentes, aunque se prevé que sea la que experimente el mayor crecimiento de aquí a 2025. La tendencia de crecimiento de la adopción de teléfonos inteligentes se está produciendo al mismo tiempo que los teléfonos inteligentes y los planes de datos se vuelven más asequibles, como se analiza a continuación.

b) Asequibilidad de los teléfonos inteligentes y de los planes de datos móviles

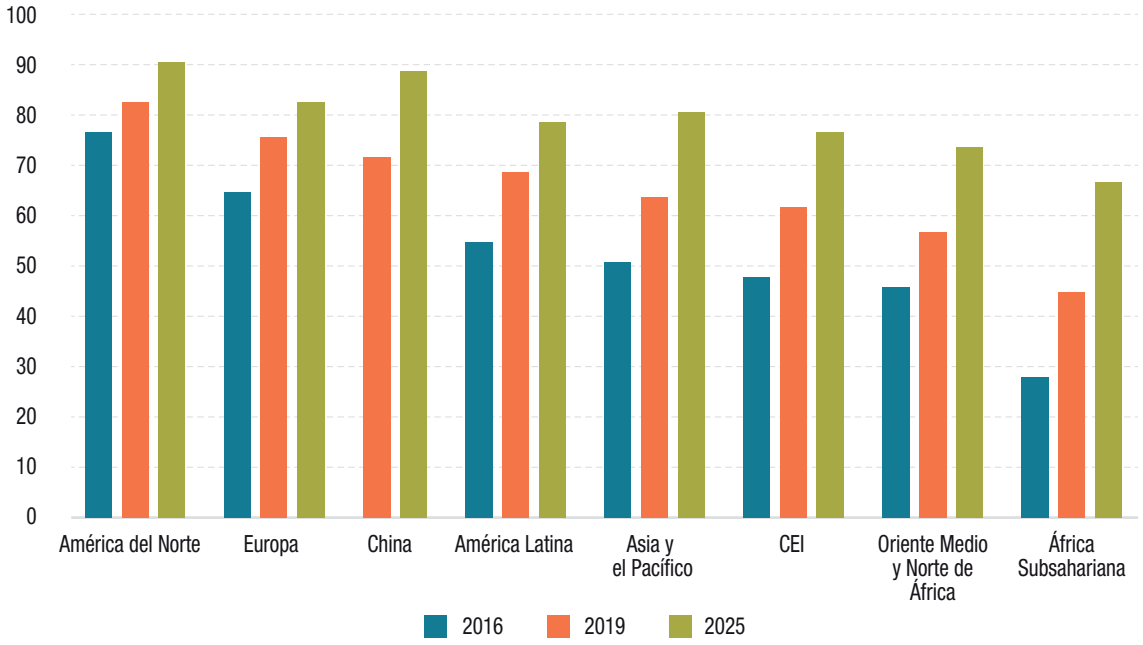
En los países en desarrollo, el costo de los teléfonos inteligentes constituye un obstáculo para conectarse a Internet y beneficiarse plenamente de la economía digital impulsada por los datos. GSMA (2020b) evaluó la asequibilidad del teléfono básico con acceso a Internet o del teléfono inteligente más barato en diferentes regiones. En 2019, su costo representaba en promedio el 4 % del producto interno bruto (PIB) mensual per cápita en los países de ingreso alto. En países con menores ingresos per cápita, ese porcentaje era más del doble (9 %) en América Latina y el Caribe y llegaba al 30 % en África Subsahariana. Ahora bien, adquirir un teléfono básico con acceso a Internet o un teléfono inteligente no implica tener automáticamente acceso a Internet, para lo cual es necesario también contratar un plan de datos móviles.

Los planes de datos móviles son esenciales para sacar el máximo partido a los dispositivos móviles[9] y reducir la brecha existente entre los países desarrollados y los países en desarrollo con el fin de que puedan mantenerse conectados a un precio justo. La meta 2 de la Comisión sobre la Banda Ancha para el Desarrollo Sostenible establece que, para 2025, los servicios básicos de banda ancha deben ser asequibles en los

[8] El porcentaje de la población rural sin acceso a una red móvil se obtiene de la diferencia entre el 100 % de la población rural y la suma de los porcentajes de la población rural con cada uno de los tres tipos de tecnología (84 %). El porcentaje de la población rural que no podía conectarse a Internet con un dispositivo móvil resulta de la diferencia entre el 100 % de la población rural y la suma de los porcentajes de la población rural con cobertura 3G y 4G (65 %).

[9] En este contexto, el término datos tiene que ver con la capacidad de transmitir información convertida en ceros y unos, es decir, los *bytes* que se pueden utilizar.

Figura I.4. Adopción de teléfonos inteligentes, por región, en años seleccionados
(Porcentaje)



Fuente: UNCTAD, a partir de GSMA (2017) y GSMA (2020a).
Notas: Los grupos de países son los establecidos por la fuente. Los datos correspondientes a 2025 son previsiones.

países en desarrollo, con un costo inferior al 2 % del ingreso nacional bruto (INB) mensual per cápita[10]. En 2019, 95 países cumplían el objetivo de poderse acceder a 1,5 *gigabytes* (GB) de banda ancha móvil por un precio inferior al 2 % del INB mensual per cápita: 47 países desarrollados, 44 países en desarrollo y 4 PMA (figura I.5). La UIT y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) señalaron en su informe sobre el estado de la banda ancha que, si bien los precios de los planes de datos a escala mundial disminuyeron entre 2013 y 2019 (-15 % de media anual), "en al menos 40 países, principalmente PMA, los servicios básicos de banda ancha móvil cuestan el 5 % o más del INB mensual medio per cápita. En 19 de esos países, el costo medio alcanza valores alarmantes que superan el 10 % y el 20 %" (ITU y UNESCO, 2020:16).

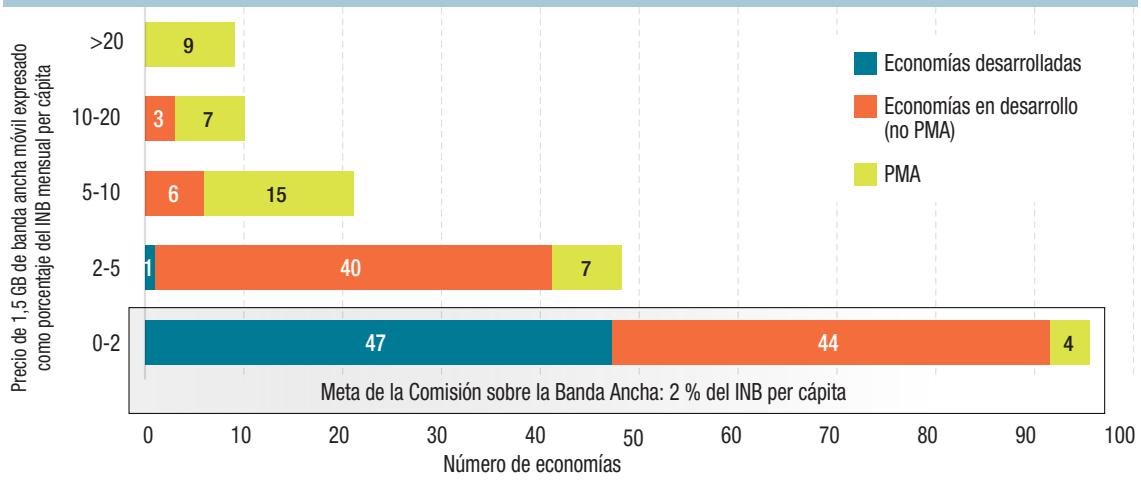
3. Velocidad de la conexión a Internet

La velocidad de las conexiones a Internet es un factor clave para determinar la capacidad de generar tráfico de datos y utilizarlo. La calidad de la conexión es importante, ya que la tecnología y el uso de Internet han evolucionado muy rápidamente en los últimos 20 años. Algunas velocidades medias de conexión pueden ser suficientes para actividades básicas como la navegación por Internet o el correo electrónico, pero no para otras, como las videollamadas.

En 2020, la velocidad de la conexión a Internet de banda ancha *fija* era, en promedio, superior a la de la conexión a Internet de banda ancha *móvil* en todos los grupos de economías, excepto en los PMA (figura I.6). La diferencia era menos acentuada en las economías en desarrollo y en transición, pero en las economías desarrolladas la velocidad media de la conexión fija era hasta el doble de la de la conexión móvil. Hay una gran diferencia entre la calidad de la conexión a Internet en las economías desarrolladas y en el resto de las economías. En lo que respecta a la conexión de banda ancha fija, la velocidad media observada en las economías desarrolladas era casi ocho veces superior a la de los PMA, lo que pone de manifiesto las carencias en materia de infraestructuras y tecnología (por ejemplo, en el desarrollo de la fibra óptica).

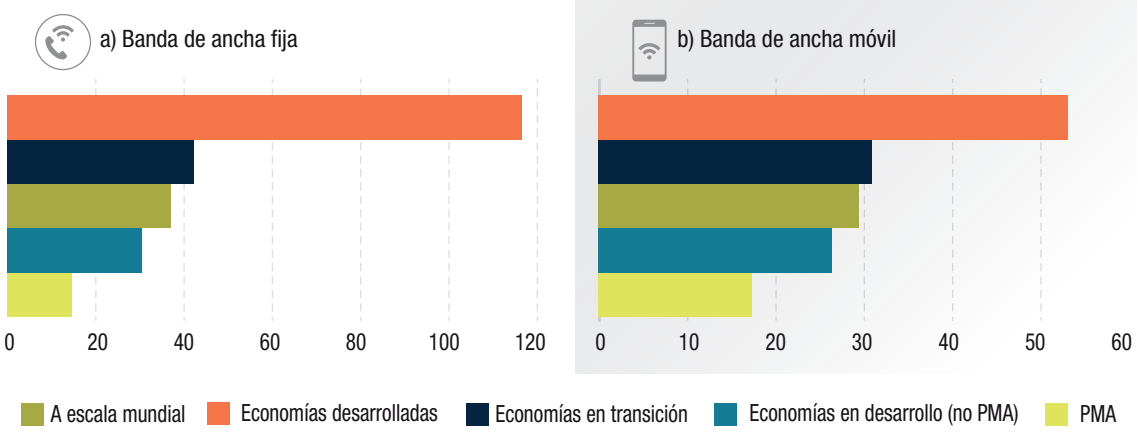
[10] En 2018, la Comisión sobre la Banda Ancha para el Desarrollo Sostenible puso en marcha las Metas para 2025 con el fin de "Conectar a la otra mitad" de la población mundial (véase www.broadbandcommission.org/broadband-targets/).

Figura I.5. Precio de 1,5 GB de banda ancha móvil expresado como porcentaje del INB per cápita, 2019
(Número de economías)



Fuente: UNCTAD, a partir de ITU y UNESCO (2020).

Figura I.6. Velocidades de conexión de banda ancha a Internet, a escala mundial y por grado de desarrollo, 2020
(Megabits por segundo)



Fuente: UNCTAD, cálculos basados en el Speedtest Global Index (Índice Global de Velocidad de Internet), de Ookla, disponible en https://www.speedtest.net/global-index (consultado en abril de 2021).
Notas: Los valores a escala mundial y para cada grupo se han obtenido a partir de la mediana de las velocidades medias ses del grupo en cuestión.

La diferencia entre las economías desarrolladas y el resto de las economías en cuanto a velocidad de la conexión de banda ancha móvil es menor. La puesta en marcha de la banda ancha móvil parece ser más beneficiosa para las economías en desarrollo y en transición, dado su costo y las capacidades técnicas que se requieren. Se podría decir, por tanto, que el camino para los PMA debería ser priorizar el desarrollo del acceso a la banda ancha móvil, que permite una mayor velocidad media de conexión a Internet. No obstante, aunque las tecnologías 3G y 4G parezcan suficientes hoy en día, puede que no lo sean para ejecutar adecuadamente las aplicaciones del futuro. Por consiguiente, sería aconsejable que los países con infraestructuras de banda ancha móvil en ciernes se saltaran directamente las etapas correspondientes a las tecnologías más antiguas y se centraran en la implantación de la tecnología 5G, cuando tengan la financiación y las capacidades técnicas necesarias.

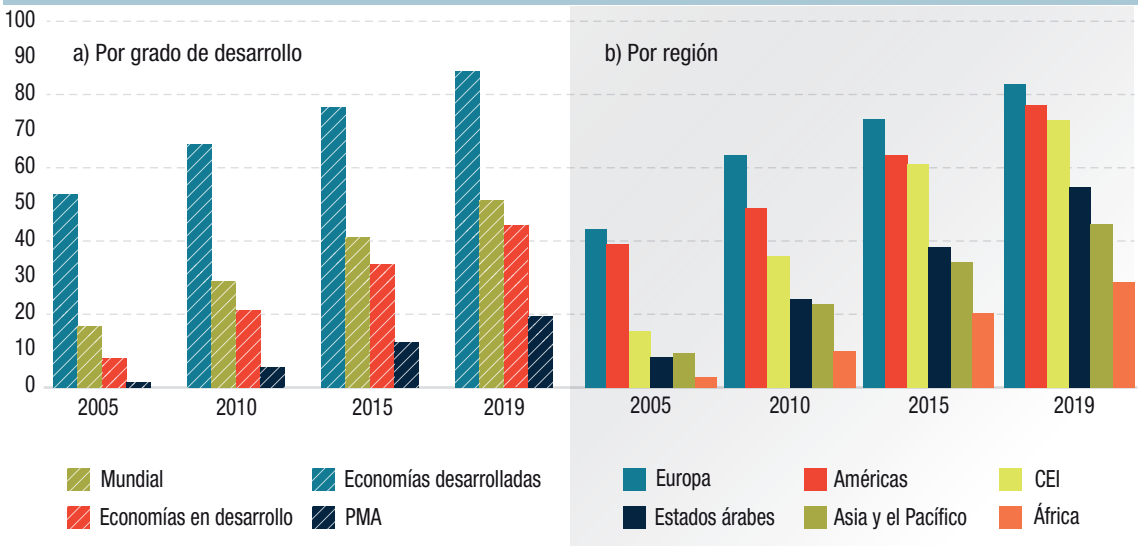
4. Uso de Internet

La implementación de la conectividad fija y móvil, el abaratamiento de los planes de datos, el mayor uso de los dispositivos móviles (teléfonos básicos, teléfonos inteligentes y tabletas) y las conexiones a Internet más rápidas han contribuido a que Internet se use cada vez más (figura I.7). En 2019, más de la mitad de la población mundial utilizaba Internet, lo que supone un aumento considerable frente a poco más de la décima parte de la población que lo usaba a principios de la década de 2000. No obstante, el porcentaje de internautas en los países en desarrollo (44 %) y en los PMA (20 %) es todavía mucho menor que en los países desarrollados. Esta brecha sigue siendo un gran motivo de preocupación para la comunidad internacional. La meta 3 de la Comisión sobre la Banda Ancha para el Desarrollo Sostenible establece que, en 2025, la tasa de penetración de Internet de banda ancha (o tasa de personas usuarias de Internet) debería alcanzar el 75 % a escala mundial, el 65 % en los países en desarrollo y el 35 % en los PMA. "Las previsiones basadas en las proyecciones de crecimiento actuales indican que la tasa de penetración de Internet a escala mundial podría alcanzar solo el 70 % en 2025 [...], y el 31 % en los PMA" (ITU y UNESCO, 2020:21).

Desde una perspectiva regional, Europa y la región de las Américas (que incluye los Estados Unidos, el Canadá y América Latina y el Caribe) han llevado la delantera en el uso de Internet en los últimos 15 años. En cambio, aunque en otras zonas (sobre todo África y los Estados árabes) el uso de Internet aumentó considerablemente, al final del período seguía siendo mucho menor. Quedaba rezagada en particular África, donde en 2019 menos del 30 % de la población utilizaba Internet. El uso de Internet en América Latina era del 67 % (ECLAC, 2021).

En lo que respecta al desarrollo económico, también es relevante saber cuáles son los tipos de actividades en los que se utiliza Internet. Por ejemplo, la participación en las redes sociales es menos productiva para la economía que la compra o venta de bienes a través de Internet (el comercio electrónico se aborda en la siguiente subsección). En el cuadro I.1 se indican las actividades que realizan las personas a través de Internet. El uso de la banca por Internet es mucho mayor en las economías desarrolladas que en las economías en desarrollo o en transición, aunque entre estas últimas, Asia está a la cabeza con diferencia. Lo mismo ocurre con la compra o el pedido de bienes o servicios. La participación en los medios sociales es elevada en todas las regiones consideradas, y es mayor en las economías en desarrollo que en las economías desarrolladas y en las economías en transición.

Figura I.7. Uso de Internet, en el mundo, por grado de desarrollo y por región, en años seleccionados
(Porcentaje)



Fuente: UNCTAD, a partir de la base de datos estadísticos de la UIT, que puede consultarse en https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
Nota: Los grupos de países son los establecidos por la fuente.

Cuadro I.1. Actividades realizadas por particulares a través de Internet, por grado de desarrollo y por región
(Porcentaje)

Actividad realizada en Internet	Economías desarrolladas	Economías en transición	Economías en desarrollo (África)	Economías en desarrollo (Asia)	Economías en desarrollo (América Latina y el Caribe)
Banca por Internet	62,3	14,9	9,8	34,8	11,6
Enviar o recibir correo electrónico	84,9	44,8	46,6	59,7	52,4
Hacer llamadas (llamar por teléfono a través de Internet/Voz sobre protocolo de Internet, utilizando Skype, iTalk, etc.)	56,9	71,0	47,6	63,2	73,4
Leer o descargar periódicos o revistas en línea o libros electrónicos	76,4	41,5	38,6	46,0	30,3
Obtener información sobre bienes o servicios	83,9	50,9	30,6	68,0	51,8
Obtener información de entidades de la administración pública	55,1	11,1	17,6	20,9	23,2
Contactar con entidades de la administración pública	54,5	5,7	12,1	25,6	10,7
Comprar o solicitar bienes o servicios	53,9	18,2	14,6	29,1	13,1
Buscar información sobre la salud (lesiones, enfermedades, nutrición, etc.)	62,4	37,5	24,3	47,1	41,1
Concertar una cita con un profesional de la salud a través de un sitio web	16,4	3,9	4,0	7,6	3,1
Participar en redes sociales	70,4	70,7	86,3	87,2	79,0
Acceder a sitios web de chat, blogs, grupos de noticias o debates en línea o publicar opiniones en ellos	13,9	11,6	45,1	26,5	26,0
Vender bienes o servicios	16,8	7,0	3,5	6,4	9,3
Contratar servicios relacionados con viajes o alojamientos	55,0	5,7	7,5	25,2	28,4
Hacer un curso oficial en línea	8,1	4,5	17,5	15,9	28,5
Consultar wikis, enciclopedias en línea u otros sitios web con fines de aprendizaje formal	23,8	14,6	17,2	13,2	31,4
Escuchar la radio por Internet	61,2	17,0	13,3	20,9	11,2
Ver la televisión por Internet	41,1	8,8	30,2	33,1	18,1
Reproducir o descargar imágenes, películas, vídeos o música, jugar a juegos o descargarlos	57,4	52,9	64,2	66,4	50,8
Descargar *software* o aplicaciones	19,0	5,5	62,8	41,0	20,7
Buscar ofertas de empleo o enviar una solicitud de empleo	17,4	9,8	14,3	19,9	16,6
Participar en redes profesionales	21,0	3,6	5,9	6,4	0,7
Subir a un sitio web contenidos de creación propia para compartirlos	38,8	33,4	12,7	21,3	35,6
Participar en consultas o votaciones en línea sobre cuestiones cívicas o políticas	9,8	3,5	5,5	8,1	N/A
Utilizar espacio de almacenamiento en Internet para guardar documentos, imágenes, música, vídeo u otro tipo de archivos	38,7	15,0	17,5	20,8	21,7
Utilizar programas informáticos ejecutados en línea para editar documentos de texto, hojas de cálculo o presentaciones	28,0	4,3	6,1	11,7	4,8

Fuente: UNCTAD, cálculos a partir de la base de datos Indicadores de las telecomunicaciones/TIC mundiales de la UIT.
Notas: Los grupos de países son los establecidos por la fuente. Los valores para cada grupo de países se obtienen de la mediana de los valores medios en todos los países del grupo para los que se dispone de datos en el último año, que varía entre 2015 y 2019.

5. Uso del comercio electrónico

El tipo de actividades que realizan las personas que utilizan Internet varía considerablemente. Mientras que el porcentaje de internautas que compran por Internet en algunos países europeos supera el 80 %, en muchos PMA es menos del 10 % (UNCTAD, 2021c). En Rwanda, por ejemplo, en 2017 solo el 9 % de los internautas utilizó Internet para comprar algo en línea. La evolución del comercio electrónico depende en gran medida de la capacidad o la preparación de un país para participar en la economía digital y beneficiarse de ella. El índice de comercio electrónico de empresa a consumidor (B2C) de la UNCTAD, obtenido como el promedio de cuatro indicadores, muestra las diferencias existentes entre los países. En el cuadro I.2 figuran los valores de dicho índice correspondientes a 2020 en cada región. Los puntos fuertes y débiles relativos son, en general, diferentes. En el caso de Asia Oriental, Meridional y Sudoriental, el único indicador que está por debajo del promedio mundial es el de uso de Internet. En América Latina y el Caribe, las principales oportunidades de mejora tienen que ver con la fiabilidad postal. Para que el comercio electrónico sea más inclusivo, los países africanos deberían mejorar en todos los aspectos cubiertos por el índice.

6. Brechas digitales de género

Si bien hasta aquí nos hemos centrado en la brecha digital entre los países, dentro de cada país la brecha digital de género es muy visible, tanto en lo que respecta a la adquisición de teléfonos inteligentes como al uso de Internet.

a) Brecha de género en la adquisición de teléfonos inteligentes

Según un estudio realizado en 2018 sobre el número de personas con teléfono inteligente a partir de una muestra de personas de ambos sexos de países desarrollados y de países en desarrollo (Pew Research Center (2019)), en promedio, hay menos personas, tanto mujeres como hombres, con teléfonos inteligentes en los países en desarrollo que en los países desarrollados (48 % y 71 % de mujeres con teléfono inteligente, 52 % y 80 % de hombres con teléfono inteligente, respectivamente). La brecha de género, entendida como la diferencia entre la tasa de adquisición de teléfonos inteligentes correspondiente a los hombres y la correspondiente a las mujeres, dividida por la primera, era en promedio mayor en las economías en desarrollo que en las desarrolladas. Sin embargo, entre 2015 y 2018 la brecha de género media disminuyó. La mayor brecha de género en 2018 se registró en la India (56 %) y la menor en Filipinas (-9,6 %), donde había más mujeres que hombres con teléfonos inteligentes.

Cuadro I.2. Índice de comercio electrónico B2C, por región, 2020

Grupos, por región y grado de desarrollo	Porcentaje de particulares que usan Internet (2019 o últimos datos disponibles)	Porcentaje de particulares con una cuenta bancaria (>15 años, 2017)	Servidores de Internet seguros (valor normalizado, 2019)	Indicador de fiabilidad postal de la UPU (2019 o últimos datos disponibles)	Valor del índice en 2020	Valor del índice en 2019 (datos de 2018)
África	30	40	28	21	30	31
Asia Oriental, Meridional y Sudoriental	57	60	54	58	57	58
América Latina y el Caribe	64	53	50	29	49	48
Asia Occidental	77	58	45	50	58	59
Economías en transición	71	58	60	59	62	63
Economías desarrolladas	88	93	84	80	86	87
A escala mundial	60	60	53	47	55	55

Fuente: UNCTAD (2021c).

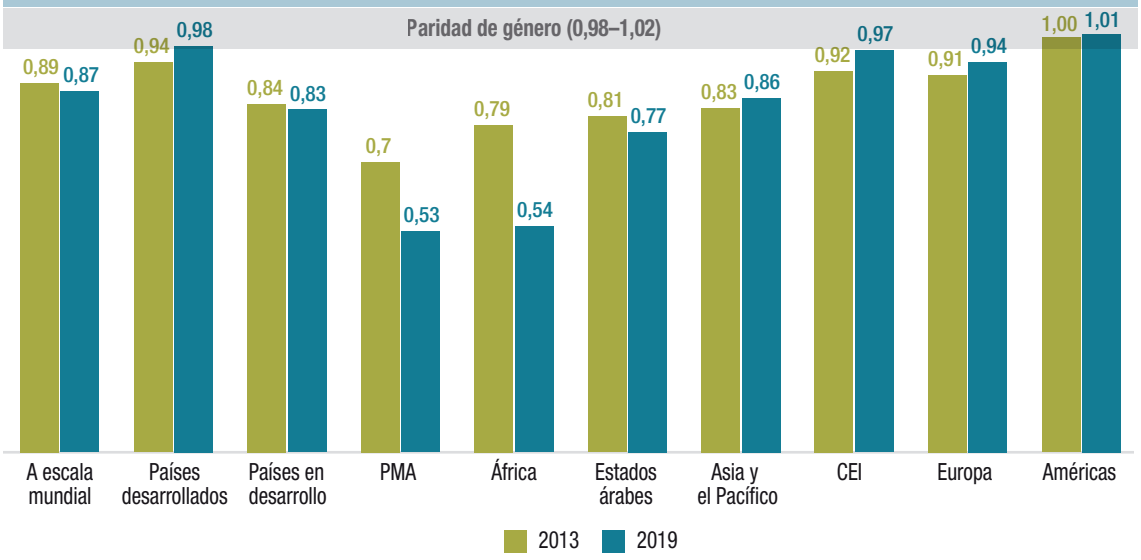
b) *Brecha de género en el uso de Internet*

Según los cálculos realizados por la UIT (ITU, 2020), a nivel mundial, el porcentaje de población masculina y femenina que en 2019 usaba Internet era del 55 % y el 48 %, respectivamente, es decir, que el indicador de paridad de género era 0,87 (figura I.8), mientras que la paridad entre los géneros se alcanza cuando es 1. El indicador de paridad de género se calcula dividiendo el porcentaje de las mujeres que usan Internet por el correspondiente a los hombres[11]. A escala mundial, el indicador disminuyó ligeramente entre 2013 y 2019. Aumentó en Asia y el Pacífico, la CEI, Europa y las Américas. Sin embargo, disminuyó en los Estados árabes, y sobre todo en África (de 0,79 a 0,54). Asimismo, mientras que aumentó en los países desarrollados, disminuyó ligeramente en los países en desarrollo, y de forma significativa en los PMA (de 0,70 a 0,53).

La pandemia de COVID-19 puso de manifiesto todas las brechas de conectividad a Internet y de su uso comentadas anteriormente. Dado que ante las medidas de confinamiento decretadas a causa de la pandemia la gente tuvo que conectarse más a Internet para poder continuar sus actividades, los países y sectores más rezagados en cuanto a conectividad encontraron mayores dificultades para salir adelante. Aunque en 2020 se produjo un auge del comercio electrónico en todo el mundo, numerosas pequeñas empresas de los países en desarrollo tuvieron dificultades para pasarse a la tecnología digital y atender la creciente demanda de ventas en línea[12].

Tradicionalmente, las enormes brechas aún existentes entre países y a escala nacional en materia de conectividad, acceso, asequibilidad y disponibilidad de las TIC han ocupado un lugar destacado en los análisis y las políticas. En adelante será cada vez más importante reducir esas brechas para que los países en desarrollo, y en particular los PMA, puedan avanzar en la economía digital en favor del desarrollo. A medida que se digitalizan más aspectos de la vida y actividades, y los datos van cobrando cada vez más importancia como recurso clave para el desarrollo, aparecen nuevas brechas digitales relacionadas con la capacidad de acceso a los datos y de transferencia de los mismos. En las siguientes secciones se examina la evolución mundial del tráfico de Internet y de datos, así como las brechas que están surgiendo en relación con la recopilación, la transmisión y el uso de los datos.

Figura I.8. Indicador de paridad de género en el uso de Internet, por grado de desarrollo y por región, 2013 y 2019



Fuente: UNCTAD, a partir de información de la UIT (ITU, 2020).
Nota: Los grupos de países son los establecidos por la fuente.

[11] Un valor inferior a 1 indica que hay más hombres que usan Internet que mujeres, mientras que un valor superior a 1 indica lo contrario.

[12] En UNCTAD (2021a) se puede consultar un análisis a escala mundial sobre la COVID-19 y el comercio electrónico.

D. EVOLUCIÓN MUNDIAL DEL TRÁFICO DE INTERNET Y DE DATOS

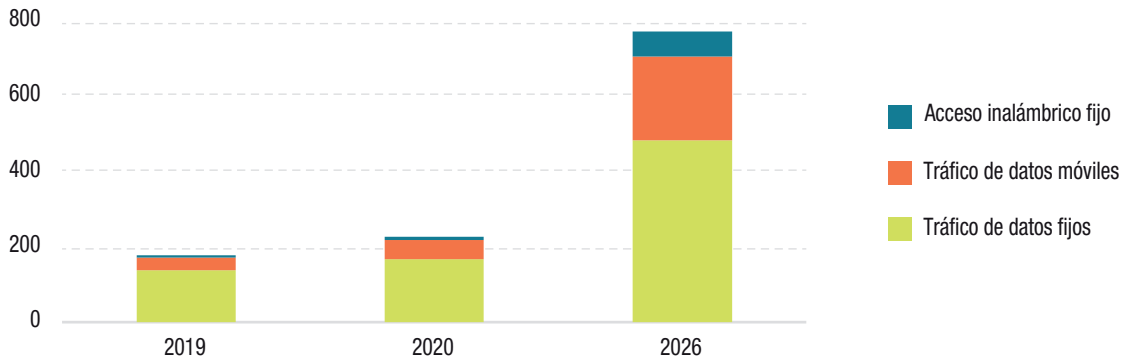
Los datos digitales e Internet son cada vez más importantes para las economías y las sociedades. Su crecimiento, dado por el tráfico mediante el protocolo Internet (tráfico IP), se estima a partir de datos estadísticos del sector privado amparados por un derecho de propiedad intelectual, ya que no existen estadísticas oficiales de los países al respecto. Las metodologías utilizadas no están estandarizadas ni son del todo claras, y los datos no siempre se publican con regularidad. En consecuencia, no resulta fácil analizar la evolución mundial del tráfico de Internet y de datos. No obstante, todas las estimaciones indican que se ha disparado en los últimos decenios, y se espera que siga creciendo a un ritmo vertiginoso debido al rápido progreso de las tecnologías digitales.

Los datos más actualizados sobre el tráfico IP a escala mundial parecen ser los ya presentados en UNCTAD (2019a)[13], a saber: se espera que el tráfico IP aumente más del triple entre 2017 y 2022. La mayor parte del tráfico de Internet tiene lugar en las regiones de Asia y el Pacífico y de América del Norte, mientras que en América Latina y la región de Oriente Medio y Norte de África se genera un pequeño porcentaje. Según una previsión, se espera que el tráfico IP a escala mundial supere en 2022 todo el tráfico de Internet hasta 2016[14]. Además, el número de dispositivos conectados a redes IP será más de tres veces la población mundial en 2023 (Cisco, 2020).

La pandemia de COVID-19 tuvo un inmenso impacto en el tráfico de Internet, debido a que la mayoría de las actividades pasaron a realizarse cada vez más en línea. En gran parte como consecuencia de la pandemia, el uso de ancho de banda de Internet a escala mundial aumentó un 35 % en 2020, lo que supuso un incremento sustancial respecto al 26 % del año anterior y representó el mayor aumento anual desde 2013. Pese a que a partir de marzo de 2020 se disparó el volumen de tráfico y se modificaron las tendencias del mismo, se ha demostrado que Internet ha resistido extraordinariamente a los cambios repentinos asociados a la pandemia. Son muchos los operadores de redes que han acelerado sus planes de ampliación de capacidad para adelantarse a la demanda (TeleGeography, 2021a).

Según Ericsson (2020), el tráfico de datos de redes móviles aumentó un 50 % entre el tercer trimestre (Q3) de 2019 y el Q3 de 2020. El tráfico mundial de datos alcanzó 180 y 230 *exabytes* mensuales en 2019 y 2020, respectivamente (figura I.9). Para 2026, se prevé que ese volumen aumente más del triple y llegue a 780 *exabytes* mensuales. El tráfico de datos fijos representó casi tres cuartas partes de todo el tráfico de datos en 2019. Sin embargo, con el creciente número de dispositivos móviles y el auge de la Internet de las cosas, se espera que el tráfico de datos de banda ancha móvil crezca más rápido y llegue a ser en 2026 casi un tercio del volumen total de datos.

Figura I.9. Tráfico mundial de datos, en años seleccionados
(*Exabytes* por mes)



Fuente: UNCTAD, a partir de Ericsson (2020).

[13] Los análisis que aparecen en UNCTAD (2019a) se basaron en Cisco (2018). Parece que Cisco ya no publica esas previsiones y tendencias, sino un Informe Anual de Internet (Cisco, 2020), que no incluye datos estadísticos sobre el tráfico IP.

[14] Véase Cisco, 27 de noviembre de 2018, "Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet".

Según otras estimaciones, en 2020 se crearon o copiaron 64,2 *zettabytes* de datos, pese a que la pandemia ejerció una presión sistémica a la baja en muchos sectores, y sus repercusiones persistirán durante varios años. Se calcula que la cantidad de datos digitales creados en los próximos cinco años será más del doble de la cantidad creada desde la aparición del almacenamiento digital. La creación y la copia de datos a escala mundial aumentarán a una tasa de crecimiento anual compuesta del 23 % según las previsiones para el período 2020-2025 (IDC, 2021a).

E. ESTIMACIONES DEL VALOR DE LOS DATOS Y DE LOS MERCADOS DE DATOS

Medir el valor de los datos sigue siendo una tarea tremendamente difícil. El concepto de "cadena de valor de los datos" es fundamental para hacer una estimación del valor de los datos. El valor se genera en el proceso de transformación de los datos brutos —desde la recopilación de los datos, pasando por el procesamiento y el análisis, hasta convertirlos en inteligencia digital— que pueden monetizarse con fines comerciales o utilizarse para objetivos sociales (UNCTAD, 2019a). Los datos por sí solos no tienen valor si no se agregan y procesan. Y no puede haber inteligencia digital si no hay datos brutos. Para la creación y captura de valor, se necesitan tanto los datos brutos como las capacidades para procesarlos y convertirlos en inteligencia digital.

A priori, si no se sabe cómo se van a utilizar los datos, no se puede estimar el valor de los datos brutos. Sin embargo, sí se puede entender que los datos brutos tienen un valor potencial. Además, al contrario que los bienes, los datos no son rivales y pueden utilizarse varias veces sin agotarse. Asimismo, no existen mercados formales de datos brutos debidamente desarrollados; como se explicará con más detalle en el capítulo III, no se puede pensar en los datos en términos de propiedad, sino sobre todo en términos de derechos y acceso. Actualmente no existe un mercado con oferta y demanda de datos brutos, sino que estos se obtienen principalmente de los usuarios. La mayoría de las veces, cuando se habla de mercados de datos, se trata de mercados de inteligencia digital (o productos de datos).

Muchas de las estimaciones del valor de los datos se refieren en realidad al valor de esos mercados de productos de datos. Dichas estimaciones pueden proporcionar una idea del valor de los datos brutos utilizados para obtener esos productos de datos: si el valor de los productos de datos aumenta, el valor de los datos brutos debería también aumentar. Pero no ayudan mucho a distinguir el valor de los datos brutos del valor que se añade con su procesamiento y monetización. Y en materia de desarrollo, lo que importa es el valor agregado nacional en los procesos de producción de los países en desarrollo.

En ese sentido, la herramienta de seguimiento del mercado de datos de la Unión Europea (European Data Market Monitoring Tool) considera que el mercado de datos es "el mercado en el que se intercambian datos digitales en forma de 'productos' o 'servicios' resultantes del procesamiento de datos brutos" (European Commission, 2020a). La herramienta permite realizar comparaciones internacionales del valor del mercado de datos de la Unión Europea (incluido el Reino Unido) con los de los Estados Unidos, el Japón y el Brasil, como se muestra en la figura I.10. El valor de los mercados de datos ha aumentado de forma significativa en los últimos cinco años en todas las economías analizadas, aunque en el Brasil se mantiene relativamente bajo durante todo el período evaluado. El análisis muestra claramente la posición dominante de los Estados Unidos[15].

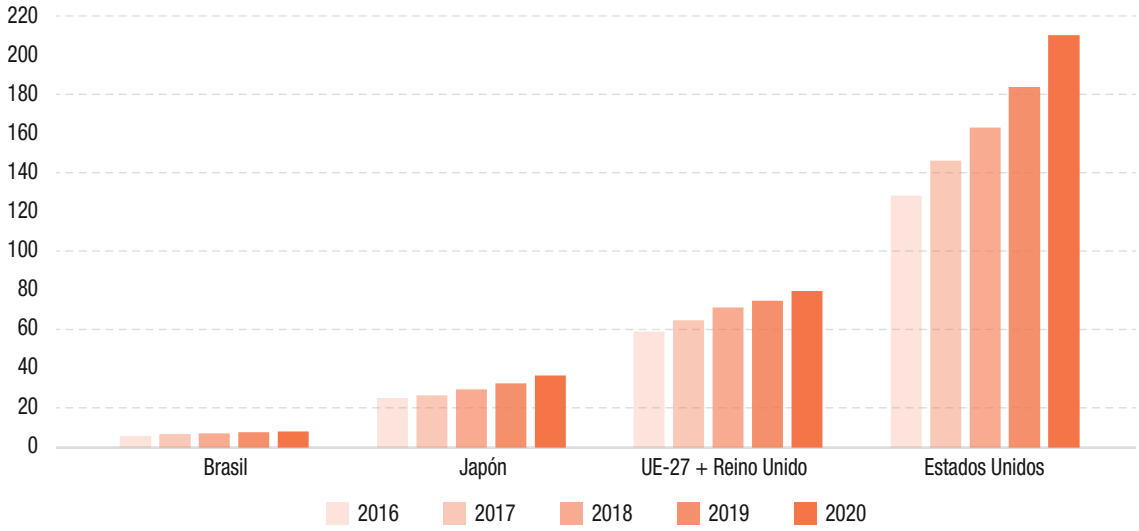
F. MEDICIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Medir los flujos de datos transfronterizos es aún más difícil. De hecho, actualmente no hay ninguna forma de medirlos en la práctica. Principalmente se cuantifican utilizando indicadores indirectos, pero sin demasiado éxito, ya que estos distan mucho de proporcionar indicios e información concluyentes para la formulación de políticas y para el desarrollo[16].

[15] Las oficinas de estadística de varios países están tratando de mejorar las estimaciones del valor de los datos. Véase, por ejemplo, Statistics Canada (2019).

[16] Se pueden consultar otros análisis sobre las dificultades para medir los flujos de datos transfronterizos y la importancia de mejorar su medición en National Telecommunications and Information Administration (2016); Coyle y Nguyen (2019); y Cory (2020).

Figura I.10. Valor de los mercados de datos, en economías seleccionadas, 2016-2020
(Milliones de euros)



Fuente: UNCTAD, cálculos basados en información de la Comisión Europea (European Commission, 2020a).

En términos de volumen, la principal medida utilizada es el ancho de banda internacional. Según la UIT, "por ancho de banda internacional de Internet se entiende la capacidad total utilizada de ancho de banda de Internet a escala mundial, en megabits por segundo (Mbit/s). El ancho de banda internacional de Internet utilizado se refiere a la intensidad media de tráfico de Internet por los cables de fibra óptica y los radioenlaces internacionales. Dicha media se calcula para los 12 meses del año de referencia y tiene en cuenta el tráfico de todos los enlaces internacionales de Internet [...]. La intensidad media de tráfico combinada de diferentes enlaces internacionales de Internet puede expresarse como la suma de las intensidades medias de tráfico de cada uno de los enlaces"[17].

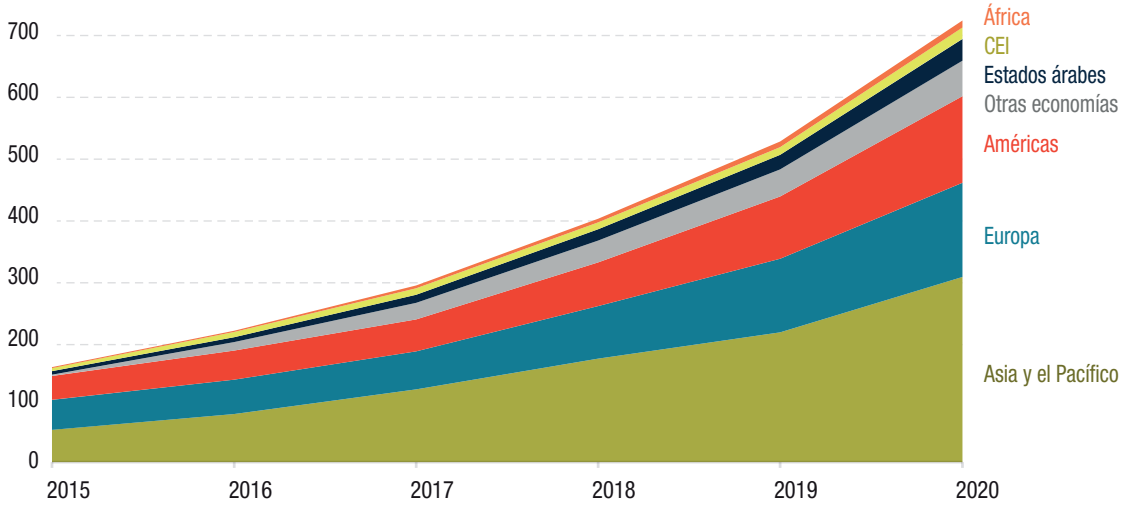
Los datos sobre el ancho de banda internacional son proporcionados por la UIT y TeleGeography. La UIT facilita datos estadísticos sobre la capacidad y el uso de ancho de banda internacional por países. El uso total de ancho de banda internacional experimentó un auge considerable en 2020. La mayor parte del uso de ancho de banda internacional se concentró en las regiones de Asia y el Pacífico, Europa y las Américas, mientras que el porcentaje correspondiente a África se mantuvo muy bajo (figura I.11).

Los datos de acceso abierto de TeleGeography, representados en la figura I.12, ilustran el crecimiento del ancho de banda internacional y la previsión para 2024. La mayor parte del uso de ancho de banda internacional se realiza entre las regiones de América del Norte y Europa, y entre América del Norte y Asia. En cuanto a los países en desarrollo, la conexión Norte-Sur entre América del Norte y América Latina registra el porcentaje de uso de ancho de banda internacional más elevado. No obstante, se trata solo de la cantidad de datos que circulan expresada en *bytes*, ya que no se indica en qué dirección lo hacen. Tampoco se distingue entre los flujos de entrada y salida de datos de cada región/país en particular. Además, los *bytes* indicados corresponden tanto a datos brutos como a productos de datos[18].

[17] Si el tráfico es asimétrico, es decir, si hay más tráfico de entrada (enlace descendente) que de salida (enlace ascendente), se utiliza la intensidad media del tráfico de entrada (enlace descendente). Véase "ICT Development Index (IDI): conceptual framework and methodology", disponible en www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx.

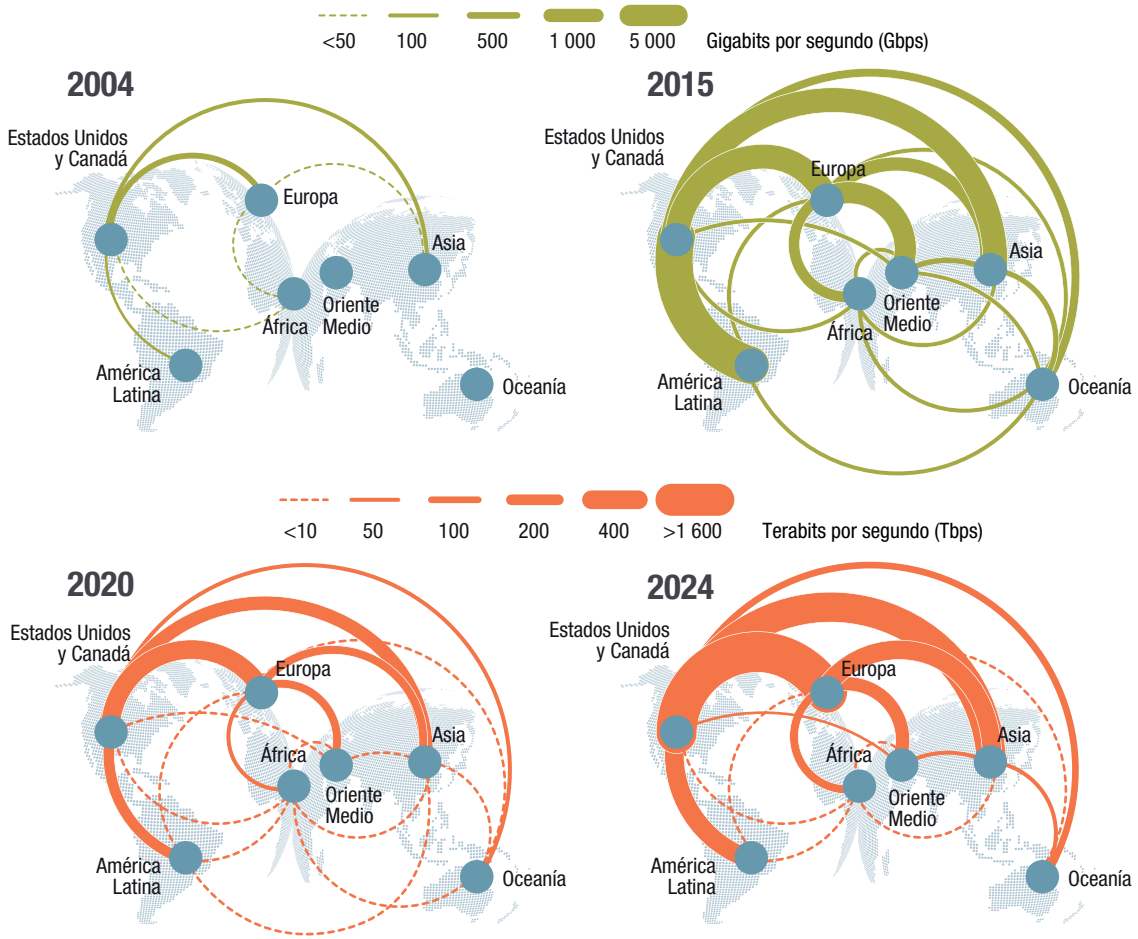
[18] Se trata de información que es de acceso abierto. TeleGeography es la mayor fuente de datos y análisis sobre las redes de larga distancia y el mercado de cables submarinos. Los datos correspondientes a capacidad, propiedad, precios al por mayor (sin descuento) y otras magnitudes están disponibles mediante suscripción. Por consiguiente, podría haber datos estadísticos más detallados, pero de uso reservado. TeleGeography es también la fuente en la que se basan las publicaciones del McKinsey Global Institute, en las que se presentan análisis relativos a los flujos de datos transfronterizos (que muy a menudo se citan como referencias fidedignas en la materia, pero que no estaría de más examinarlas con detenimiento).

Figura I.11. Ancho de banda internacional, por región, 2015-2020
(Terabits por segundo)



Fuente: UNCTAD, cálculos basados en información de la UIT (ITU, 2020) y en su informe interactivo titulado "Measuring digital development, Facts and figures 2020", disponible en https://www.itu.int/en/ITU-D/Statistics/Pages/ff2020interactive.aspx.
Nota: Los grupos de países son los establecidos por la fuente. Los datos relativos a 2020 son estimaciones de la UIT.

Figura I.12. Evolución del ancho de banda internacional entre regiones, en años seleccionados



Fuente: UNCTAD, a partir de TeleGeography (2015, 2019, 2021b).
Nota: Un *terabyte* equivale a 1.000 *gigabytes*. Los datos correspondientes a 2024 son previsiones.

Un análisis realizado por Nikkei a partir de datos estadísticos de la UIT y de TeleGeography mostró que, en 2019, los flujos de datos transfronterizos de China —incluido Hong Kong (China)— superaron en gran medida a los de los otros diez países o territorios y regiones examinados, incluidos los Estados Unidos. El 23 % de los flujos de datos transfronterizos en el mundo correspondió a China, mientras que los Estados Unidos ocuparon el segundo lugar, con un 12 %. El origen del liderazgo de China radica en sus conexiones con el resto de Asia. Si bien en 2001 los Estados Unidos generaron el 45 % de los flujos de datos de entrada y salida de China, esa cifra pasó a ser solo del 25 % en 2019. Los países asiáticos producen ya más de la mitad del total, sobre todo Viet Nam, con un 17 %, y Singapur, con un 15 %[19].

Aunque los datos estadísticos de la UIT y de TeleGeography proporcionan información e indicios interesantes sobre la evolución de los flujos de datos transfronterizos, la cantidad de datos no es el aspecto más importante. También hay que examinar la naturaleza y la calidad de los datos. Es probable que una parte significativa de los datos recopilados no tengan ninguna utilidad económica, aunque generen ingresos para algunas empresas. De hecho, IBM estima que el 90 % de los datos procedentes de sensores y de conversiones analógico-digitales no se utilizan. Además, según Sandvine (2020), casi el 80 % de todo el tráfico de Internet está relacionado con vídeos, redes sociales y juegos.

Desde el punto de vista económico, también sería conveniente poder medir el valor de los flujos de datos transfronterizos. En 2016, la Administración Nacional de Telecomunicaciones e Información de los Estados Unidos elaboró un informe en el que se analizaba dicha medición y se ofrecían algunas recomendaciones al respecto (recuadro I.2). En relación con la segunda recomendación, sobre la necesidad de contar con definiciones estándar, conviene señalar que el propio informe, cuyo objetivo es examinar la situación con respecto a la medición de los flujos de datos transfronterizos, no arroja ninguna luz sobre lo que son realmente dichos flujos.

Desde la publicación de ese informe han pasado cinco años, un período muy largo si se tiene en cuenta la rápida evolución del desarrollo tecnológico impulsado por los datos. Sin embargo, aunque la economía digital impulsada por los datos ha cambiado significativamente durante ese tiempo, se ha avanzado poco en la medición de los flujos de datos. Para que los responsables políticos puedan tomar decisiones con base empírica destinadas a regular esos flujos, es necesario contar con más estadísticas oficiales sobre las cuestiones relacionadas con los datos, por cuanto las estadísticas más importantes en esa esfera son proporcionadas en su mayoría por empresas como TeleGeography, Cisco o International Data Corporation.

En particular, para promover el desarrollo, sería importante poder distinguir entre datos brutos y productos de datos. En la economía ordinaria, por lo que respecta a la relación entre el comercio internacional y el desarrollo, el análisis se centra en la estructura de las importaciones y las exportaciones según su nivel de especialización y contenido tecnológico. El aumento del nivel de especialización y contenido tecnológico de las exportaciones frente al de las importaciones sería un indicio de que se ha añadido valor a escala nacional y, por lo tanto, de desarrollo. Del mismo modo, en el caso de los flujos de datos transfronterizos, en el contexto de la cadena de valor de los datos —desde la reunión de datos brutos hasta la producción de inteligencia digital (productos de datos), que implica añadir valor—, sería importante examinar la estructura de los flujos de entrada y salida de datos para determinar si son datos brutos o productos de datos. Actualmente hay indicios de que la mayoría de los flujos de salida de datos de los países en desarrollo son flujos de datos brutos, mientras que los flujos de entrada de datos consisten más bien en inteligencia digital producida en los países que están en condiciones más ventajosas en materia de datos y más capacitados para procesar datos brutos (véase también el capítulo III). Por consiguiente, sería importante contar con medidas que permitan distinguir entre los flujos de salida y de entrada de datos, así como entre datos brutos y productos de datos[20].

[19] Véase *Nikkei*, 24 de noviembre de 2020, "China rises as world's data superpower as internet fractures", disponible en https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures. La metodología utilizada en el análisis no está nada clara, por lo que no es fácil averiguar cómo se ha realizado y de dónde proceden los datos estadísticos relativos a los flujos de datos de entrada y salida de China.

[20] Véase también el capítulo II para un repaso de las publicaciones sobre cuestiones de medición de datos.

Recuadro I.2. Recomendaciones de la Administración Nacional de Telecomunicaciones e Información de los Estados Unidos formuladas en su informe sobre la medición del valor de los flujos de datos transfronterizos

Se recomendó, entre otras cosas:

- Mejorar la cobertura global y la calidad de los datos estadísticos del Estado sobre el sector de los servicios.
- Desarrollar una nomenclatura estándar o definiciones estándar para los conceptos relacionados con los flujos de datos transfronterizos, y distinguir entre conceptos como economía digital, economía digital intensiva, economía digitalmente habilitada y TIC.
- Comprender mejor la manera en que las empresas utilizan los flujos de datos transfronterizos y el valor económico que estos aportan. Estos datos estadísticos deben abarcar toda la economía de los Estados Unidos, así como sectores específicos.
- Desarrollar estadísticas macroeconómicas mejoradas y coherentes para medir el valor de los flujos de datos transfronterizos y la economía digital, en particular su contribución al PIB. Estos datos estadísticos deben abarcar toda la economía de los Estados Unidos, así como sectores específicos.
- Proseguir el diálogo entre el Departamento de Comercio y el sector privado para facilitar el intercambio de datos y la vinculación de conjuntos de datos públicos y privados, siempre que sea legal, factible y compatible con una protección sólida de la privacidad de las empresas.
- Mantener la colaboración entre el Departamento de Comercio y las organizaciones internacionales para garantizar que los países de todo el mundo dispongan de indicadores sobre los flujos de datos transfronterizos y la economía digital.

Fuente: National Telecommunications and Information Administration (2016).

G. RECOPILACIÓN DE DATOS

Los datos pueden ser recopilados por diferentes actores y de diversas maneras (véase el capítulo III). Como se mostrará en esta sección y en las siguientes, las plataformas digitales globales desempeñan un papel cada vez más importante en todas las etapas de la cadena de valor de los datos. En esta sección se analiza su papel como entidades que más datos recopilan a escala mundial. Posteriormente se examina la evolución de la Internet de las cosas, dado que se espera que el auge de los dispositivos con acceso a Internet y las conexiones entre máquinas impulsen considerablemente la generación y los flujos de datos.

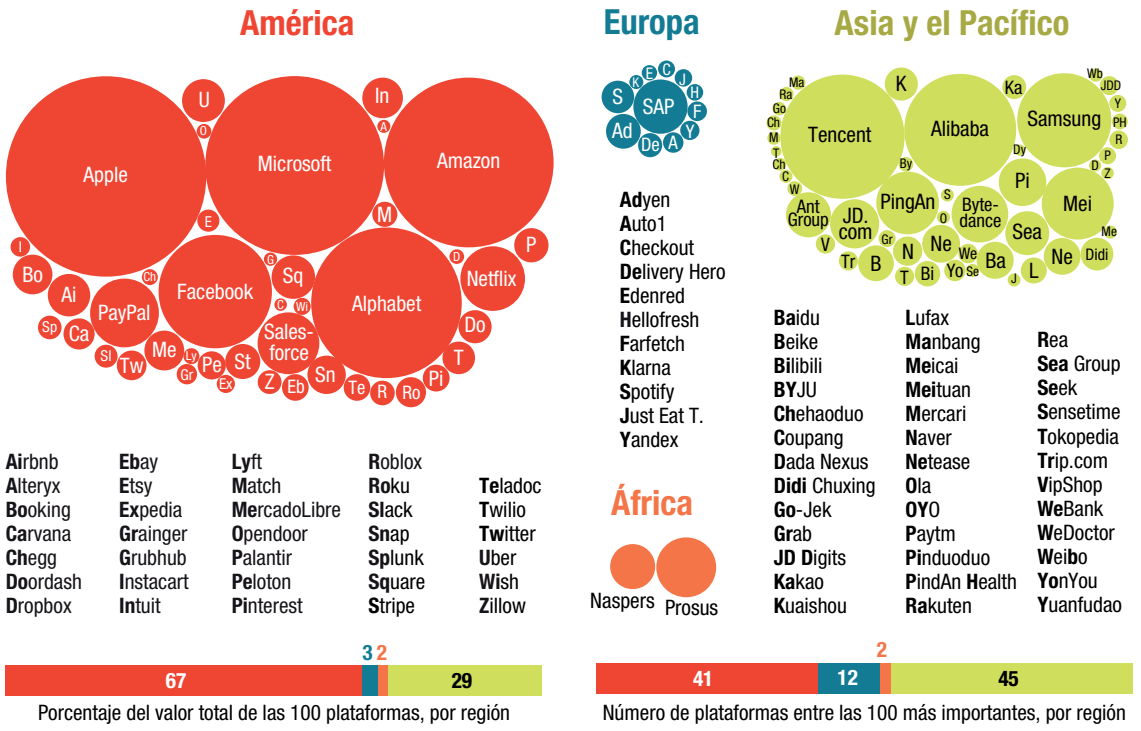
1. Plataformas digitales

Las plataformas digitales globales se encuentran en una situación inmejorable para recopilar datos de forma masiva, debido al gran número de usuarios que acceden a sus servicios. Cuentan, por tanto, con una importante ventaja competitiva. Dado que no existe un sistema internacional adecuado de gobernanza global de los datos, dicha ventaja en la recopilación de datos hace que las plataformas puedan acaparar la mayor parte de las ganancias monetarias generadas con la economía digital impulsada por los datos y, por ende, con los flujos de datos transfronterizos.

Los efectos de red, combinados con el acceso a los datos y las economías de escala y de alcance, han dado lugar a tendencias monopolísticas y a un mayor poder de mercado de las principales plataformas digitales del mundo, que tienen su sede sobre todo en los Estados Unidos y China. Las plataformas han reforzado su posición realizando adquisiciones estratégicas de otras empresas, expandiendo sus actividades a nuevos sectores y defendiendo sus intereses ante los poderes públicos (UNCTAD, 2019a, 2019b). En 2020, reforzaron aún más su situación durante la pandemia. En la figura I.13 se muestra la distribución geográfica de las plataformas digitales globales en 2021.

En esta sección se analizan las repercusiones de la pandemia en las plataformas digitales. A continuación, se examinan las prácticas de cabildeo de algunas plataformas que tratan de influir en los responsables

Figura I.13. Distribución geográfica de las 100 principales plataformas digitales globales, por capitalización bursátil (2021)



Fuente: Holger Schmidt, disponible en www.netzoekonom.de/vortraege/#tab-id-1 (datos de mayo de 2021).
Nota: Como referencia, la capitalización bursátil de Apple es de 2,22 billones de dólares, mientras que la de Mercado Libre es de 88.700 millones de dólares, la de Baidu de 80.200 millones de dólares y la de Spotify de 59.700 millones de dólares.

políticos para beneficio propio. Además, habida cuenta de que una gran parte de los datos sirven para alimentar los algoritmos utilizados en el ámbito de la IA, y de que la evolución de esta tiene importantes consecuencias para el futuro de la economía digital mundial, en la última parte de esta sección se examina la inversión realizada en IA por las principales plataformas digitales globales.

a) Repercusiones de la pandemia en las plataformas digitales globales

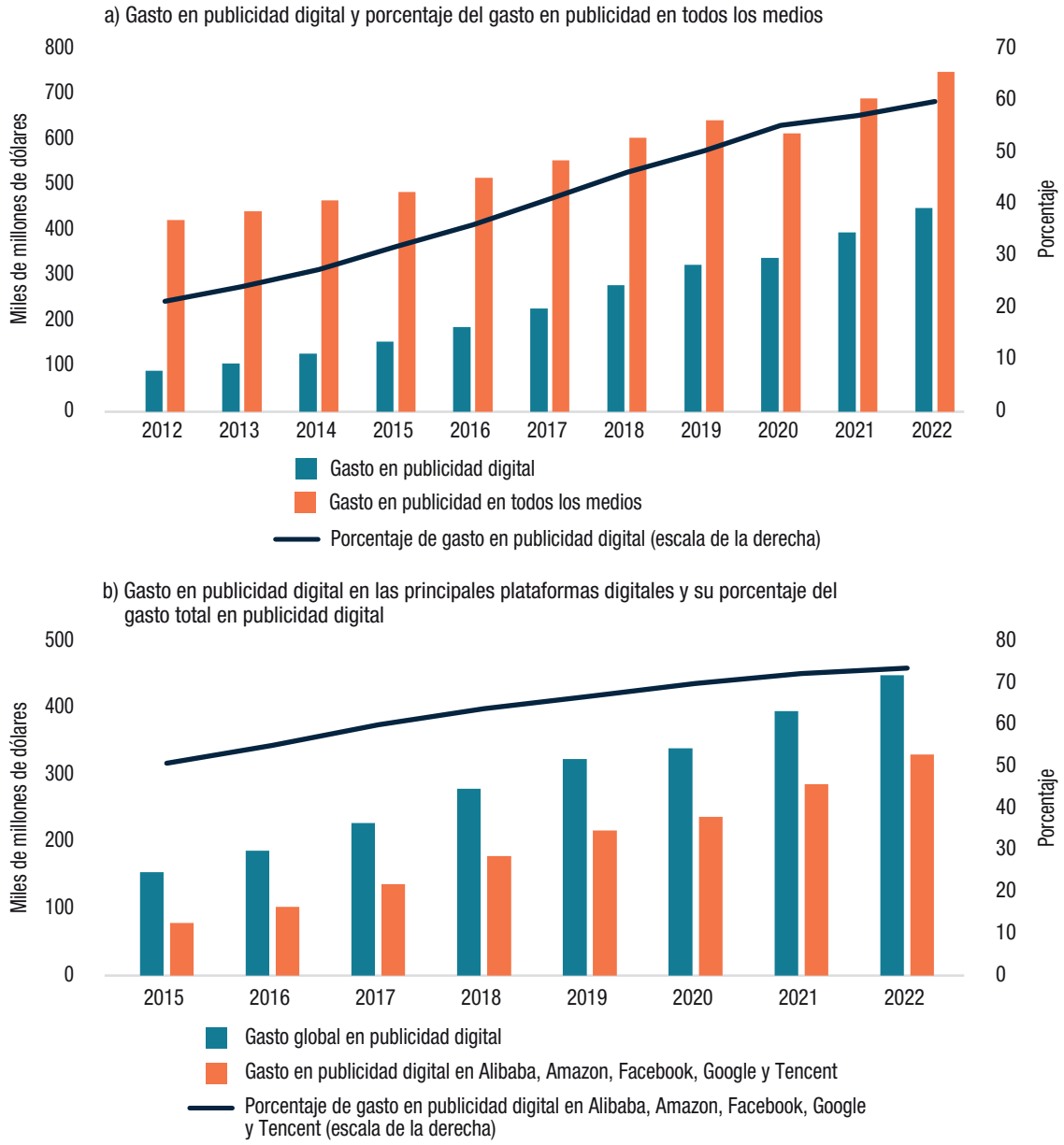
Los beneficios y el valor de la capitalización bursátil de las principales plataformas digitales han aumentado considerablemente a raíz de la pandemia. No es de extrañar, ya que la mayoría de las soluciones digitales adoptadas para hacer frente a los confinamientos y las restricciones a los viajes han sido aportadas por unas pocas grandes empresas. Por ejemplo, el aumento del comercio electrónico ha impulsado considerablemente el negocio de venta minorista en línea de Amazon. Asimismo, las operaciones comerciales de Amazon en la nube han crecido enormemente, debido al aumento de la demanda y el tráfico de Internet. Lo mismo ha sucedido con Microsoft. Además, Apple ha registrado un fuerte aumento de la demanda de sus dispositivos, ya que la gente ha pasado a realizar sus actividades cada vez más a través de Internet.

A continuación se analiza la evolución en los últimos años de la publicidad digital, los beneficios, los precios de las acciones y la capitalización bursátil de esas empresas, con especial hincapié en las repercusiones de la pandemia.

i) Publicidad digital

Una de las principales formas en que algunas plataformas digitales monetizan sus datos es con la publicidad digital. Las plataformas digitales globales han seguido consolidando su posición dominante en ese mercado. Para 2022, se espera que el gasto en publicidad digital alcance el 60 % del gasto en publicidad en todos los medios, lo que representa aproximadamente el doble del porcentaje de 2013 (figura I.14a). Para ese mismo año, se prevé que el porcentaje de gasto en publicidad en las cinco principales plataformas digitales supere el 70 % del gasto total en publicidad digital (figura I.14b).

Figura I.14. Gasto en publicidad digital, 2012-2022



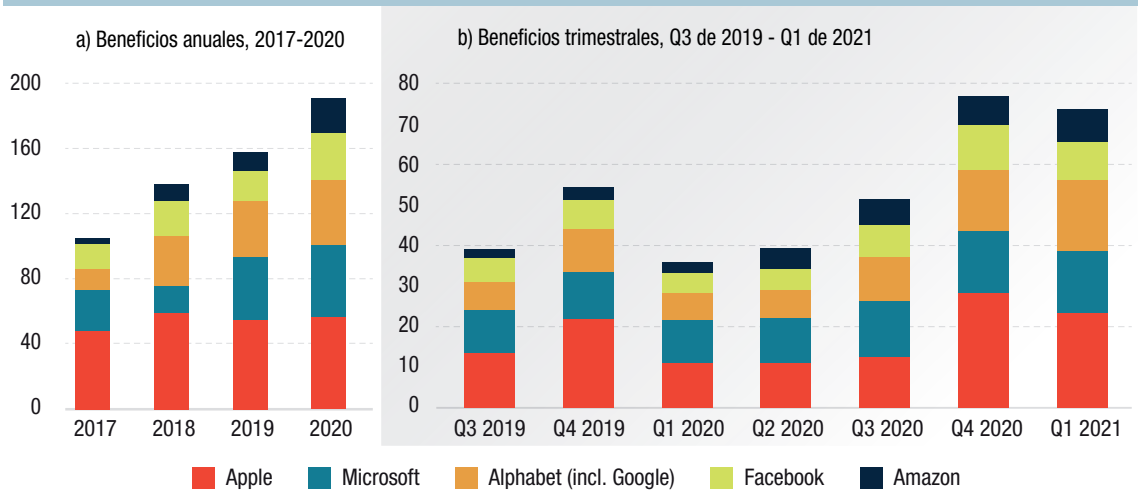
Fuente: UNCTAD, a partir de datos de eMarketer, "Global Digital Ad Spending Update Q2 2020", disponible en www.emarketer.com/content/global-digital-ad-spending-update-q2-2020.
Nota: Los datos de 2020 a 2022 son estimaciones.

ii) Beneficios

Desde 2017, los beneficios de las principales plataformas digitales han venido aumentando, incluso en 2020, en medio de la crisis económica resultante de la pandemia (figura I.15a). Los ingresos netos de las principales plataformas digitales de los Estados Unidos alcanzaron 192.400 millones de dólares en 2020, lo que representó un aumento del 21,1 % respecto al año anterior.

En la figura I.15b se representan los beneficios trimestrales obtenidos por dichas plataformas digitales desde el segundo semestre de 2019 hasta el primer trimestre de 2021, lo que permite conocer mejor las repercusiones de la pandemia en esas empresas. Los valores en los trimestres tercero (Q3) y cuarto (Q4) de 2019 dan cuenta de una situación anterior a la crisis con unos ingresos netos y un crecimiento de estos suficientes. En el primer trimestre (Q1) de 2020, las empresas en cuestión registraron una caída

Figura I.15. Beneficios de las principales plataformas digitales de los Estados Unidos
(Miles de millones de dólares)



Fuente: UNCTAD, cálculos basados en *The Wall Street Journal*, en https://www.wsj.com/market-data/quotes/company-list/ (consultado en mayo de 2021).

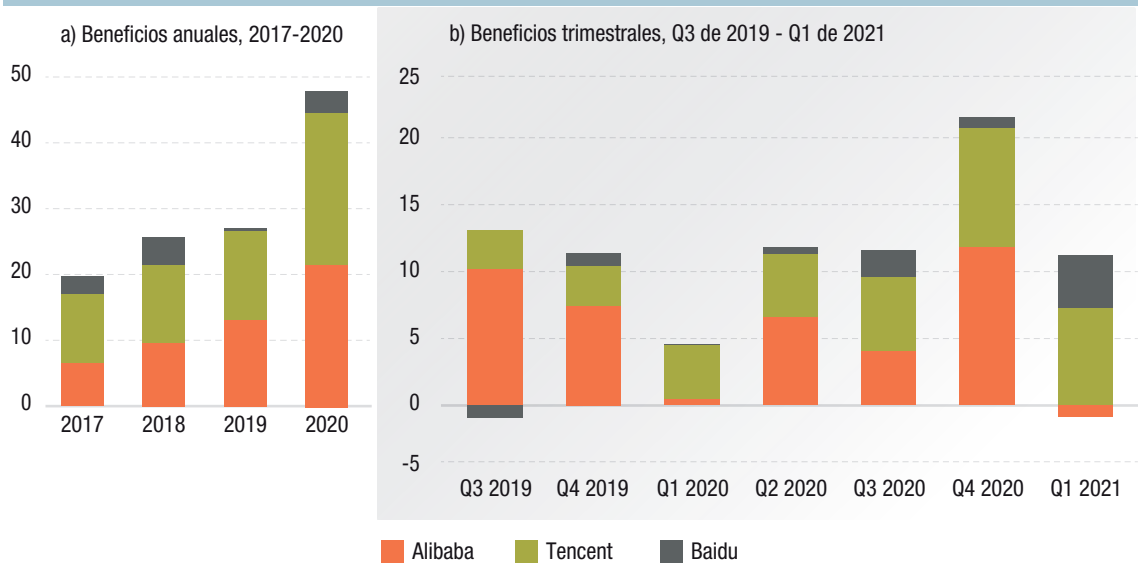
de sus beneficios, en comparación con el Q4 de 2019, como consecuencia de la crisis provocada por la pandemia que sacudió significativamente a todos los países entre febrero y marzo de 2020. Pese a la drástica caída de los ingresos netos, esas empresas seguían siendo rentables en el Q1 de 2020. Tras el impacto inicial, la pandemia propició un aumento de la demanda de servicios en la nube, compras en línea, vídeos y juegos, redes sociales y videoconferencias. Como consecuencia, los ingresos netos de esas empresas crecieron en el segundo trimestre (Q2) de 2020 y, en particular, los ingresos netos de Amazon aumentaron más del doble respecto al Q1 de 2020. En el Q3 y el Q4 de 2020, esas plataformas digitales más importantes, domiciliadas en los Estados Unidos, parecían haber vuelto a la normalidad, e incluso estar en una situación más favorable. De hecho, si se compara con el mismo período del año anterior, los ingresos netos combinados de Amazon, Alphabet (incluido Google), Apple, Facebook y Microsoft aumentaron un 31 % en el Q3 de 2020 y un 41 % en el Q4 de 2020. Aunque el beneficio acumulado disminuyó ligeramente entre el Q4 de 2020 y el Q1 de 2021, este último aumentó más del doble respecto al Q1 de 2020. Estas tendencias ponen de manifiesto que las empresas mencionadas no solo han resistido a la crisis, sino que sus modelos de negocio y su predominio, combinados con la fuerte demanda de servicios digitales, han hecho que aumenten sus ingresos en medio de la crisis económica mundial.

Las principales plataformas digitales chinas —Alibaba, Baidu y Tencent— también salieron beneficiadas, ya que sus ingresos netos acumulados aumentaron un 37 %, de casi 20.000 millones de dólares en 2017 a 27.000 millones de dólares en 2019 (figura I.16a). El aumento de los beneficios fue aún más notable en 2020, ya que los ingresos netos acumulados rondaron 48.000 millones de dólares, lo que representó un incremento del 78 % respecto a 2019. En cuanto a las repercusiones de la pandemia, que comenzó a manifestarse en China a finales de 2019 —antes que en los Estados Unidos—, parece que solo Alibaba se vio afectada en el Q4 de 2019 (figura I.16b). Aunque en el Q1 de 2020 los beneficios del conjunto de estas empresas disminuyeron bruscamente (sobre todo por la caída de los beneficios de Alibaba), Tencent resultó ganadora, con unos beneficios superiores a los de los dos trimestres anteriores. En el Q2 y el Q3 de 2020, los ingresos netos trimestrales aumentaron, sobre todo en el caso de Alibaba, de modo que los beneficios acumulados de esas empresas chinas en el Q3 de 2020 fueron similares a los del Q3 de 2019. El hecho de que los ingresos netos acumulados se dispararan en 2020 se atribuye a los cuantiosos beneficios obtenidos por Alibaba y Tencent en el Q4 de 2020.

iii) Precios de las acciones y capitalización bursátil

El aumento de los beneficios de las principales plataformas digitales globales no ha pasado desapercibido para el mundo de la inversión, como demuestra la subida de los precios de las acciones de dichas plataformas. En la figura I.17 se compara el crecimiento del precio de las acciones de esas empresas

Figura I.16. Beneficios de las principales plataformas digitales de China
(Miles de millones de dólares)



Fuente: UNCTAD, cálculos basados en *The Wall Street Journal*, en www.wsj.com/market-data/quotes/company-list/ (consultado en mayo de 2021).

desde el Q4 de 2019 hasta enero de 2021 con la evolución del índice compuesto de la Bolsa de Nueva York, indicador del estado de la economía en los Estados Unidos.

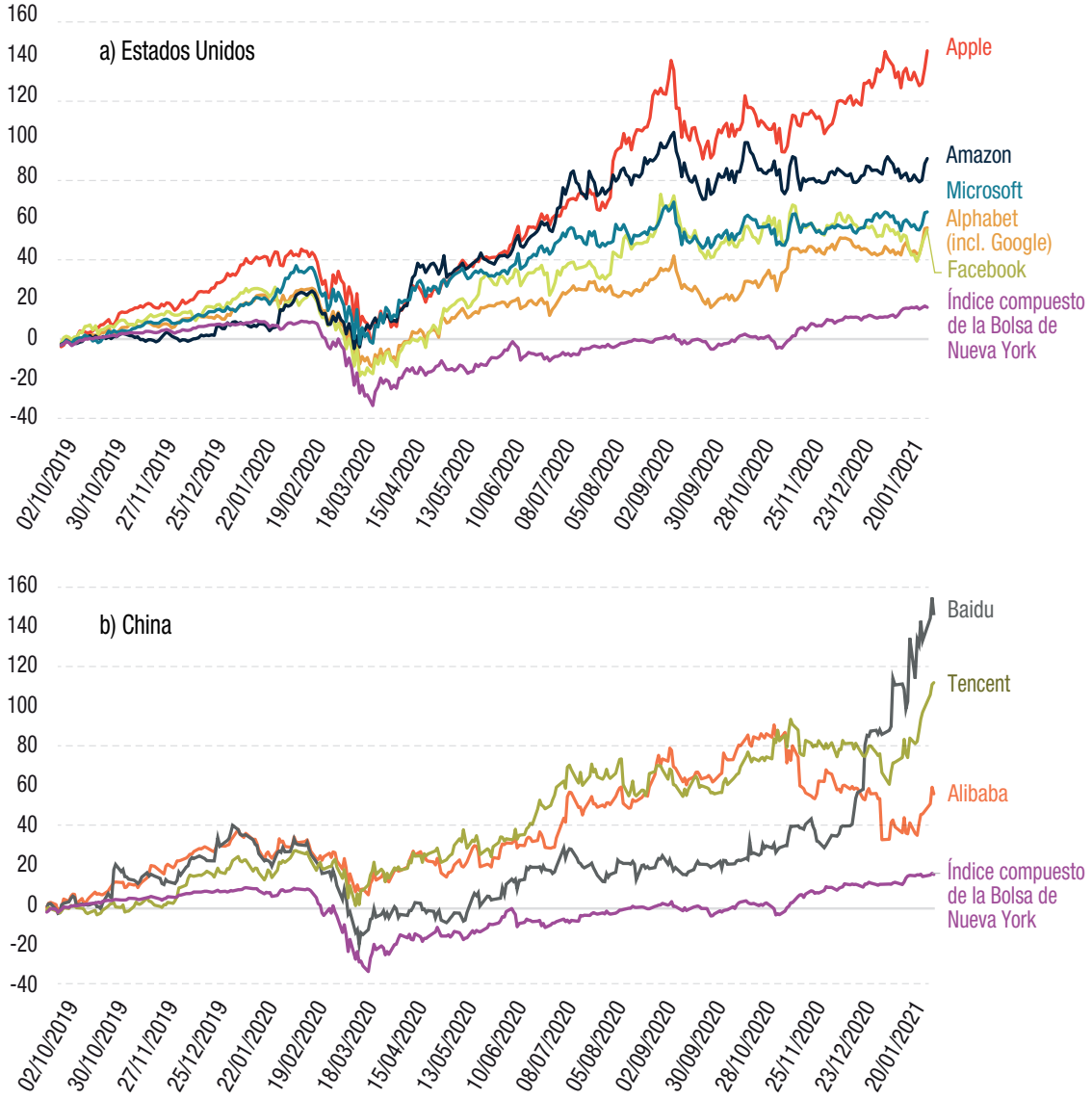
Desde finales de febrero hasta finales de marzo de 2020, los precios de las acciones de las principales plataformas digitales de los Estados Unidos y China, así como el índice compuesto de la Bolsa de Nueva York, experimentaron caídas significativas respecto a sus valores a 1 de octubre de 2019 o, en el mejor de los casos, un crecimiento menor, como consecuencia del impacto inicial de la crisis sanitaria y económica mundial. La tasa de crecimiento del precio de las acciones alcanzó su punto más bajo para Amazon el 12 de marzo de 2020 (-3,4 %); para Facebook, Microsoft y Tencent el 16 de marzo de 2020 (-17 %, -1,2 % y +1,4 %, respectivamente); para Baidu el 18 de marzo de 2020 (-18 %); para Alphabet (incluido Google), Apple y Alibaba el 23 de marzo de 2020 (-12,6 %, -0,1 % y +6,8 %, respectivamente); mientras que el índice compuesto de la Bolsa de Nueva York alcanzó su valor más bajo el 23 de marzo de 2020 (31,6 %).

No obstante, desde mediados y finales de marzo de 2020, los precios de las acciones de las plataformas digitales globales y de las empresas incluidas en el índice compuesto de la Bolsa de Nueva York empezaron a recuperarse. La recuperación fue, en promedio, menor para el índice compuesto de la Bolsa de Nueva York que para las plataformas digitales globales. Entre el 1 de octubre de 2019 y el 21 de enero de 2021, el índice compuesto de la Bolsa de Nueva York aumentó un 17 %. En el mismo período, las tasas de crecimiento del precio de las acciones de las empresas seleccionadas fueron al menos tres veces mayores: Facebook (55 %), Alphabet (incluido Google, 56 %), Alibaba (57 %), Microsoft (64 %), Amazon (90 %), Tencent (113 %), Apple (144 %) y Baidu (147 %).

En general, la recuperación del índice compuesto de la Bolsa de Nueva York en el marco de una profunda crisis económica apunta a cierta desconexión entre los mercados financieros y la economía real. Y, lo que es más significativo, las notables subidas del precio de las acciones de las principales plataformas digitales evidencian una desconexión aún mayor entre la economía digital y la economía real.

Las grandes subidas del precio de las acciones de las principales plataformas digitales globales durante 2020 dieron lugar a cambios considerables en la capitalización bursátil de esas empresas (figura I.18). En lo que respecta a las empresas estadounidenses, a finales de 2019, la capitalización bursátil de Microsoft y Apple ya superaba el billón de dólares cada una, la de Alphabet (incluido Google) y Amazon se acercaba a esa cifra, y Facebook estaba valorado en más de 0,6 billones de dólares. A lo largo de 2020, la capitalización bursátil de esas empresas registró importantes aumentos: del 22 % para Facebook,

Figura I.17. Precio de las acciones de las plataformas digitales globales de los Estados Unidos y China frente al índice compuesto de la Bolsa de Nueva York
(Variación en porcentaje)



Fuente: UNCTAD, cálculos basados en datos de Yahoo! Finance disponibles en https://finance.yahoo.com (consultado en enero de 2021).
Nota: Las cifras indican la variación del precio de las acciones en cada fecha respecto al 1 de octubre de 2019.

del 27 % para Alphabet (incluido Google), del 34 % para Microsoft, del 66 % para Apple y del 70 % para Amazon. Como consecuencia, después de un año en el que se produjeron numerosas quiebras y se concedieron cuantiosas subvenciones estatales para salvar industrias en todo el mundo, en enero de 2021, el valor de mercado de Facebook era de 716.000 millones de dólares, el de Alphabet de 1,17 billones de dólares, el de Amazon de 1,56 billones de dólares y el de Microsoft de 1,61 billones de dólares. Apple superó a las demás plataformas y alcanzó un valor de mercado de más de 2 billones de dólares, lo que la convirtió en la primera empresa estadounidense en superar esa cifra.

Los tres gigantes digitales chinos tenían una menor capitalización bursátil a finales de 2019 en comparación con los de los Estados Unidos. Baidu tenía entonces el valor de mercado más bajo, pero en 2020 su valor aumentó un 86,4 %, hasta alcanzar 81.500 millones de dólares en enero de 2021. Alibaba, que tenía

Figura I.18. Capitalización bursátil de las plataformas digitales globales de los Estados Unidos y China, Q4 de 2019 - enero de 2021
(Miles de millones de dólares)

Fuente: UNCTAD, cálculos basados en datos de Yahoo! Finance disponibles en https://finance.yahoo.com (consultado en enero de 2021).

la mayor capitalización bursátil a finales de 2019 (571.000 millones de dólares), registró un aumento del 17,8 % en su valor, que alcanzó 672.800 millones de dólares. La capitalización bursátil de Tencent fue la que más aumentó en términos absolutos en 2020 (un 51,9 %), hasta 699.800 millones de dólares, por encima de la de Alibaba.

b) Influencia en las políticas públicas

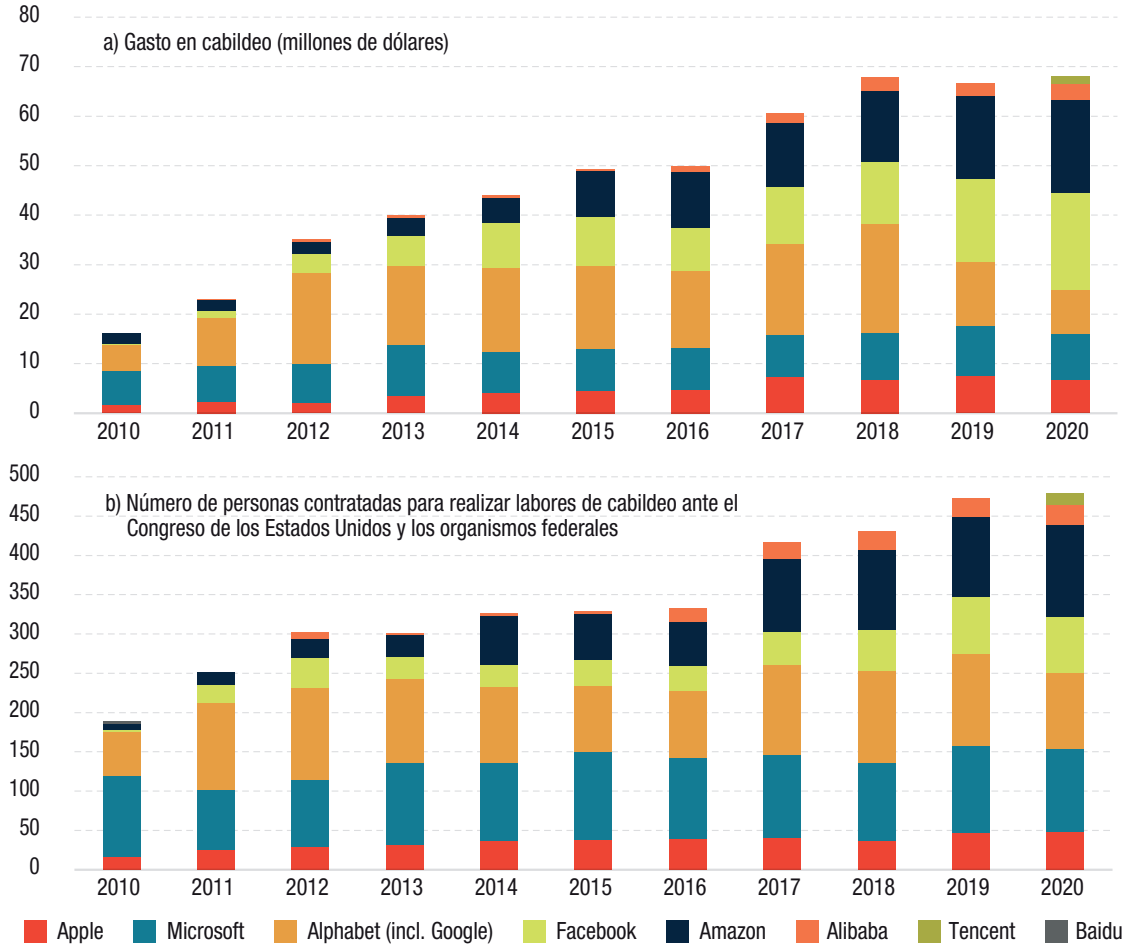
Algunas de las principales plataformas digitales recurren al cabildeo para tratar de influir en las normativas.

i) El cabildeo en los Estados Unidos

Las plataformas digitales dedican importantes esfuerzos a intentar influir en las decisiones del Congreso de los Estados Unidos: gastan grandes cantidades de dinero en actividades de cabildeo y en la contratación de personas con conexiones políticas. En 2020, Facebook y Amazon estaban entre las diez empresas que más gastaron en cabildeo, superadas únicamente por las principales asociaciones sectoriales (Center for Responsive Politics, 2021). Las plataformas digitales de los Estados Unidos (Alphabet (incluido Google), Amazon, Apple, Facebook y Microsoft) pasaron de gastar 16 millones de dólares en 2010 a más de 63 millones en 2020 (figura I.19a). Alibaba ha realizado una intensa labor de cabildeo ante el Congreso de los Estados Unidos, aunque en menor medida que las empresas estadounidenses por lo que respecta al gasto[21]. A principios de la década de 2010, Google y Microsoft eran las empresas que más gastaban en cabildeo, mientras que la actividad de Amazon, Apple y Facebook a ese respecto era bastante menor. Sin embargo, Facebook y Amazon fueron las que más aumentaron su gasto en cabildeo en el período 2010-2020. El gasto de Facebook pasó de 0,35 millones de dólares en 2010 a casi 20 millones, valor que superó al de las otras cuatro empresas. Como era de esperar, el aumento del gasto conllevó la contratación de más personal para realizar actividades de cabildeo (figura I.19b).

[21] Tencent solo gastó en cabildeo en 2020, y no se registró ningún gasto de Baidu en ese concepto en la última década.

Figura I.19. Cabildeo de las plataformas digitales globales en los Estados Unidos, 2010-2020



Fuente: UNCTAD, cálculos basados en "Lobbying Data Summary", Center for Responsive Politics, disponible en https://www.opensecrets.org/federal-lobbying.

ii) El cabildeo en la Unión Europea

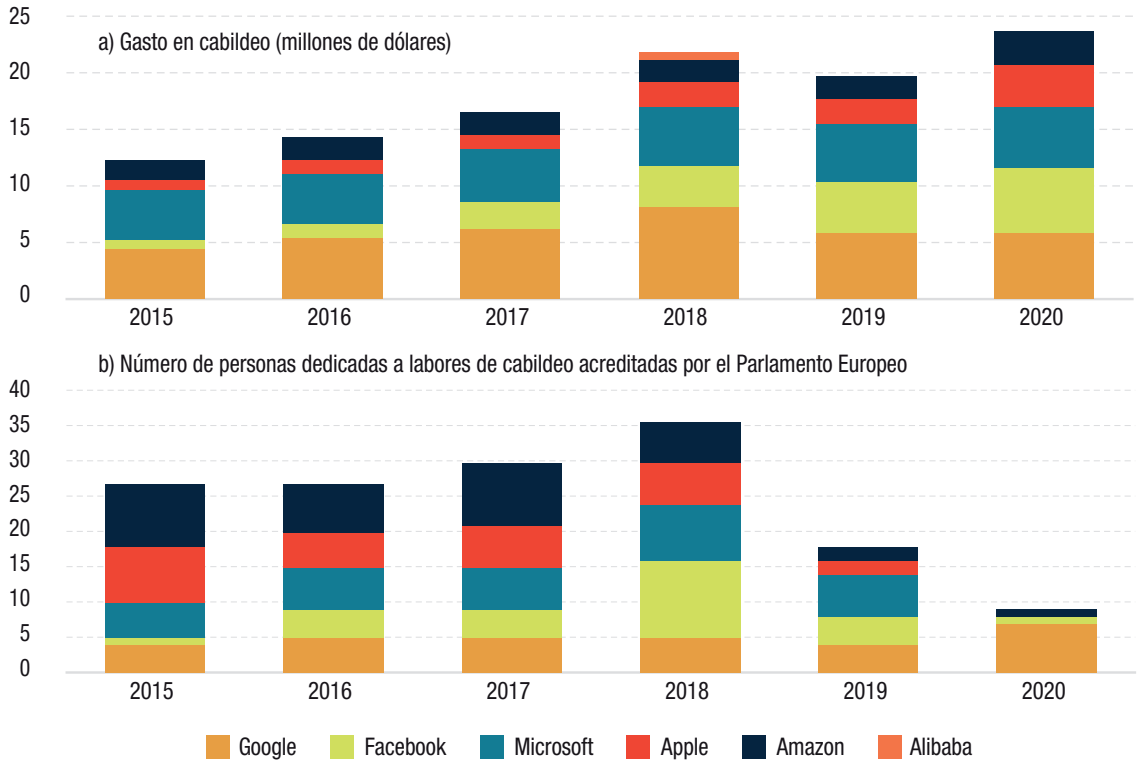
Las plataformas digitales globales de los Estados Unidos también ejercen bastante influencia en la Unión Europea. Aunque su gasto es menor en Bruselas que en Washington D. C., al 15 de abril de 2021 Google, Facebook (Facebook Ireland Limited) y Microsoft ocupaban, en ese orden, los tres primeros puestos de la lista de gasto en cabildeo de empresas y grupos en la Unión Europea; Apple y Amazon (Amazon Europe Core SARL) se encontraban entre los 20 y 30 primeros puestos, respectivamente, de esa misma lista[22].

Conjuntamente, esas empresas estadounidenses gastaron en 2015 más de 12 millones de dólares en actividades de cabildeo en la Unión Europea, y en 2020 casi duplicaron esa cifra, alcanzando 24 millones de dólares (figura I.20a). De las plataformas digitales chinas, solo Alibaba gastó en cabildeo en 2018, pero a un nivel menor que el de las empresas estadounidenses. El volumen del personal de cabildeo contratado por las plataformas digitales en la Unión Europea fue bastante menor que en los Estados Unidos (figura I.20b). No obstante, parece que en la Unión Europea también ejercen influencia financiando a algunos grupos de reflexión —organizaciones que pueden influir en las nuevas normativas mediante la publicación de estudios y documentos de posición y la organización de foros de debate—, aunque esas conexiones no suelen estar del todo claras[23]. El aumento de las actividades de cabildeo de las plataformas digitales globales en la Unión Europea es un signo evidente de su creciente poder, pero

[22] Véase la base de datos LobbyFacts, disponible en https://lobbyfacts.eu/reports/lobby-costs/all/0/2/2/2/21/0/2021-04-15.

[23] Véase Corporate Europe Observatory, "Big Tech Lobbying: Google, Amazon & friends and their hidden influence", disponible en: https://corporateeurope.org/en/2020/09/big-tech-lobbying.

Figura I.20. Cabildeo de las plataformas digitales globales en la Unión Europea, 2015-2020



Fuente: UNCTAD, a partir de la base de datos LobbyFacts, disponible en https://lobbyfacts.eu/about-lobbyfacts.
Nota: Esta base de datos no incluye información sobre Baidu ni sobre Tencent.

también de que están intentando prepararse para las políticas clave sobre tecnología que se avecinan en la Unión Europea y que podrían marcar el futuro de la industria.

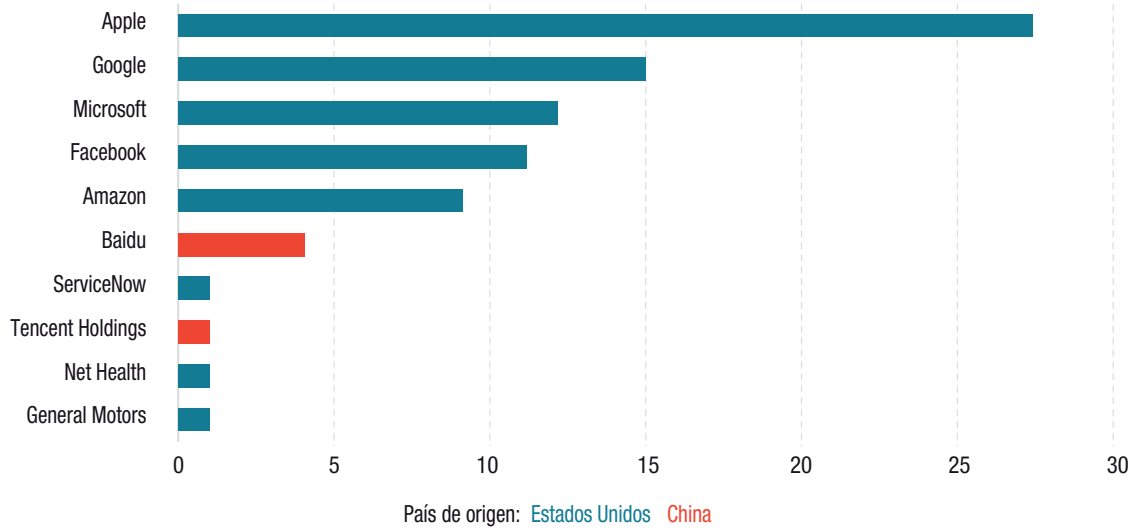
c) Inversión de las principales plataformas digitales en empresas emergentes de IA y en investigación y desarrollo en el ámbito de la IA

Las plataformas digitales también están aumentando su poder de mercado en la cadena de valor de los datos adquiriendo empresas emergentes e invirtiendo en su expansión horizontal y vertical (UNCTAD, 2019a). Aquellas que manejan cantidades masivas de datos son también las que han invertido cada vez más en IA, lo que a su vez las ayuda a utilizar los datos con eficacia, mejorar el servicio que ofrecen y atraer a nuevos usuarios (y conseguir así más datos). Además, esas plataformas digitales, y los países en los que tienen su sede, ocupan una mejor posición de liderazgo en el ámbito de la IA, así como en la gestión de datos globales, componente crucial de la economía digital actual y del crecimiento futuro en todas las industrias. Más adelante se analiza la situación de los avances en IA en distintos países.

En cuanto a las fusiones y adquisiciones de empresas emergentes del sector de la IA, entre el 1 de enero de 2016 y el 22 de enero de 2021 se produjeron 308 de esas operaciones, por valor de 28.400 millones de dólares. Como se muestra en la figura I.21, en la lista de plataformas digitales más importantes del mundo, por número de empresas emergentes de IA adquiridas en el período referido, los cinco primeros puestos correspondieron a grandes compañías tecnológicas estadounidenses, mientras que las plataformas digitales chinas Baidu y Tencent ocuparon los lugares sexto y octavo, respectivamente. Apple encabezó la lista, seguida de Google y Microsoft. Por el momento, parece que la competencia en el ámbito de la IA se basa exclusivamente en los beneficios esperados y en lograr el liderazgo a escala mundial.

Las grandes plataformas digitales que disfrutan de las ventajas derivadas de los datos están invirtiendo cada vez más en investigación y desarrollo en el ámbito de la IA, que se considera fundamental para poder beneficiarse en el futuro del procesamiento y el análisis de los datos. La investigación en IA se lleva a cabo principalmente en universidades, instituciones de investigación y empresas privadas. En el

Figura I.21 Las diez compañías líderes en adquisición de empresas emergentes de IA y su número de adquisiciones, 2016-2021



Fuente: UNCTAD, a partir de CBInsights, disponible en https://www.cbinsights.com (consultado el 22 de enero de 2021).

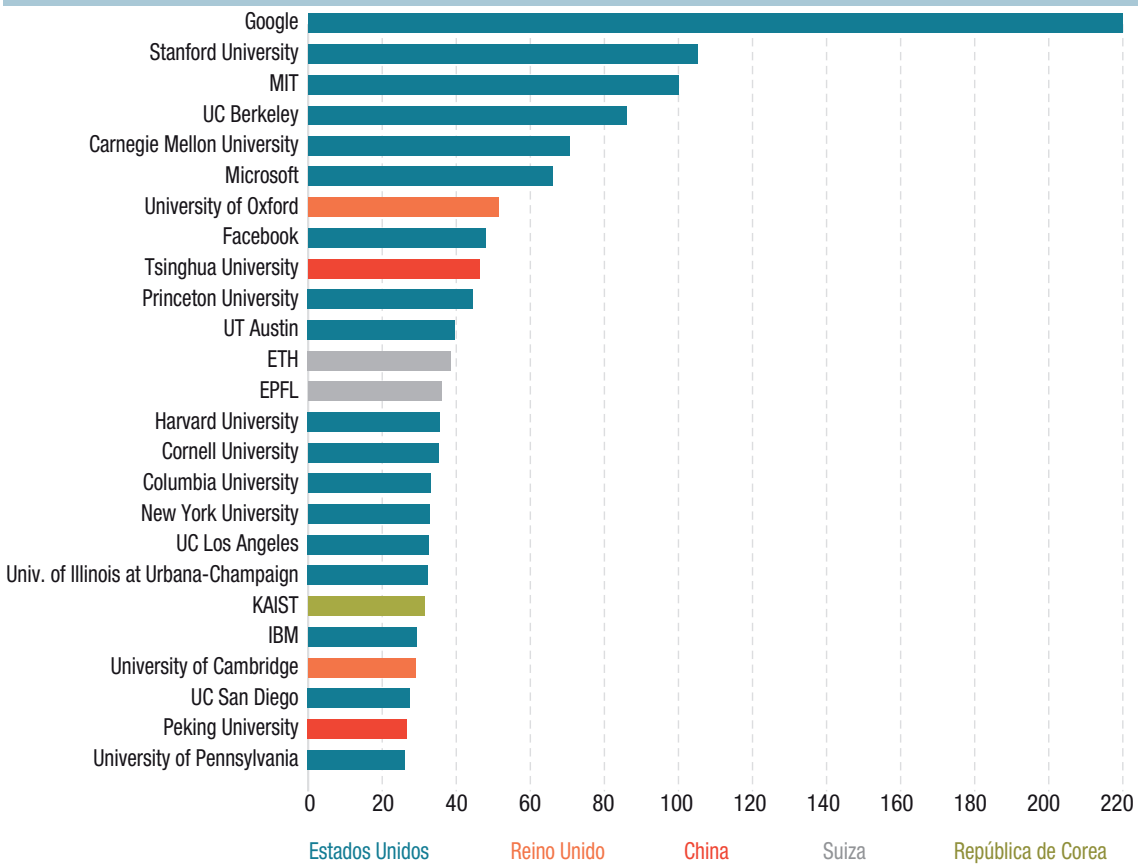
período 2000-2019, las empresas tecnológicas privadas aumentaron cada vez más su participación en las principales conferencias sobre IA (Zhang y otros, 2021) y llegaron a dominar en cuanto al número de trabajos presentados en las conferencias más prestigiosas. Como se muestra en la figura I.22, Google es, con diferencia, la institución de investigación en IA más importante. Microsoft y Facebook también se encuentran entre las diez primeras.

Las plataformas de los Estados Unidos y China tienen un acceso particularmente bueno al personal especializado y a las competencias necesarias para sacar partido a los datos y a la IA. La mayoría de las personas dedicadas a investigar en IA —el 59 %— trabajan en los Estados Unidos, mientras que China acoge al 11 %, y el 30 % restante se distribuye por el resto del mundo (figura I.23). En cuanto al origen de esas personas, el 29 % son de China y el 20 % de los Estados Unidos. Un buen porcentaje de ellas proceden también de la India y la República Islámica del Irán.

Alrededor de dos tercios de todas las personas que en el período 2016-2017 obtuvieron títulos de maestría o doctorado en el ámbito de la IA en los Estados Unidos eran extranjeras. Casi el 90 % de las personas extranjeras que terminaron su doctorado en los Estados Unidos en el período 2014-2018 y empezaron a trabajar se quedaron en el país (Zwetsloot y otros, 2019). Los resultados de Zhang y otros (2021) fueron muy parecidos: el 64,3 % de las personas que terminaron sus estudios de doctorado sobre IA en los Estados Unidos en 2019 eran extranjeras, y el 81,8 % de ellas se quedaron en el país.

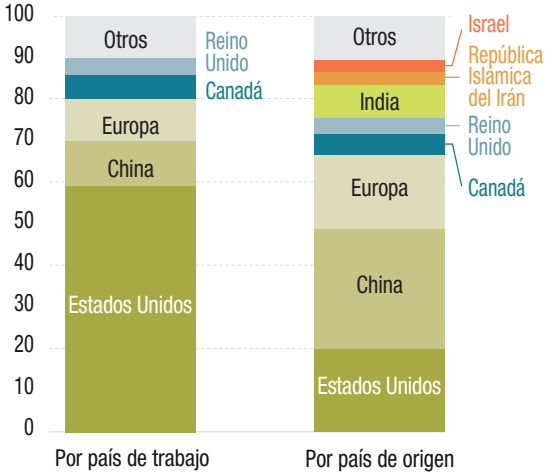
Una cuestión conexa es la salida profesional por la que se decantan las personas que cursan estudios sobre IA tras su graduación. Las entidades reguladoras del sector público tienden a quedarse a la zaga de las principales empresas privadas en lo que respecta a conocimientos técnicos sobre IA, ya que no consiguen atraer a los mejores profesionales. Según Zhang y otros (2021), el porcentaje de personas recién doctoradas en el ámbito de la IA que eligieron un trabajo en el sector aumentó del 44,4 % en 2010 al 65,7 % en 2019. Por el contrario, el porcentaje de esas personas que optaron por el mundo académico se redujo del 42,1 % en 2010 al 23,7 % en 2019. En cuanto al porcentaje restante en 2019 (el 10,6%), cabe suponer que se incorporaron al sector público o a organizaciones sin fines de lucro, o se dedicaron a otras actividades. Zwetsloot y otros (2019) investigaron con más detalle el mismo tema. Analizaron dos grupos de personas que se habían doctorado en los Estados Unidos en el ámbito de la IA, nacionales y extranjeras. Concluyeron que las primeras se dedicaban en su mayoría a trabajar en el sector privado o en el mundo académico, y que solo el 8 % se había incorporado al sector público o a organizaciones sin fines de lucro (figura I.24). Esa tendencia era más acentuada en el caso de las segundas, ya que la gran mayoría trabajaba en el sector privado (sobre todo en grandes empresas), y solo el 4 % en el sector público.

Figura I.22. Las 25 instituciones de investigación en IA más importantes
(Número de artículos publicados)



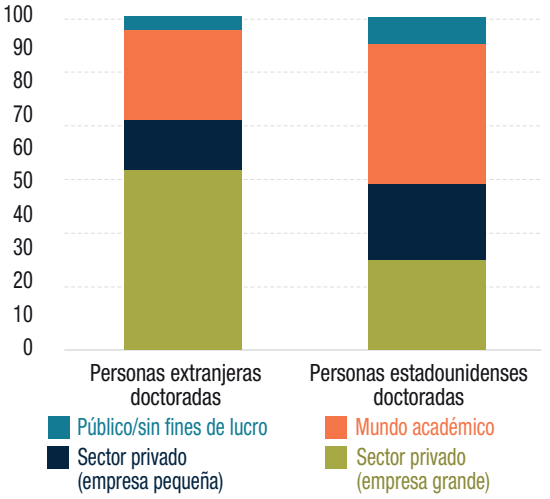
Fuente: UNCTAD, a partir de "AI Research Rankings 2020: Can the United States Stay Ahead of China?", disponible en https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.
Nota: Los datos se refieren a las ponencias aceptadas en las dos conferencias sobre investigación en IA más prestigiosas: International Conference on Machine Learning (ICML) y Conference on Neural Information Processing Systems (NeurIPS) (2020).

Figura I.23. Distribución geográfica de las personas investigadoras en IA, por país de trabajo y por país de origen, 2019
(Porcentaje)



Fuente: UNCTAD, a partir de "The Global AI Talent Tracker", disponible en https://macropolo.org/digital-projects/the-global-ai-talent-tracker/.

Figura I.24. Personas doctoradas en el ámbito de la IA que se quedan en los Estados Unidos y trabajan por primera vez, por sector, 2014-2018
(Porcentaje)



Fuente: UNCTAD, a partir de Zwetsloot y otros (2019).

El desarrollo de las perspectivas de carrera tampoco beneficia al sector público. En relación a las personas que se titularon en el curso académico 2014/15 y cambiaron de sector, de "aquellas que empiezan en empleos públicos o en organizaciones sin fines de lucro, casi el 75 % se pasa al sector privado o al mundo académico en un plazo de cuatro años. Alrededor del 20 % de las personas tituladas que empezaron en el mundo académico se cambiaron al sector privado, y el 10 % de las que empezaron en el sector privado recorrieron el camino a la inversa" (Zwetsloot y otros, 2019:13). También preocupa cada vez más que las personas dedicadas a investigar en IA abandonen el mundo académico y se incorporen al sector privado. Esa tendencia, debida a que en dicho sector hay una elevada demanda de personal de investigación en IA con conocimientos técnicos avanzados, puede dar lugar a una fuga de cerebros que reduzca la reserva de personas especializadas disponible para las investigaciones en IA de interés público (Jurowetzki y otros, 2021). Según Ahmed y Wahed (2020), la inequidad en la distribución de la potencia computacional en el mundo académico, o brecha computacional, está aumentando la desigualdad en la era del aprendizaje profundo. Las grandes empresas tecnológicas tienen más recursos para diseñar productos de IA, pero también suelen tener menos diversidad que las instituciones menos importantes o más pequeñas. Esto plantea problemas de sesgo y equidad en el ámbito de la IA.

Este desequilibrio —entre el sector privado, por un lado, y los sectores público y académico, por otro— en cuanto a la capacidad para atraer al personal más capacitado en el ámbito de la IA debería corregirse cuanto antes (es probable que en otras economías avanzadas y en China exista una brecha similar a la de los Estados Unidos). Si no se logra resolver esta cuestión, habrá consecuencias a largo plazo. Si las autoridades públicas no cuentan con una capacidad técnica suficiente en materia de IA, les resultará difícil, si no imposible, diseñar y aplicar normativas en unos mercados digitales que cambian rápidamente debido a los constantes avances innovadores en IA. En consecuencia, las plataformas digitales globales y otras empresas privadas estarán siempre por delante de las entidades reguladoras. Además, la probable fuga de cerebros del mundo académico hará que la investigación en IA esté sesgada hacia los métodos de esas empresas para alcanzar sus objetivos comerciales, lo que ya está suscitando preocupación en cuestiones como el uso de herramientas de vigilancia y sus consecuencias para la privacidad de las personas. Ahora bien, los desequilibrios en la atracción de especialistas en el ámbito de la IA al sector público no son los únicos que hay que resolver. Hay otros desequilibrios, por ejemplo, con respecto al género. En el recuadro I.3 se aborda el papel de las mujeres en la investigación sobre IA.

2. Internet de las cosas

La Internet de las cosas será probablemente la principal forma de recopilar datos en un futuro próximo, con los datos generados por miles de millones de dispositivos electrónicos conectados a Internet. Los datos pueden ser recopilados por medio de dispositivos conectados a Internet, como sensores, contadores, equipos de identificación por radiofrecuencia y otros elementos que pueden estar integrados en objetos utilizados cotidianamente y conectados a Internet. Debido a la creciente digitalización de la economía mundial, la cadena de valor de los datos se desarrolla en distintos países y se acelera debido al abaratamiento de los costos y a la facilidad de uso de tecnologías más sofisticadas, incluida la Internet de las cosas (Nguyen y Paczos, 2020). Por consiguiente, el uso cada vez mayor de la Internet de las cosas dará lugar a un aumento de los flujos de datos transfronterizos sin que sea necesario recurrir a la intervención humana (Voss, 2020).

La pandemia de COVID-19 ha puesto de manifiesto el destacado papel de la Internet de las cosas en nuestra vida. Algunas de las aplicaciones de la Internet de las cosas que han ayudado a combatir la pandemia mediante el suministro de datos esenciales son las cámaras térmicas conectadas, los dispositivos de rastreo de contactos y los dispositivos portátiles de control de la salud. Además, los sensores de temperatura y el seguimiento de paquetes han contribuido a garantizar la entrega segura de las delicadas vacunas contra la COVID-19. No obstante, el uso cada vez mayor de la Internet de las cosas también ha planteado problemas relacionados con la seguridad, la privacidad, la interoperabilidad y la equidad (WEF, 2020a), que deben abordarse mediante una gobernanza adecuada.

El mercado mundial de la Internet de las cosas alcanzó 308.970 millones de dólares en 2020. Se prevé que pase de 381.300 millones de dólares en 2021 a 1,85 billones de dólares en 2028, lo que representa una

Recuadro I.3. Mujeres dedicadas a la investigación en IA

Existe una considerable brecha de género en el personal dedicado al ámbito de la IA, tanto en el sector académico como en el empresarial, y en todos los países con actividad en dicho ámbito.

En el mundo académico, hay muchos más hombres que mujeres entre los estudiantes de doctorado en IA. Según el informe de 2021 del AI Index de la Universidad de Stanford (Zhang y otros, 2021), en el período 2010-2019, de todas las personas doctoradas en IA y ciencias de la computación en América del Norte, solo el 18,3 % eran mujeres. Otro indicador indirecto de la brecha de género es el hecho de que en una de las conferencias anuales de IA más prestigiosas (Neural Information Proccessign Systems), entre 2016 y 2019, solo un 10 % (en promedio) de las personas asistentes al taller dedicado específicamente a la participación de las mujeres en el aprendizaje automático (Women in Machine Learning) eran mujeres.

Según otro estudio sobre las 21 principales conferencias académicas de IA en 2018, solo el 18 % de las personas que presentaron trabajos en dichas conferencias eran mujeres, y, en cuanto a su sector laboral de origen, el 19 % de las autoras procedían del mundo académico y el 16 % del sector privado. Si se comparan los países, algunas economías están prestando más atención a esta cuestión que otras, pero los porcentajes siguen estando muy lejos de corresponder a una situación de equilibrio de género. En la lista de países con los mejores porcentajes figuran España (26 %), la Provincia China de Taiwán (23 %) y Singapur (23 %). Los tres países con mayor número absoluto de mujeres investigadoras en IA tienen los siguientes porcentajes de autoras de trabajos: Estados Unidos (20 %), China (22 %) y Reino Unido (18 %) (Gagné y otros, 2019). Con una metodología de cálculo diferente, se estimó que en 2020 el porcentaje de mujeres autoras de publicaciones sobre IA era del 15 % (Gagné y otros, 2020).

En Google, líder en publicaciones en las dos conferencias más prestigiosas de IA, las autoras representaban solo el 10 % de todo el personal de investigación en IA (Chin, 2018). La cuestión de la brecha de género en el desarrollo y la implantación de la tecnología de IA es importante debido al impacto potencial del aprendizaje automático en toda la población, probablemente la más importante de todas las tecnologías actuales para el futuro de nuestras sociedades.

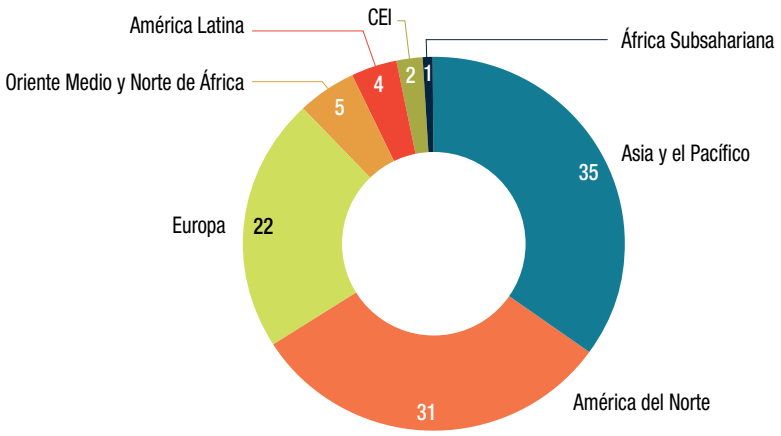
Fuente: UNCTAD.

tasa de crecimiento anual compuesta del 25,4 % en ese período (Fortune Business Insights, 2021). Según IDC (2020a), si bien el gasto mundial en la Internet de las cosas se ha visto afectado negativamente por la pandemia, se prevé una vuelta al crecimiento de dos dígitos (por encima del 10 %) a medio y largo plazo y una tasa de crecimiento anual compuesta del 11,3 % durante el período 2020-2024. Las tres cuartas partes del gasto total en la Internet de las cosas corresponderán a China, los Estados Unidos y Europa Occidental. Aunque en un principio tendrán totales de gasto similares, el gasto de China crecerá más rápidamente que el de las otras dos regiones (un 13,4 % de tasa de crecimiento anual, frente a un 9 % y un 11,4 %, respectivamente), lo que la convertirá en el país con mayor gasto en la Internet de las cosas. Las tasas mayores de crecimiento anual del gasto en la Internet de las cosas se registrarán en las regiones de Oriente Medio y Norte de África (19 %), Europa Central y Oriental (17,6 %) y América Latina (15,8 %).

En 2020, por primera vez, había más conexiones de la Internet de las cosas (por ejemplo, coches conectados, dispositivos domésticos inteligentes y equipos industriales conectados) que conexiones de otro tipo (teléfonos inteligentes, computadoras portátiles, tabletas y computadoras). Para 2025 se espera que haya una media de casi cuatro dispositivos de la Internet de las cosas por persona[24]. GSMA (2019a) estima que el número total de conexiones de la Internet de las cosas aumentará de 9.100 millones en 2018 a 25.200 millones en 2025, lo que representará una oportunidad de ingresar 1,1 billones de dólares en 2025. Sin embargo, como se muestra en la figura I.25, esos ingresos no se distribuirán geográficamente de forma equitativa. Se prevé que los ingresos de África Subsahariana, la CEI y América Latina representarán solo el 7 % de los ingresos totales.

[24] Véase *IoT Analytics*, 19 de noviembre de 2020, "State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time", disponible en https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

Figura I.25. Distribución geográfica de los ingresos de la Internet de las cosas para 2025
(Porcentaje)



Fuente: UNCTAD, cálculos basados en GSMA (2019a).
Nota: Los grupos de países son los establecidos por la fuente.

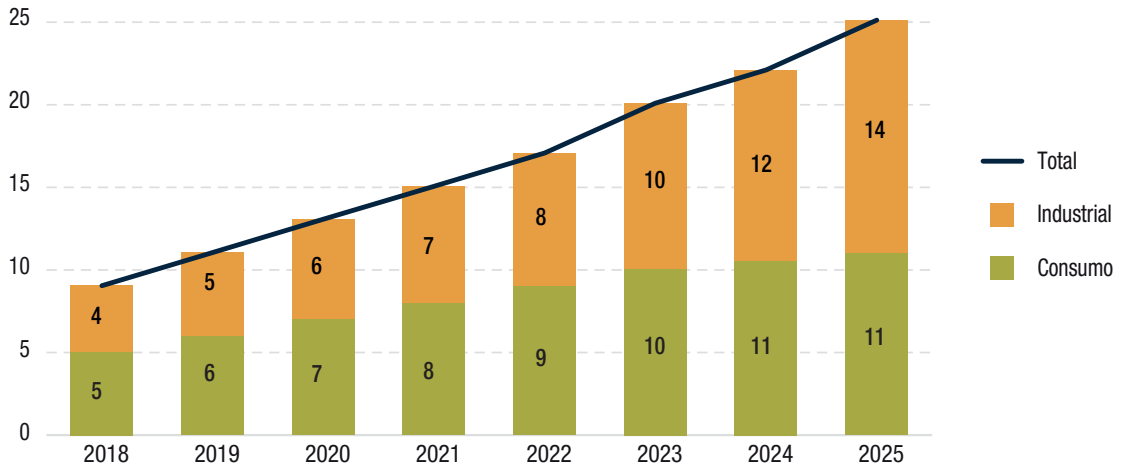
Se estima que en 2018 los beneficios de productividad para las empresas que usaban la Internet de las cosas reportaron a la economía mundial unos 175.000 millones de dólares, lo que representa el 0,2 % del PIB mundial. Más de la mitad de esos beneficios correspondieron a empresas de producción, que son, por tanto, el sector que más se beneficia del uso de la Internet de las cosas. Se espera que los beneficios de productividad derivados del uso de la Internet de las cosas por las empresas asciendan a 3,7 billones de dólares en 2025, lo que supondría el 0,34 % del PIB mundial. Los Estados Unidos y China son los países con mayores ganancias de productividad derivadas de la Internet de las cosas, que representan más del 50 % de los beneficios mundiales (GSMA, 2019b).

En cuanto a los sectores, para 2025, más de la mitad de los posibles ingresos totales provendrán de la industria conectada, seguida de los hogares inteligentes con un 23 % de los ingresos totales. El 15 % corresponderá a la electrónica de consumo, el 5 % a los vehículos conectados y el 4 % a las ciudades inteligentes (GSMA, 2019a). Las conexiones de la Internet de las cosas que más crecerán a escala global son las industriales, a una tasa media anual del 21 % entre 2017 y 2025 (figura I.26), y, como resultado de ese importante crecimiento, en 2025 representarán más de la mitad de las conexiones de la Internet de las cosas en todo el mundo. En consecuencia, se producirá un cambio significativo en la forma de trabajar de las industrias.

IDC (2020b) estima que los datos generados por los dispositivos de la Internet de las cosas conectados pasarán de 18,3 *zettabytes* en 2019 a 73,1 *zettabytes* en 2025. La mayor parte de esos datos procederán de la seguridad y la videovigilancia, aunque las aplicaciones industriales de la Internet de las cosas también generarán una parte importante. El aumento global de los datos derivados de la Internet de las cosas conllevará un incremento de los flujos de datos transfronterizos, ya que los distintos dispositivos conectados pueden estar en cualquier parte del mundo. Si bien hasta ahora los estudios sobre la relación entre el desarrollo de la Internet de las cosas y los flujos de datos transfronterizos son escasos, no parece haber duda de que la Internet de las cosas conducirá a un aumento de esos flujos. En un estudio que abarca el Brasil, Indonesia y Sudáfrica, GSMA (2021) concluye que las economías emergentes podrían conseguir importantes ganancias con la utilización de la Internet de las cosas. La libre circulación de los datos a través de las fronteras podría influir considerablemente en la producción económica, con un aumento de:

- El PIB: de hasta un 0,5 % en el Brasil, hasta un 0,9 % en Indonesia y hasta un 2,6 % en Sudáfrica.
- Las exportaciones: de hasta un 2,4 % en el Brasil, hasta un 2,9 % en Indonesia y hasta un 3,1 % en Sudáfrica.
- El empleo: de hasta un 0,2 % en el Brasil, hasta un 0,4 % en Indonesia y hasta un 1,3 % en Sudáfrica.

Figura I.26. Número de conexiones de la Internet de las cosas en el mundo, por sector, 2018-2025



Fuente: GSMA (2019b).

En cambio, la imposición de restricciones a los flujos de datos transfronterizos reduciría los beneficios económicos (medidos por el PIB) derivados de la Internet de las cosas en un 59 % en el Brasil, un 61 % en Indonesia y un 68 % en Sudáfrica.

Algunas de las principales plataformas digitales globales, como Alphabet (incluido Google), Amazon y Microsoft, son también importantes proveedoras de servicios de la Internet de las cosas (UNCTAD, 2021d), lo que les permite reforzar las ventajas en materia de datos de las que disfrutan. Lo anterior, junto con el hecho de que a África y a América Latina les corresponda un porcentaje mínimo de los ingresos previstos derivados de la Internet de las cosas, apunta a que esta red contribuirá a aumentar los desequilibrios existentes como lo hacen la mayoría de las tecnologías digitales. Se necesitarán medidas políticas para corregir las desigualdades resultantes, incluida una distribución equitativa de los beneficios derivados de los flujos de datos transfronterizos generados.

La utilización de las tecnologías de la Internet de las cosas suscita cada vez más preocupación en relación con la privacidad y la seguridad, dado que permiten una recopilación y un consumo de datos mucho más elevados. Como se analizará en el presente Informe, esa preocupación es aún mayor en el caso de los flujos de datos transfronterizos, ya que se pueden transferir datos sensibles a un país cuya jurisdicción quizá no aplique las mismas normas de protección de datos que el país donde se recopilaron. El Foro Económico Mundial, en su análisis de la situación de la gobernanza de la Internet de las cosas (WEF, 2020a: 65–66), concluye que "los numerosos riesgos inherentes a la Internet de las cosas aún no se han eliminado eficazmente y la gobernanza de la Internet de las cosas no está madura. Al mismo tiempo, sin embargo, las medidas para tratar de reducir esos riesgos pueden conducir, en algunos casos, a una regulación inadecuada, que a su vez puede poner en peligro el valor y la eficacia de muchos de los tipos de aplicaciones de la Internet de las cosas. La cuestión del intercambio transfronterizo de datos es un ejemplo de ello […]. A pesar de la importancia de regular el uso de los numerosos tipos de aplicaciones de la Internet de las cosas, la normativa sobre privacidad y ciberseguridad sigue estando fragmentada a escala mundial".

El desarrollo de la Internet de las cosas va en paralelo al de la implantación de las tecnologías 5G, que se analiza en la siguiente sección.

H. TRANSMISIÓN Y ALMACENAMIENTO DE DATOS

El hecho de que los datos sean intangibles no significa que sean entidades etéreas. Necesitan de un soporte físico, se transmiten a través de infraestructuras físicas y se almacenan en ellas. En esta sección se analiza en primer lugar la tecnología 5G como desarrollo clave de la conexión de último tramo para el

usuario final. A continuación, se describe el papel de los cables submarinos y el potencial de los satélites para la conexión de larga distancia (red troncal o *backbone*) como principales canales de transmisión de datos. Por último, se señala la importancia de los puntos de intercambio de tráfico de Internet (IXP) para la conexión de redes y el intercambio local de tráfico de Internet, así como del mercado de la computación en la nube y los centros de datos para el almacenamiento de datos. Las plataformas digitales globales también están ampliando su participación en muchos de esos ámbitos.

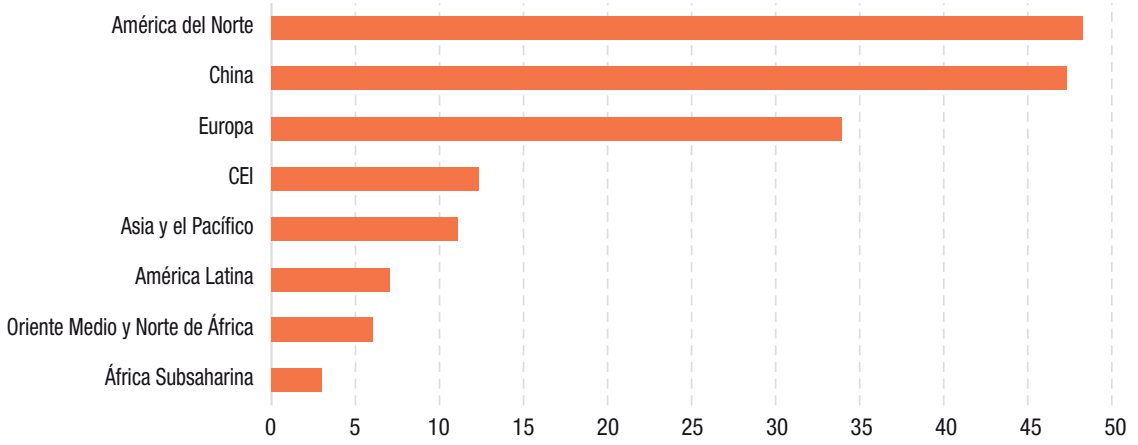
1. Banda ancha móvil 5G

La mejora y la implantación de las tecnologías inalámbricas 5G son clave para el desarrollo de la Internet de las cosas, puesto que permiten manejar cantidades ingentes de datos en comparación con las tecnologías de generaciones anteriores. Se prevé que las tecnologías 5G revolucionarán el mundo de las redes móviles mediante velocidades ultrarrápidas y supondrán el fin de la congestión, dado que reducirán significativamente el tiempo de espera o latencia.

La tecnología 5G comenzó a comercializarse en 2020. Sin embargo, se está implantando principalmente en países desarrollados y en algunos países de Asia, sobre todo en China. No se prevén muchos cambios al respecto de aquí a 2025 (figura I.27). Se espera que el tráfico de datos móviles de la tecnología 5G supere al de la tecnología 4G y anteriores en 2026 (figura I.28). Aunque América del Norte y Europa tienen un porcentaje menor de suscripciones de servicios móviles 5G con respecto al resto del mundo, su porcentaje de consumo de datos es mayor debido a la eficiencia de sus redes, a los dispositivos de alta gama que utilizan y a los paquetes grandes y asequibles de datos[25].

Además, se espera que la tecnología 5G mejore la utilización de los dispositivos móviles en cuanto a la calidad de la conexión a Internet y el aumento del volumen de datos. A escala mundial, se acelerará la tendencia a sustituir las computadoras de escritorio (banda ancha fija) por dispositivos móviles, principalmente para las compras en línea, los vídeos y los juegos. Las aplicaciones de mensajería y redes sociales, cuyo uso en los teléfonos inteligentes ya está muy extendido, se beneficiarán asimismo de la tecnología 5G, que también repercutirá en los servicios en la nube. Todo ello supondrá un aumento de las transferencias transfronterizas de datos. Debido a la gran cantidad de datos que permite manejar, así como a su posible impacto económico, la tecnología 5G es un elemento crucial en los conflictos tecnológico-comerciales entre los Estados Unidos y China, en cuyo primer plano se encuentra la empresa china Huawei, líder en el desarrollo de dicha tecnología.

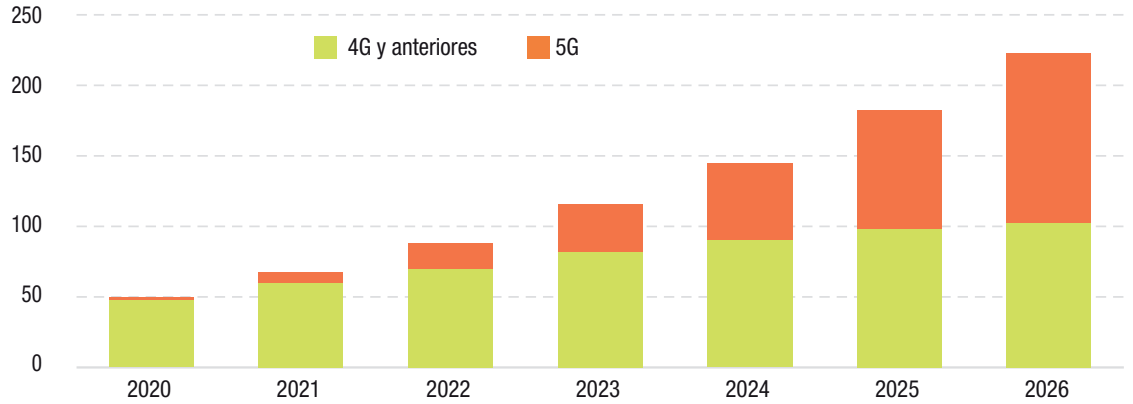
Figura I.27. Adopción de la tecnología 5G, por región, 2025
(Porcentaje del total de conexiones)



Fuente: UNCTAD, cálculos basados en GSMA (2020a).
Nota: Los grupos de países son los establecidos por la fuente.

[25] Véase Ericsson Visualizer, disponible en www.ericsson.com/en/mobility-report/mobility-visualizer?f=8&ft=2&r=1&t=1,20&s=4&u=3&y=2020,2026&c=3 (consultado en abril de 2021).

Figura I.28. Previsiones del tráfico mundial de datos móviles, por tecnología, 2020-2026
(*Exabytes* por mes)



Fuente: UNCTAD, a partir de Ericsson Visualizer, disponible en www.ericsson.com/en/mobility-report/mobility-visualizer?f=8&ft=2&r=1&t=1,20&s=4&u=3&y=2020,2026&c=3 (consultado en abril de 2021).

2. Cables submarinos

Se calcula que alrededor del 99 % del tráfico internacional de datos se realiza por cables submarinos (ITIF, 2019). La ventaja que tienen esos cables frente a otros canales, como los satélites (que se analizarán más adelante), es que pueden transmitir muchos más datos a un costo mucho menor[26].

En la figura I.29 se muestran las conexiones por cable submarino y se incluyen también rutas terrestres de transmisión. El mapa interactivo de transmisión terrestre desarrollado por la UIT permite conocer la conectividad de las redes troncales nacionales (fibras ópticas, microondas y estaciones terrenas de satélite), así como otros parámetros clave relativos a las TIC[27].

En cuanto a las rutas interregionales, en el mapa se observa que la red de cables submarinos es más densa en la ruta transatlántica del norte y en las rutas transpacíficas (entre los Estados Unidos y Europa y entre los Estados Unidos y Asia, respectivamente). También se observa que la red de conexiones intrarregionales es más densa en Europa, Asia Oriental y Asia Meridional. En África y América Latina la red es menos densa, tanto en términos de conexiones intercontinentales como de conexiones intrarregionales, y en ambas regiones quedan zonas extensas sin Internet.

Las empresas que más ancho de banda internacional utilizan son también las que más invierten en cables. Entre ellas figuran proveedores de contenidos como Google, Facebook, Amazon y Microsoft, pero también compañías operadoras en telecomunicaciones como Telxius, China Telecom y Telstra[28]. Según TeleGeography, "a diferencia de en anteriores etapas de auge de la construcción de cables submarinos, en esta última etapa de explosión los proveedores de contenidos, como Amazon, Google, Facebook y Microsoft, están desempeñando un papel más activo. Estas empresas demandan tanto tráfico de los centros de datos que son las que impulsan proyectos y la priorización de determinadas rutas de cables submarinos"[29]. En la figura I.30 se observa esa tendencia mediante la representación del porcentaje de

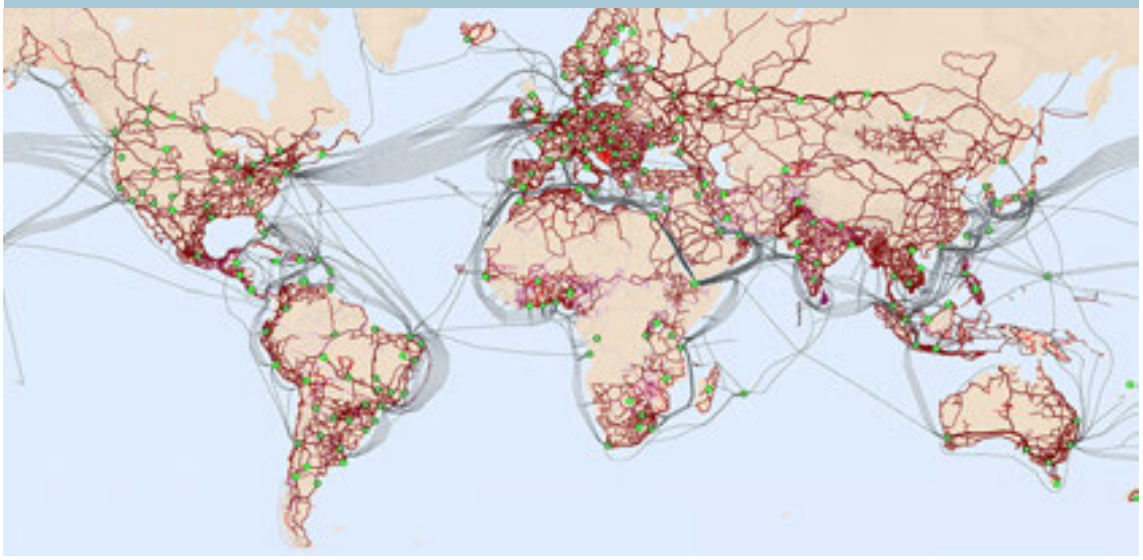
[26] Véase Submarine Cable FAQs, disponible en www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

[27] Se pueden consultar mapas más detallados de los cables submarinos en Global Internet Map 2021, disponible en https://global-internet-map-2021.telegeography.com/; y en Platform DIGITAL, disponible en https://go2.digitalrealty.com/rs/087-YZJ-646/ images/Map_Digital_Realty_2010_Platform_DIGITAL_Global_Map.pdf?_ga=2.119330761.1552758197.1613555008584212833.1613555008.

[28] Véase TeleGeography, 8 de octubre de 2019, "Is Your Planned Submarine Cable Doomed?", disponible en https://blog.telegeography.com/is-your-planned-submarine-cable-doomed.

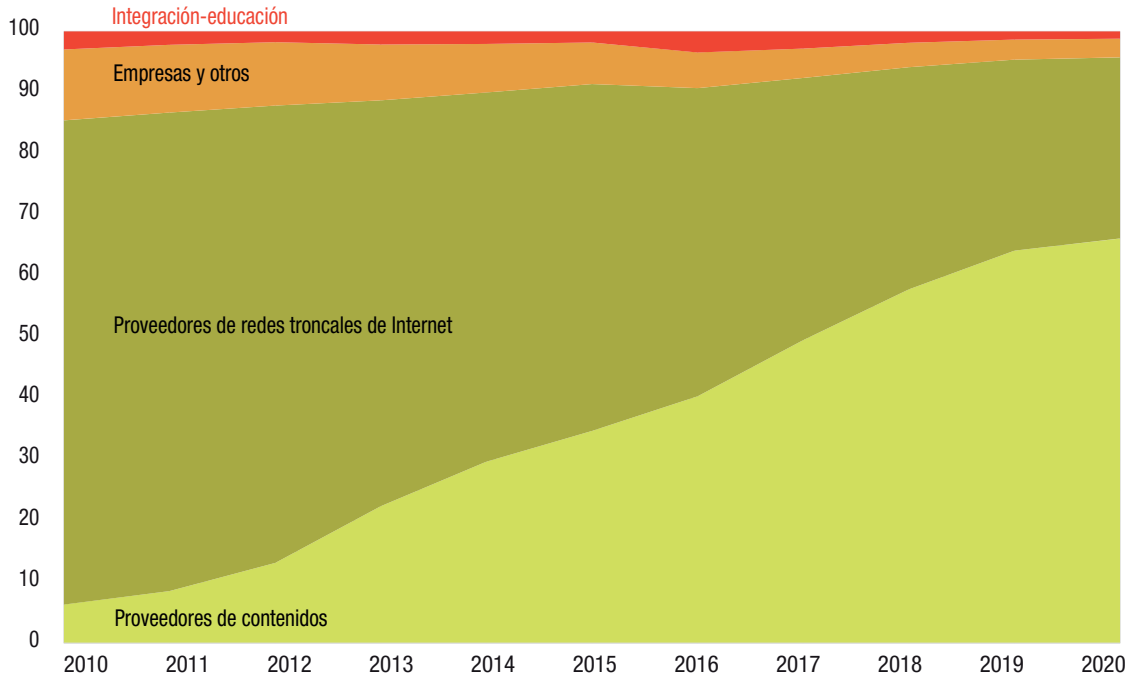
[29] Véase TeleGeography, 9 de noviembre de 2019, "A Complete List of Content Providers' Submarine Cable Holdings", disponible en https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list.

Figura I.29. Mapa de transmisiones de Internet, junio de 2021



Fuente: UNCTAD, a partir del mapa interactivo de transmisiones desarrollado por la UIT, disponible en www.itu.int/itu-d/tnd-map-public/.

Figura I.30. Ancho de banda internacional utilizado a escala mundial, por tipo de proveedor, 2010-2020
(Porcentaje)



Fuente: UNCTAD, cálculos basados en TeleGeography.

uso de ancho de banda internacional por cada tipo de proveedor[30]. Como ya se ha señalado en este capítulo, se estima que el 80 % del tráfico total de Internet corresponde a los servicios de vídeo, redes sociales y juegos, que son proporcionados en gran medida por las principales plataformas digitales, como YouTube (Google), Netflix y Facebook.

[30] Para más información sobre la situación de la industria de cables submarinos, véase "Submarine Telecoms Industry Report 2020/2021", disponible en https://subtelforum.com/products/submarine-telecoms-industry-report/.

3. Satélites

Los satélites son útiles para proporcionar cobertura a zonas remotas a las que no llega la fibra. IDC (2021b) analiza la situación de la conexión por satélite de nueva generación y cómo dará lugar a nuevos usos de la conectividad, no solo en lugares remotos, sino también en ciudades, suburbios y pueblos. Concluye que el borde operativo, el borde táctico y el borde de empresas y administraciones públicas (oficinas remotas) recibirán un gran impulso en términos de conectividad y funcionalidad si se logra conectar los dispositivos 5G con los satélites. La conexión de las redes 5G con los satélites permitirá desarrollar importantes aplicaciones para el transporte comercial y militar, la agricultura, las industrias del petróleo, el gas y la minería, y los servicios públicos, así como la conectividad de banda ancha en zonas residenciales remotas.

Grandes empresas como SpaceX y Amazon han realizado cuantiosas inversiones en banda ancha rápida por satélite. Cada una de esas dos empresas tiene previsto gastar aproximadamente 10.000 millones de dólares[31]. Con ello pretenden llevar la banda ancha a lugares remotos sin ese servicio, ayudar en las actividades de los centros educativos y de las administraciones públicas en el extranjero, o facilitar el acceso a Internet en regiones afectadas por catástrofes naturales o conflictos. Otra de las principales razones por las que realizan esas inversiones es la posibilidad de mejorar el acceso a los datos de un mayor número de internautas y, con ello, generar más ingresos. La rentabilidad de la inversión puede ser considerable. Morgan Stanley (2020) estima que "la industria espacial mundial podría generar unos ingresos de [...] 1 billón de dólares o más en 2040, frente a los 350.000 millones de dólares que aporta en la actualidad. Sin embargo, las oportunidades más importantes a corto y medio plazo pueden provenir del acceso a Internet de banda ancha por satélite [...]. El 50 % del crecimiento previsto de la economía espacial mundial de aquí a 2040 —y hasta el 70 % en la previsión más optimista— corresponderá al servicio de banda ancha por satélite. La puesta en órbita de satélites para suministrar Internet de banda ancha contribuirá a reducir el costo de los datos, justo cuando la demanda de los mismos se está disparando".

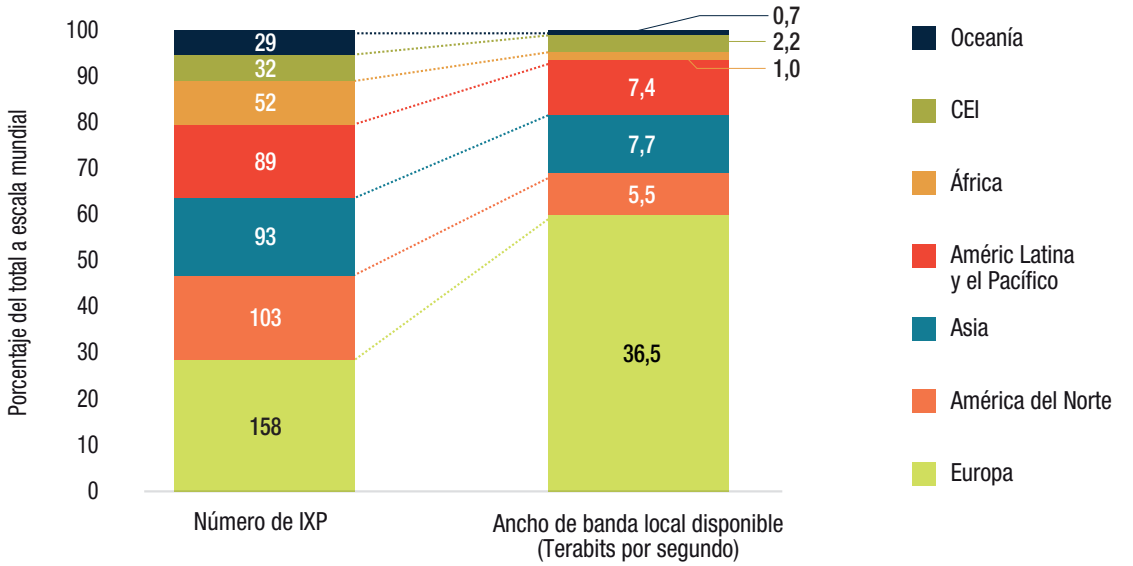
4. Puntos de intercambio de tráfico de Internet

El desarrollo de la infraestructura de Internet relacionada con los datos en cada país es tan importante para el funcionamiento de Internet como la calidad de la conectividad y la cobertura de Internet, con el fin de que cada vez más personas y empresas participen en la economía digital impulsada por los datos. Dicha infraestructura incluye los puntos de intercambio de tráfico de Internet (IXP) y los centros de datos coubicados. Los IXP son lugares donde se conectan diferentes redes para intercambiar tráfico de Internet a través de infraestructuras de conmutación compartidas. Las redes que convergen en los IXP pueden ser de proveedores de servicios de Internet, proveedores de contenidos, empresas de alojamiento web o administraciones públicas, entre otras entidades. Los IXP están distribuidos en diferentes países, lo que permite que las redes locales intercambien información de forma eficaz, ya que hacen innecesario el envío del tráfico local de Internet al extranjero. Se ha demostrado que las velocidades de acceso a los contenidos locales pueden mejorar hasta diez veces con un IXP, ya que el tráfico se enruta de forma más directa (Internet Society, 2015).

Hasta abril de 2021 había 556 IXP en el mundo; la mayoría de ellos (293) estaban en economías desarrolladas, mientras que había 220 y 43 en economías en desarrollo y economías en transición, respectivamente. El número medio de IXP por país era de 7,9, 3,9 y 2,6 en las economías desarrolladas, las economías en transición y las economías en desarrollo, respectivamente. Las regiones con mayor número de IXP eran Europa, seguida de América del Norte y de Asia (figura I.31). En cuanto al volumen del tráfico de datos que pasaba por esos IXP regionales, Europa, con el 28 % de todos los IXP, estaba también a la cabeza, además de registrar el mayor ancho de banda local del mundo (el 60 % del total). Esto se debe en parte a que hay varios IXP que funcionan como concentradores *(hubs)* intercontinentales en Europa. África tenía el 9 % de todos los IXP, pero su ancho de banda local representaba solo el 2 % del total.

[31] Véase *Reuters*, 30 de julio de 2020, "Taking on SpaceX, Amazon to invest $10 billion in satellite broadband plan".

Figura I.31. Puntos de intercambio de tráfico de Internet, número de IXP y ancho de banda disponible a través de los IXP, por región, abril de 2021



Fuente: UNCTAD, cálculos basados en la base de datos Packet Clearing House, disponible en https://www.pch.net/ixp/dir/summary_growth_by_country (consultado en abril de 2021).

El hecho de contar con un IXP no siempre puede garantizar más beneficios a los clientes locales. Por ejemplo, en Djibouti hay un IXP que actúa como concentrador regional que presta servicios a los países vecinos y, sin embargo, la estructura monopolística de su sector de las telecomunicaciones hace que las tarifas de Internet sean desorbitadas (World Bank, 2021). Por consiguiente, que en un país haya un IXP o un mayor volumen de datos intercambiados a través de él no conlleva necesariamente velocidades de Internet más rápidas ni tarifas de conexión más bajas a escala local. En cambio, un IXP destinado a asociados nacionales, internacionales y diversos, que ofrezca las mismas condiciones a todas las partes (a menudo competidoras), puede fomentar el intercambio de datos entre sus redes. Sin embargo, la mayoría de los países en desarrollo carecen de la infraestructura necesaria para intercambiar a través de IXP los datos generados localmente —pese a que el material para establecer un IXP no es caro (Internet Society, 2015)—, almacenarlos en centros de datos coubicados y procesarlos en plataformas ubicadas en la nube (World Bank, 2021). En la siguiente subsección se describe la situación a escala mundial de los centros de datos coubicados y los mercados de la computación en la nube.

5. Mercados de la computación en la nube y centros de datos

La computación en la nube permite prestar servicios informáticos a través de Internet, de modo que las empresas pueden acceder más rápido a procesos de innovación y recursos flexibles y beneficiarse de las economías de escala, al tiempo que almacenan sus datos a un costo mucho menor. Gartner (2019) estima que, para 2025, el 80 % de las empresas habrán cerrado sus centros de datos ordinarios (el 10 % ya lo hizo en 2019) y, en su lugar, recurrirán a centros de datos coubicados y a centros de datos de hiperescala.

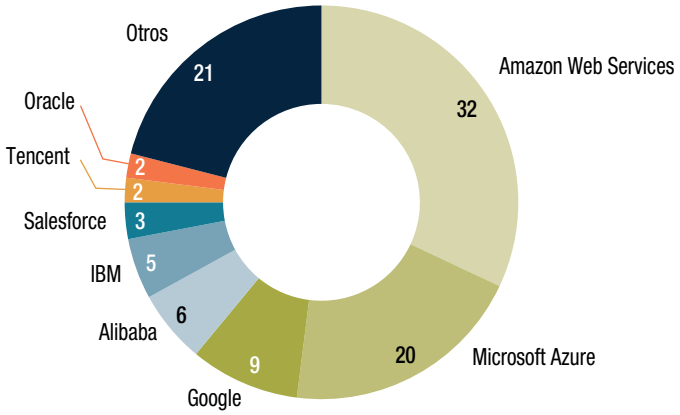
La mayoría de los centros de datos coubicados están en países desarrollados. En enero de 2021, de un total de 4.714 centros de datos coubicados, casi el 80 % estaban en países desarrollados, principalmente en América del Norte y Europa. Solo 897 se encontraban en países en desarrollo, sobre todo en Asia, y 119 en economías en transición. África y América Latina tenían, respectivamente, 69 y 153 de esos centros de datos. Conviene señalar que, a pesar de que la UE-27 y el Reino Unido contaban, respectivamente, con 1.105 y 273 centros de datos coubicados (frente a los 1.796 de los Estados Unidos y los 154 de China), Europa no ha sido capaz de aprovechar los beneficios de los datos en la medida en que lo han

hecho los Estados Unidos y China, lo que indica que para tener una economía de datos exitosa hace falta algo más que invertir en centros de datos[32].

En el caso de los centros de datos de hiperescala[33], a finales de 2020, la mayoría de ellos —el 39 % de los 597 que había en total— estaban en los Estados Unidos, el 10 % en China y el 6 % en el Japón. El número total de centros de datos de hiperescala ha aumentado más del doble desde 2015, y más de la mitad de ellos son gestionados por Amazon, Microsoft y Google. Amazon y Google fueron los que más centros de datos abrieron en 2020: la mitad de todos los nuevos (Synergy Research Group, 2021a). Como se muestra en la figura I.32, el 52 % del total de los ingresos por servicios de infraestructura en la nube correspondió a dos empresas estadounidenses (Amazon y Microsoft).

El análisis y el uso de los datos, a través sobre todo de los centros de datos, pueden ser muy útiles para alcanzar objetivos de sostenibilidad, incluida la lucha contra el cambio climático. Ahora bien, la economía digital, y en particular los centros de datos, tienen un impacto ambiental que ha de tenerse en cuenta (véase el recuadro I.4). La ubicación de los centros de datos puede obedecer a criterios ambientales (por ejemplo, en los países de clima templado se ahorra energía en la refrigeración de las infraestructuras), pero también se basa en otros factores, como la fiabilidad de las infraestructuras energéticas locales y el costo de su utilización (véase el capítulo III). La ubicación de los centros de datos es una cuestión clave en relación con los flujos de datos transfronterizos. Como se analizará en detalle en el capítulo IV, los requisitos de emplazamiento de los centros de almacenamiento de datos en un territorio concreto repercuten en la regulación de los flujos de datos transfronterizos. El crecimiento de la Internet de las cosas y la adopción de la tecnología 5G pueden suponer una transformación del mercado de los centros de datos de modo que se pase de un predominio de los centros de datos de hiperescala a los denominados “centros de datos de borde”, por cuanto los requerimientos de latencia en la transmisión de datos exigirán que los centros de datos se encuentren más cerca de donde se generan los datos[34]. Hay indicios de que se está avanzando hacia un sistema multinube que combine diferentes tipos de centros de datos.

Figura I.32. Ingresos por servicios de infraestructura en la nube, por proveedor, Q4 de 2020
(Cuota de mercado en porcentaje)



Fuente: UNCTAD, a partir de Synergy Research Group (2021b) y Statista (2021).

[32] Cálculos de la UNCTAD, a partir de la base de datos de Data Center Map, disponible en www.datacentermap.com/datacenters.html (consultado en enero de 2021).

[33] Según Equinix (2020): “Un centro de datos de hiperescala es un tipo de centro de coubicación a gran escala diseñado según los requisitos técnicos, operativos y tarifarios de las empresas de hiperescala, como Amazon, Alibaba, Facebook, Google, IBM, Microsoft y algunas otras. Estos ‘hiperescaladores’ requieren enormes cantidades de espacio y energía para hacer posible el procesamiento masivo en miles de servidores de tareas en la nube, tareas de análisis de macrodatos o tareas de almacenamiento”.

[34] Véase CBInsights, 11 de marzo de 2021, “What is edge computing?”, disponible en www.cbinsights.com/research/what-is-edgecomputing/.

Recuadro I.4. Consumo energético de los centros de datos y las redes de transmisión de datos

La infraestructura y el consumo energéticos son factores críticos para la economía digital impulsada por los datos. Según The Shift Project (2019:16), el consumo energético asociado a la economía digital en relación con el consumo energético mundial aumentó del 1,9 % en 2013 al 2,7 % en 2017, y se preveía que alcanzaría el 3,3 % en 2020. De los diferentes segmentos de la economía digital, el 35 % del consumo total de energía en 2017 correspondió a los centros de datos y a las redes de transmisión de datos (19 % y 16 %, respectivamente). Según la Agencia Internacional de Energía (AIE), la demanda energética de los centros de datos y de las redes de transmisión de datos a escala mundial fue, respectivamente, de 200 TWh (o el 0,8 %) y de 250 TWh (o el 1 %); dos tercios del consumo de las segundas correspondió a las redes móviles (IEA, 2020).

Los centros de datos consumen electricidad para recopilar, almacenar, transmitir y analizar los datos. Aunque su nivel de consumo a escala mundial se ha mantenido constante a lo largo del tiempo, lo que ha cambiado radicalmente es la estructura de los tipos de centros de datos. El consumo energético de los centros de datos ordinarios respecto al de todos los centros de datos se redujo del 90 % en 2010 al 30 % en 2019, lo que era indicativo de un aumento de los centros de datos en la nube y de hiperescala. La AIE prevé que, en 2022, el consumo energético de los centros de datos de hiperescala representará casi el 50 % del consumo energético de todos los centros de datos. En efecto, "si se mantienen las tendencias actuales en la eficiencia del *hardware* y de la infraestructura de los centros de datos, la demanda mundial de energía de los centros de datos puede permanecer casi constante hasta 2022, pese a un aumento del 60 % en la demanda de servicios. El gran crecimiento de la demanda de servicios de centros de datos sigue siendo compensado por las continuas mejoras en la eficiencia de los servidores, los dispositivos de almacenamiento, los conmutadores de red y la infraestructura de los centros de datos, así como por el notable aumento del porcentaje de centros de datos en la nube y de hiperescala. [...] El paso de centros de datos pequeños e ineficientes a centros de datos en la nube y de hiperescala mucho más grandes se refleja en el menor consumo energético de las instalaciones de los centros de datos respecto a la demanda total de energía" (IEA, 2020)".

Fuente: UNCTAD.

I. PROCESAMIENTO Y USO DE DATOS: INTELIGENCIA ARTIFICIAL

Los beneficios y los costos asociados a los datos se derivan en gran medida de su uso para alimentar los algoritmos de IA para aportar conocimiento y predecir comportamientos. Existe una relación bidireccional entre la IA y los datos: sin los datos, la contribución de la IA se limitaría a sistemas basados en el conocimiento regidos por reglas condicionales "si-entonces"; y sin la IA, el valor que podría extraerse de los datos se limitaría a la experiencia humana y a la comprensión teórica de los fenómenos del mundo real, solo mejorada con las capacidades de cálculo más rápido y preciso que podrían ofrecer las máquinas. De la IA y del control de los datos pueden obtenerse enormes beneficios, no solo económicos, sino también por su enorme poder y capacidad para controlar y modelar el futuro de la tecnología, la economía y la sociedad. Como consecuencia, distintos países de todo el mundo compiten intensamente por conseguir liderar en la esfera de la IA. Asimismo, existe una fuerte competitividad en el sector privado entre las grandes plataformas digitales, que invierten todas bastante en IA.

En el plano de los países, los Estados Unidos están a la cabeza en el desarrollo de la IA, pero China está acortando distancias con rapidez. Entre 2016 y 2020, en esos dos países se originó el 94 % de toda la financiación de las empresas emergentes de IA[35]. La Unión Europea se está quedando atrás[36]. Los países en desarrollo se encuentran en una situación de desventaja en cuanto a los avances en IA, sobre todo en África y América Latina. Un estudio sobre el actual y posible uso de la IA por las empresas emergentes y las pequeñas y medianas empresas en países de ingresos bajos y medianos de cuatro regiones —África

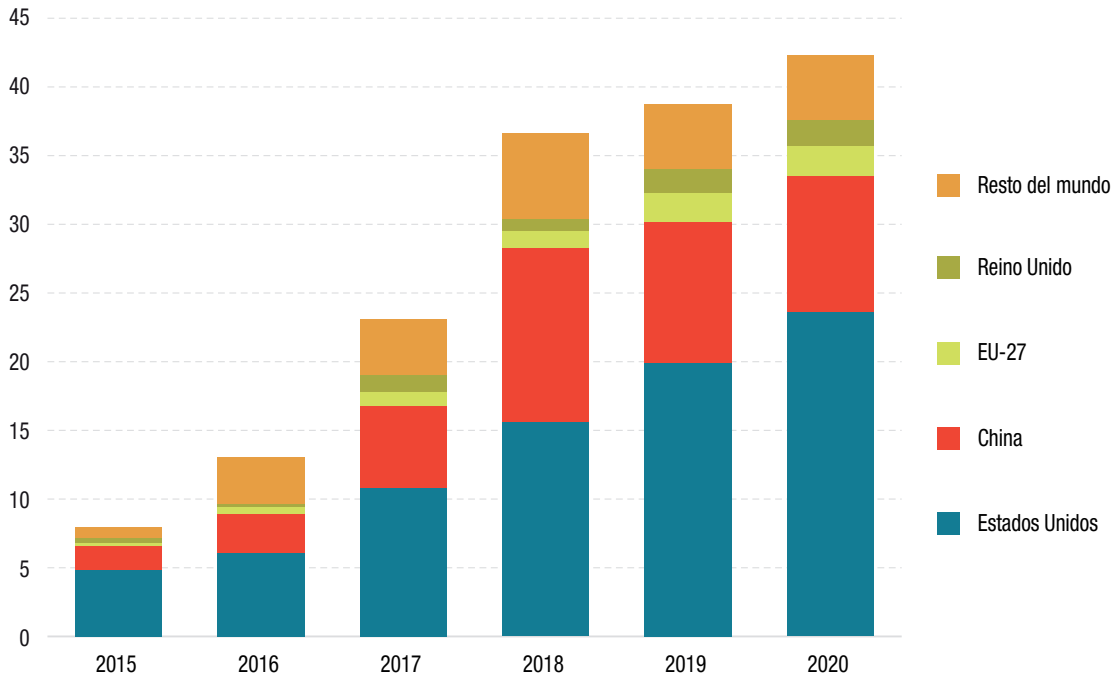
[35] UNCTAD, a partir de datos de CBInsights, disponible en www.cbinsights.com (consultado en enero de 2021).

[36] Para una comparación exhaustiva de la situación del desarrollo de la IA en los Estados Unidos, China y la Unión Europea, véase Castro y McLaughlin (2021).

Subsahariana, Norte de África, Asia Meridional y Asia Sudoriental— concluyó que, "aunque la IA pueda aportar bienestar social, no hay garantías de buenos resultados. Surgen muchas cuestiones cruciales sobre la protección de datos, los sesgos inherentes a los deficientes métodos de recopilación de datos, la inclusión social y el uso responsable de la IA. La IA hace que las nuevas tecnologías mejoren la eficiencia y la productividad, pero también puede aumentar las desigualdades, lo que dificulta la consecución de los Objetivos de Desarrollo Sostenible de las Naciones Unidas. Dado que el aumento del uso de los datos plantea más problemas éticos y de privacidad, las soluciones de IA deben regirse por principios éticos y de privacidad sólidos" (GSMA, 2020c:2).

Según las estimaciones, la inversión mundial en empresas de IA ha aumentado enormemente en los últimos cinco años. Solo en 2019, las empresas privadas de IA atrajeron casi 40.000 millones de dólares en inversiones accionariales consignadas a través de más de 3.100 transacciones distintas. Dado que algunas transacciones no se han hecho públicas, el valor total de las transacciones podría haber sido significativamente mayor, hasta 74.000 millones de dólares. Los Estados Unidos tienen el mercado de inversión en empresas privadas de IA más importante del mundo (Arnold y otros, 2020). Las plataformas digitales globales están desempeñando un papel fundamental debido a la ventaja que supone poder acceder a cantidades ingentes de datos[37]. En la figura I.33 se representa la evolución de la inversión privada en empresas de IA en los últimos años, y se observa el escaso papel de los países en desarrollo, a excepción de China. En lo que respecta al gasto público en IA, China ocupa el primer lugar (con unos 22.000 millones de dólares), seguida de la Arabia Saudita, Alemania, el Japón (todos por debajo de 4.000 millones de dólares) y los Estados Unidos (con unos 2.000 millones de dólares)[38].

Figura I.33 Inversión privada en empresas de IA, por economía, 2015-2020
(Millones de dólares)



Fuente: UNCTAD, cálculos basados en la base de datos de acceso público de NetBase Quid, "2021 AI Index Report" (Zhang y otros, 2021), disponible en https://aiindex.stanford.edu/report/ (consultado en abril de 2021).

[37] Véase Unite.ai, 17 de octubre de 2020, "Investments by Tech Giants In Artificial Intelligence is Set to Grow Further", disponible en www.unite.ai/the-investments-of-tech-giants-in-artificial-intelligence-is-set-to-grow-further/.

[38] Los datos son los publicados en los informes sobre la estrategia nacional de IA. Véase Tortoise, "The Global AI Index, Spotlighting the G20 nations", disponible en www.theglobalaisummit.com/FINAL-Spotlighting-the-g20-Nations-Report.pdf.

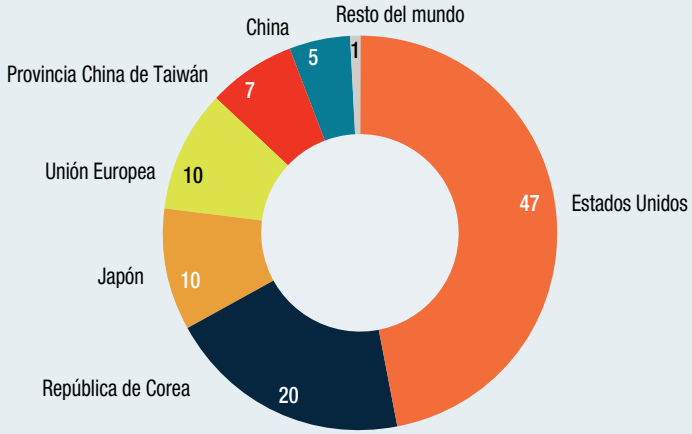
Tras haberse repasado la situación de todas las etapas de la cadena de valor de los datos, desde que se recopilan hasta que se usan en aplicaciones de IA, pasando por su transmisión y almacenamiento, conviene señalar que la utilización de semiconductores desempeña un papel importante en todas esas etapas. Son esenciales para los flujos de datos y para que la economía digital marche. El mercado de los semiconductores se ha visto perjudicado por la interrupción de las cadenas mundiales de valor causada por la pandemia. Los semiconductores son también un factor importante de la dinámica geopolítica relacionada con los avances de la tecnología digital (véase el recuadro I.5).

Recuadro I.5. El mercado de los semiconductores

Con el crecimiento exponencial de los datos, los chips son cada vez más necesarios para generarlos, transferirlos, procesarlos y almacenarlos. Pese a que la mayor parte de los avances tecnológicos digitales tienen lugar en los Estados Unidos y China, este último país no desempeña un papel destacado en el mercado de los semiconductores. Un 47 % de las ventas totales en 2020 correspondió a los Estados Unidos, y un 20 % a la República de Corea (figura del recuadro), mientras que China ocupó solo el sexto lugar, con un 5 % de las ventas totales.

El mercado de los semiconductores está atravesando una situación de escasez en 2021, debido a la pandemia. El auge de la electrónica de consumo ha conducido a un aumento de la demanda de semiconductores y su cadena mundial de valor ha experimentado dificultades, lo que ha provocado la escasez de suministro (Varas y otros, 2021).

Figura del recuadro. Venta de semiconductores, por economía, 2020
(Porcentaje del total a escala mundial)



Fuente: UNCTAD, cálculos basados en 2021 Factbook, Semiconductor Industry Association, disponible en https://www.semiconductors.org/wp-content/uploads/2021/05/2021-SIA-Factbook-FINAL1.pdf.

J. LOS DATOS Y SU RELACIÓN CON LOS DERECHOS HUMANOS Y LA SEGURIDAD

Los datos no son solo un recurso para la economía; también están estrechamente relacionados con cuestiones de privacidad y derechos humanos en general, así como de seguridad. Se puede hacer un uso indebido o incorrecto de los datos, lo que puede afectar a los sistemas políticos y a la democracia. Algunos sucesos de gran relevancia sirven para recordar la necesidad de abordar cuidadosamente esas cuestiones. Entre los incidentes más sonados figuran: la revelación por Edward Snowden de la existencia de programas de vigilancia a escala mundial (2013); la noticia de que la consultora Cambridge Analytica obtuvo datos personales de usuarios sin su consentimiento (2018); o las revelaciones e investigaciones sobre protección de datos en relación con la empresa de reconocimiento facial Clearview (2020-2021). La

economía digital impulsada por los datos también ha dado lugar a casos graves de información errónea y desinformación. El mundo digital está repleto de noticias falsas, con las que se puede manipular a la sociedad. La divulgación de información falsa se acentuó con la pandemia de COVID-19, y dio lugar a lo que la Organización Mundial de la Salud denomina "infodemia"[39].

En el índice de rendición de cuentas empresarial de Ranking Digital Rights de 2020 se evalúan "26 de las plataformas digitales y empresas de telecomunicaciones más poderosas del mundo en lo que respecta a sus políticas y prácticas reveladas que afectan a la privacidad y a la libertad de expresión e información. La capitalización bursátil del total de esas empresas supera 11 billones de dólares. Sus productos y servicios llegan a la mayoría de los 4.600 millones de internautas del mundo. En 2020, la mayoría de las empresas introdujeron mejoras y hubo ejemplos notables de buenas prácticas. Sin embargo, esas mejoras quedaron eclipsadas por las conclusiones que mostraban que, a escala mundial, Internet atraviesa una crisis sistémica en cuanto a transparencia y rendición de cuentas. Quienes utilizan las plataformas digitales y los servicios de telecomunicaciones más potentes del mundo no tienen ni idea de quién puede acceder a su información personal y en qué circunstancias. La gente carece de información básica sobre quién controla su capacidad de conectarse, hablar en línea o acceder a información, y qué información se promueve y prioriza"[40]. En el cuadro I.3 figuran los resultados relativos a las plataformas digitales.

Si bien las cuestiones de derechos humanos y seguridad son de naturaleza más cualitativa y no pueden cuantificarse fácilmente, en esta sección se proporciona información sobre tendencias que apuntan a un aumento de preocupaciones sociales que deben abordarse.

1. Privacidad y vigilancia

Las cuestiones de privacidad se han convertido en una gran preocupación en todo el mundo debido al aumento vertiginoso de los flujos de datos y a que la mayoría de los datos son personales. Varias

Cuadro I.3. Índice de rendición de cuentas empresarial de Ranking Digital Rights relativo a las plataformas digitales, 2020
(Porcentaje)

Empresa	Total	Gobernanza	Libertad de expresión	Privacidad
Twitter	53	47	60	51
Verizon Media	52	64	40	51
Microsoft	50	65	40	51
Google	48	54	46	48
Facebook	45	62	35	46
Apple	43	49	22	54
Kakao	42	42	38	44
Mail.Ru	27	23	19	33
Yandex	27	24	20	33
Alibaba	25	7	17	36
Baidu	25	11	13	37
Samsung	23	29	15	25
Tencent	22	4	15	32
Amazon	20	6	14	28

Fuente: UNCTAD, a partir del índice de rendición de cuentas empresarial de Ranking Digital Rights de 2020, disponible en https://rankingdigitalrights.org/index2020/.

[39] Véase Organización Mundial de la Salud, Infodemic, disponible en www.who.int/health-topics/infodemic#tab=tab_1.

[40] Véase el índice de rendición de cuentas empresarial de Ranking Digital Rights de 2020, disponible en https://rankingdigitalrights.org/index2020.

encuestas ponen de manifiesto que la población está cada vez más preocupada por su privacidad a medida que aumenta la digitalización. Por ejemplo, según la encuesta mundial sobre la seguridad y la confianza en Internet realizada en 2019 por CIGI-Ipsos en colaboración con la UNCTAD, el 78 % de las personas encuestadas mostraron preocupación por su privacidad en Internet y, de ellas, más de la mitad estaban más preocupadas que un año atrás. Por quinto año consecutivo, la mayoría de las personas encuestadas aseguraban sentirse más preocupadas por su privacidad en Internet que el año anterior[41]. En los Estados Unidos, otra encuesta de 2019 reveló que la mayoría piensa que "sus datos personales están menos seguros ahora, que la recopilación de datos plantea más riesgos que beneficios, y que no es posible vivir el día a día sin ser objeto de rastreo"[42].

Durante la pandemia se han desarrollado una serie de aplicaciones de rastreo de contactos con el fin de seguir el rastro de los contagios y prevenir el contacto con personas infectadas por el virus. Esas aplicaciones suscitaron debate en relación con la privacidad y la protección de datos, y parece que han tenido más éxito en Asia que en Europa o los Estados Unidos. De hecho, en una encuesta realizada por Cisco en 2020 sobre la privacidad durante la pandemia, el 60 % de las personas expresaron su preocupación por la protección de sus datos en las herramientas que utilizaban[43].

El escándalo de Snowden sirvió para advertir a todo el mundo sobre las actividades de vigilancia de la población por los Gobiernos. No obstante, la vigilancia se practica por igual en el sector público y en el privado, ya que todas las empresas manejan una gran cantidad de datos personales. La diferencia es que los Gobiernos recurren a la vigilancia principalmente con fines de seguridad y control político, mientras que la vigilancia de las empresas privadas está orientada a la explotación comercial de los datos. La vigilancia puede tener importantes consecuencias para los derechos humanos. Según el análisis realizado por Feldstein (2019) sobre el aumento a escala mundial de la vigilancia mediante IA, cada vez son más los Estados que están implementando herramientas avanzadas de vigilancia mediante IA para controlar, rastrear y vigilar a la ciudadanía. La tecnología de vigilancia mediante IA se está extendiendo a un ritmo más rápido y a un mayor número de países de lo normal, según las personas especialistas. Al menos 75 países de un total de 176 utilizan las tecnologías de IA con fines de vigilancia. Entre ellos figuran países con plataformas de ciudades inteligentes/ciudades seguras, sistemas de reconocimiento facial y servicios policiales inteligentes. China es uno de los principales impulsores de la vigilancia mediante IA en todo el mundo, y las empresas de los Estados Unidos también desempeñan un papel activo en ese ámbito. La tecnología de vigilancia mediante IA suministrada por esas empresas está presente en 32 países.

El reconocimiento facial es un avance tecnológico clave para la vigilancia. Se trata de una tecnología que ha suscitado una gran controversia en todo el mundo y ante la que se levantan voces para prohibirla. En total, ya hay 109 países que utilizan la tecnología de reconocimiento facial con fines de vigilancia o que han aprobado su uso. En 2019, Bélgica consideró que un proyecto piloto que utilizaba tecnología de reconocimiento facial en un aeropuerto infringía la ley federal, y recientemente Francia y Suecia prohibieron el uso del reconocimiento facial en las escuelas. En los Estados Unidos, en 2019 San Francisco se convirtió en la primera ciudad del país en prohibir totalmente la tecnología de reconocimiento facial. Desde entonces, otras ciudades, como Oakland y Northampton, han votado a favor de prohibirla[44]. Las autoridades de protección de datos de la Unión Europea también han pedido que se prohíba el uso de ese tipo de tecnologías[45].

41 Véase www.cigionline.org/internet-survey-2019.

42 Pew Research Center, 15 de noviembre de 2019, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information", disponible en www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

43 Cisco, 2020, "Consumer Privacy Survey: Protecting Data Privacy During the Pandemic and Beyond", disponible en www. cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-infographic-2020.pdf.

44 Para más información, véase el mapa mundial del reconocimiento facial, disponible en https://surfshark.com/facial-recognition-map; y *Nature*, 18 de noviembre de 2020, "Resisting the rise of facial recognition".

45 Véase Supervisor Europeo de Protección de Datos, 21 de junio de 2021, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", disponible en https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-callban-use-ai-automated-recognition_en.

2. Seguridad

Existen numerosas amenazas de seguridad relacionadas con los datos en Internet, como las filtraciones de datos, el robo de identidad, los programas maliciosos *(malware*), los programas secuestradores *(ransomware)* y otros tipos de ciberdelitos. Un análisis de la evolución reciente de las filtraciones de datos muestra que, en general, el número de incidentes de seguridad disminuyó entre 2015 y 2019. Sin embargo, los incidentes que resultaron en la divulgación confirmada de datos a partes no autorizadas (filtraciones de datos) se mantuvieron bastante constantes en el período 2015-2018 (unos 2.000 casos), y se dispararon en 2019 a 3.950 casos. La región más afectada por incidentes y filtraciones de datos fue, con diferencia, América del Norte, y la segunda, Asia y el Pacífico —donde se produjeron más filtraciones de datos en relación con el total de incidentes—, seguidas de Europa, Oriente Medio y África. El análisis no incluyó a todos los países de América Latina y el Caribe, por lo que detectó menos incidentes y filtraciones de datos, lo que no implica que el sistema de seguridad en la región fuera mejor[46].

Las filtraciones de datos son cada vez más frecuentes debido a la computación en la nube y al aumento del almacenamiento digital. Como consecuencia de la pandemia, 2020 fue un año excepcional en el que las industrias se vieron gravemente afectadas en todos los rincones del planeta. La pandemia allanó el camino para que los ciberdelincuentes atacaran a posibles víctimas en el sector sanitario, así como a personas desempleadas o que trabajaban a distancia. Por ejemplo, las estafas aumentaron un 400 % en marzo de 2020, de modo que la pandemia ha representado la mayor amenaza de seguridad de la historia. En 2020, los Estados Unidos registraron la filtración de datos con un mayor costo medio, 8.640 millones de dólares. Se estima que, de aquí a 2025, la ciberdelincuencia costará al mundo 10,5 billones de dólares anuales[47].

La inversión en empresas de ciberseguridad alcanzó más de 11.000 millones de dólares en 2020, la cifra más alta desde 2016, en medio de la crisis económica mundial. El importe medio por contrato de ciberseguridad aumentó más del doble entre 2016 y 2020 (de 10 a 23 millones de dólares). Ese aumento podría deberse en gran medida al mayor riesgo de incidentes de seguridad y filtraciones de datos derivado del proceso acelerado de digitalización de la sociedad y de los ataques dirigidos contra el sector de la salud tras el inicio de la crisis sanitaria en 2020. En el período 2016-2020, los Estados Unidos fueron, con diferencia, la primera economía en cuanto a inversión en empresas de ciberseguridad (con casi tres cuartas partes de las inversiones a escala mundial), seguidos de China e Israel (CBInsights, 2021).

3. Interrupciones de Internet

Pese a que el uso de Internet se ha hecho más necesario debido a la pandemia, en 2020 se registraron 155 casos de interrupción de Internet. Aunque el número de casos disminuyó con respecto a los 196 de 2018 y los 213 de 2019, no debe considerarse que esa disminución sea un indicio de un menor impacto de las interrupciones o de un aumento general de los derechos digitales. De hecho, el número de países que interrumpieron Internet fue de 25 en 2018, 33 en 2019 y 29 en 2020. De los 29 países de 2020, 10 estaban en África Subsahariana, 8 en la región de Oriente Medio y Norte de África, 6 en Asia y el Pacífico, 3 en América Latina y el Caribe y 2 en Europa. La India fue, con diferencia, el país con mayor número de interrupciones de Internet, 109 (Access Now, 2021).

Las interrupciones de Internet tienen repercusiones perjudiciales para la vida y los medios de subsistencia de la población —al dañar los derechos humanos, la salud y la seguridad públicas— y menoscaban el derecho al desarrollo (Nyokabi y otros, 2019). Además, se estima que el costo total que las restricciones de Internet han supuesto para la economía mundial desde 2019 es de 14.500 millones de dólares[48]. Las repercusiones negativas de las interrupciones durante la pandemia fueron mayores.

[46] Véase Verizon, Data Breach Investigation Reports (varios años).

[47] Véase *Varonis*, 16 de abril de 2021, “98 Must-Know Data Breach Statistics for 2021”; también proporciona detalles sobre las principales filtraciones de datos más recientes.

[48] Véase Top10VPN, 4 de enero de 2020, “The Global Cost of Internet Shutdowns”.

K. CONCLUSIONES Y ESTRUCTURA DEL RESTO DEL INFORME

En este capítulo, en el que se sientan las bases del presente Informe, se han abordado cuestiones básicas relacionadas con la definición del concepto de datos y las características de los datos, y se ha ofrecido una visión general de los últimos avances en la economía digital impulsada por los datos, en la que se enmarcan los flujos de datos transfronterizos. Se ha analizado la evolución a escala mundial de las TIC y las infraestructuras de datos, el tráfico de datos, el valor de los datos y de los mercados de datos, así como de las diferentes etapas de la cadena de valor de los datos. La tradicional brecha digital, entendida en términos de conectividad y acceso a Internet y su uso, sigue siendo considerable y es un problema recurrente para el desarrollo. Además, a medida que los datos y los flujos de datos transfronterizos han ido cobrando importancia como recurso económico, han surgido nuevas dimensiones de la brecha digital en relación con la recopilación, la transmisión, el almacenamiento, el procesamiento y el uso de los datos. Por consiguiente, a la brecha digital existente desde hace tiempo se añade una brecha relacionada con los datos.

> A la brecha digital existente desde hace tiempo se añade una brecha relacionada con los datos.

La rápida evolución de las tecnologías digitales puede ofrecer oportunidades en términos de creación y captura de valor, pero también plantea importantes retos. La economía digital impulsada por los datos se caracteriza por grandes desequilibrios de poder y desigualdades entre países y a escala nacional. Unas pocas plataformas digitales globales de los Estados Unidos y China están acaparando la mayor parte de los beneficios. La situación se ha agravado con la pandemia, que ha acelerado la digitalización, de modo que esas plataformas digitales globales han visto reforzadas sus posiciones dominantes mientras el resto de los sectores se sumían en una crisis económica.

Las plataformas digitales globales están invirtiendo cada vez más en todas las etapas de la cadena mundial de valor de los datos: en la recopilación de datos (con los servicios de las plataformas orientados a los consumidores), en la transmisión de datos (con cables submarinos y satélites), en el almacenamiento de datos (con centros de datos en la nube y de hiperescala) y en el análisis de datos (con la IA). En general, las tendencias mostradas en este capítulo ponen también de relieve que habría que dejar de llamarlas plataformas digitales globales. Aunque disfrutan de las ventajas derivadas de los datos gracias a su componente de plataforma, ya no son solo plataformas digitales. Sus negocios abarcan muchos sectores y son empresas que participan en todos los estratos de la economía digital, desde el sector digital (dimensión esencial) hasta la economía digital (dimensión acotada) y la economía digitalizada (dimensión amplia)[49]. Deberían ser consideradas como corporaciones digitales globales. En consecuencia, se hace cada vez más difícil considerar la regulación de los flujos de datos transfronterizos sin tener en cuenta también la gobernanza de esas corporaciones digitales.

Ya antes de 2020, el rápido avance de la digitalización había puesto de manifiesto la necesidad de regular la economía digital para obtener los máximos beneficios y reducir al mínimo los riesgos y desafíos, de modo que pudiera contribuir al desarrollo (UNCTAD, 2019a). La aceleración de la digitalización como resultado de la pandemia ha acentuado las brechas digitales y ha hecho que la regulación —a escala nacional, regional e internacional— sea aún más urgente. En esas circunstancias es fundamental la gobernanza de los datos, incluida la gobernanza de los flujos de datos transfronterizos, tema objeto de este Informe.

A medida que los flujos de datos transfronterizos adquieren mayor protagonismo en la economía mundial, se hace más necesario regularlos adecuadamente a escala internacional, en el marco general de la gobernanza global de los datos. En la actualidad, las empresas que pueden extraer o recopilar los datos

[49] Véase la representación de la economía digital en la figura I.1 de UNCTAD (2019a).

—y que tienen la capacidad de procesarlos posteriormente, principalmente las corporaciones digitales globales de los Estados Unidos y China— están en una posición privilegiada para apropiarse de la mayor parte del valor de los datos. Por el contrario, quienes generan o suministran los datos brutos —es decir, los usuarios de las plataformas, muchos de los cuales se encuentran en países en desarrollo y contribuyen también al valor de los datos— no obtienen beneficios en términos de desarrollo. Se necesita un nuevo sistema internacional para regular los flujos de datos transfronterizos, de modo que los beneficios conexos se distribuyan equitativamente.

> La aceleración de la digitalización como resultado de la pandemia ha acentuado las brechas digitales y ha hecho que la regulación —a escala nacional, regional e internacional— sea aún más urgente.

En ese contexto, el resto del Informe, que se centra en la dimensión internacional de los datos, está estructurado de la siguiente manera. En el capítulo II se hace un repaso de las publicaciones centradas en los flujos de datos transfronterizos y se identifican algunas cuestiones que deben abordarse, a lo que este Informe supone una contribución. En el capítulo III se da un paso atrás para analizar las principales cuestiones en juego en relación con los flujos de datos transfronterizos y el desarrollo. En el capítulo IV se analizan los enfoques de la economía digital impulsada por los datos adoptados en las regiones del mundo que más pueden influir en la gobernanza global de los flujos de datos, así como el riesgo de fragmentación en el espacio digital y sus posibles repercusiones para los países en desarrollo. En el capítulo V se ofrece una sinopsis de las principales medidas aplicadas a escala nacional para regular los flujos de datos transfronterizos, mientras que en el capítulo VI se examinan los enfoques normativos regionales e internacionales en materia de flujos de datos transfronterizos. Por último, el capítulo VII concluye con un análisis de las posibles políticas para avanzar hacia un consenso en la gobernanza de los datos y los flujos de datos transfronterizos, de forma que se garantice que los beneficios que se puedan generar contribuyan a la consecución de los objetivos globales de desarrollo, y al mismo tiempo se reduzca el riesgo de que se haga un uso indebido o incorrecto de los datos.

Antes de pasar a analizar en más detalle el papel y las implicaciones de los flujos de datos para el desarrollo y las políticas conexas, en este capítulo se hace un repaso de las publicaciones sobre los flujos de datos transfronterizos. Con ello se trata de determinar cuáles son los principales problemas, lagunas y esferas con margen de mejora que son muy pertinentes para el debate internacional sobre políticas.

En este capítulo se muestra que, en general, no existen definiciones comunes sobre los datos y los flujos de datos transfronterizos, lo que obstaculiza su medición, así como el debate constructivo y la creación de consenso acerca de su gobernanza. En pocos estudios se analizan las implicaciones para el desarrollo de los flujos transfronterizos de diferentes tipos y taxonomías de datos. Además, la mayoría de las publicaciones se centran en la dimensión comercial de los datos, y suelen pasar por alto su carácter multidimensional. Prácticamente todos los estudios proceden de países anglófonos, y muy pocos se ocupan de los países en desarrollo.

REPASO DE **LAS PUBLICACIONES** SOBRE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

II

Las publicaciones sobre los flujos transfronterizos presentan varias limitaciones y lagunas

No se ha **convenido en definiciones comunes** de datos y de flujos de datos transfronterizos, lo que dificulta su medición, así como el debate constructivo y la creación de consenso sobre su gobernanza

Pocos estudios analizan las **implicaciones para el desarrollo** de los flujos de datos transfronterizos

La mayoría de los estudios recientes sobre los flujos de datos transfronterizos los examinan principalmente desde el punto de vista comercial, y en pocos se adopta un **enfoque multidimensional que tenga en cuenta las dimensiones económicas y no económicas**

Muchos estudios presentan una clara **tendencia ideológica** que refleja determinados intereses

Pocos estudios se centran en los países en desarrollo y la mayoría proceden de países **anglófonos**

Hay pocas pruebas concluyentes que apoyen la libre circulación de los datos o las políticas estrictas de localización de los datos

Prioridades para futuras investigaciones

Trabajar en las definiciones y la medición de los datos y los flujos de datos

Profundizar en las **implicaciones para el desarrollo** de los flujos de datos

Prestar una mayor atención **al carácter multidimensional de los datos**

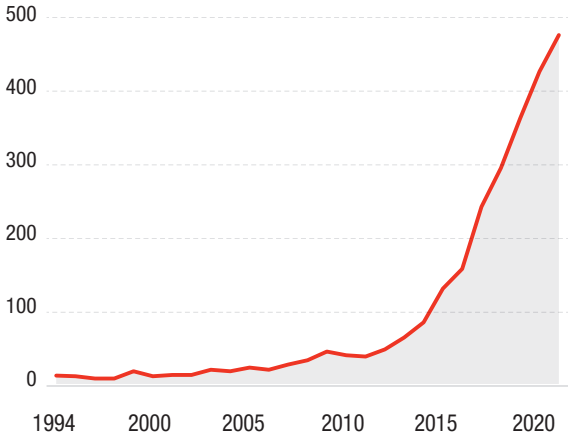
Evaluar de manera más equilibrada las políticas acerca de los flujos de datos transfronterizos y analizar las ventajas y los inconvenientes

A. INTRODUCCIÓN

El creciente papel de los datos en la evolución de la economía digital, a raíz del rápido avance de las tecnologías digitales, ha dado lugar a un aumento paralelo de las publicaciones sobre los flujos de datos transfronterizos en los últimos años. Las primeras publicaciones en las que se utilizó el término "flujos de datos transfronterizos" correspondían principalmente a documentos bancarios y publicaciones sobre la tecnología de la información (TI). El debate internacional sobre los flujos de datos transfronterizos no es nuevo. Esos flujos ya ocupaban un lugar destacado en la agenda internacional en las décadas de 1970 y 1980, cuando se estudiaban los "flujos de datos a través de las fronteras". Por ejemplo, la Organización de Cooperación y Desarrollo Económicos (OCDE) adoptó en 1980 las Directrices sobre la Protección de la Vida Privada y la Transmisión Transfronteriza de Datos Personales (Kuner, 2011)[1]. En ese momento, la atención se centraba principalmente en la protección de los datos personales y la privacidad. Durante el último decenio, al aumentar el papel de los datos como recurso económico, los debates se han desplazado hacia los aspectos relacionados con la economía.

Con la expansión de Internet, que modifica los flujos de información, bienes y servicios, los flujos de datos transfronterizos han cobrado importancia y el número de publicaciones ha aumentado. Como se muestra en la figura II.1, el número de resultados por año de la búsqueda en Google Scholar de publicaciones científicas que contienen el término "cross-border data flows" (flujos de datos transfronterizos) aumentó espectacularmente entre 1994 y 2020.

Figura II.1 Número de publicaciones sobre los flujos de datos transfronterizos, 1994-2020



Fuente: UNCTAD, a partir de Google Scholar, disponible en https://scholar.google.com (consultado el 18 de enero de 2021).
Nota: Se basa en las búsquedas de las palabras clave "cross-border data flow" (flujo de datos transfronterizo) y "cross-border data flows" (flujos de datos transfronterizos) en las publicaciones de entre 1994 y 2020. La figura pretende ser indicativa, y no aspira a ofrecer una búsqueda sistemática exhaustiva por palabras clave de los correspondientes temas.

En este capítulo se revisan las publicaciones jurídicas, económicas, de la sociedad civil y del sector privado[2] donde se evalúa el estado actual de la investigación sobre los flujos de datos transfronterizos y su regulación[3]. En concreto, se examinan las definiciones pertinentes que se utilizan actualmente, la medición de los flujos de datos, el enfoque de la investigación y las perspectivas de países con diferentes niveles de desarrollo. Para ello, se señalan algunas cuestiones que deberían investigarse más exhaustivamente. Una cuestión clave es la definición y medición de los flujos de datos transfronterizos para comprender mejor en qué punto se encuentran los debates, aunque se trata de un asunto complicado porque la importancia de los datos es cada vez mayor en diversos contextos.

Otro aspecto relevante es el predominio de la investigación sobre los países desarrollados, y procedente de esos países, que tiende a pasar por alto la función y las necesidades de los países en desarrollo en esta esfera evolutiva de la economía digital. Además, muchos estudios tienden a basarse en suposiciones implícitas y tendencias ideológicas, y no consideran todos los argumentos.

Este repaso bibliográfico no pretende ser exhaustivo ni sistemático. El objetivo es determinar cuáles son los principales problemas, lagunas y esferas con margen de mejora que son muy pertinentes para el

1 Véase el capítulo VI para más información sobre las Directrices de la OCDE.

2 Este repaso no abarca las publicaciones de los Gobiernos porque sus opiniones se reflejan principalmente en las consideraciones sobre las políticas que se analizan en los capítulos IV a VI.

3 En el anexo en línea del capítulo II (disponible en https://unctad.org/system/files/official-document/der2021_annex1_en.pdf) se presenta un cuadro con información sobre las publicaciones revisadas.

debate internacional sobre las políticas acerca de los flujos de datos transfronterizos y el desarrollo. Por consiguiente, el presente Informe pretende abordar esas deficiencias y contribuir a subsanar algunas de ellas. En concreto, en este capítulo se repasan sobre todo las publicaciones recientes por su relevancia para sustentar el actual debate internacional acerca de las políticas en esta esfera.

B. DEFINICIONES DE DATOS Y FLUJOS DE DATOS TRANSFRONTERIZOS

Aunque los flujos de datos transfronterizos ocupan un lugar cada vez más destacado en las publicaciones sobre investigaciones y políticas, todavía no se ha alcanzado un consenso acerca de los elementos más básicos: las definiciones de datos y flujos de datos transfronterizos.

A menudo, el concepto de datos se da por sentado, y se asume una interpretación común como base de muchos estudios. Sin embargo, al hablar de datos podemos referirnos a conceptos o dimensiones diferentes. Krotova y Eppelsheimer (2019) revisan las publicaciones sobre la gobernanza de los datos mediante la minería de textos y distinguen entre datos e información. La información se define como un conjunto de datos perfeccionados y procesados para aumentar su valor, mientras que los datos describen las características y propiedades de hechos u objetos. Asimismo, la OCDE define los datos como un conjunto de puntos no procesados que, mediante su tratamiento y análisis, se convierten en información (Casalini y López González, 2019; Nguyen y Paczos, 2020; Tomiura y otros, 2019).

En relación con la gobernanza de los datos, Ciuriak (2020) considera que los datos son el nuevo activo fijo para captar rentas en una economía. Aaronson (2019a) señala que con frecuencia se adopta una definición de datos demasiado limitada. No se puede considerar que los datos son simplemente otro recurso económico (como las infraestructuras, la mano de obra o el capital), ya que muchos datos surgen básicamente como un subproducto de la vida, y esto influye en la regulación y la gobernanza de los flujos de datos.

Tampoco es sencillo dar con una definición funcional de lo que constituye un flujo de datos transfronterizo, es decir, una definición que permita la medición y constituya una base común para los debates. Básicamente, se trata de una transferencia libre de datos a través de las fronteras o de diferentes mercados internacionales (Linden y Dahlberg, 2016; WEF, 2020b). Sin embargo, puesto que los datos no cruzan las fronteras por las aduanas, sería conveniente una definición más específica. La Business Software Alliance (BSA, 2017) presenta una definición un poco más funcional en cuanto a que marca un punto de inicio y finalización de un flujo, al considerar los flujos de datos transfronterizos como una transferencia de datos entre servidores situados en diferentes países.

Muchos otros autores simplemente no definen estos flujos. Los que apoyan la libre circulación de los datos a través de las fronteras se centran en sus posibles efectos positivos, como la contribución a la innovación, la productividad, la investigación y las interacciones sociales (BSA, 2017; Spiezia y Tscheke, 2020).

En general, el hecho de dar por sentadas las definiciones de datos y flujos de datos transfronterizos hace que muchos autores se centren en un aspecto específico de los datos, predominantemente relacionado con el comercio, y no tengan en cuenta otros ámbitos que se apoyan en los flujos de datos y podrían tener otras características y, en consecuencia, diferentes implicaciones para la gobernanza de los datos, la regulación y los países con diferentes niveles de desarrollo.

C. CUANTIFICACIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS Y DE SU IMPACTO

Las definiciones de flujos de datos transfronterizos de un nivel relativamente alto dejan muy abierta la cuestión de cómo medir los flujos reales, como se ha expuesto en el capítulo I. Desde un punto de vista técnico, los flujos de datos se pueden medir en bits y *bytes* por unidad de tiempo (Nicholson y Noonan, 2017). Esa forma de medirlos no tiene en cuenta el lugar en el que se debe realizar esa medición para

poder determinar si un flujo de datos es transfronterizo y si constituye un flujo de entrada o de salida. No obstante, cada vez hay más publicaciones que se centran en cuantificar el impacto de esos flujos.

En algunas investigaciones se eluden las cuestiones relacionadas con la medición definiendo los flujos de forma limitada para que resulten manejables y cuantificables. McKinsey (2014, 2016, 2019) define en gran medida estos flujos como flujos de comunicación y datos transfronterizos. En consecuencia, se miden utilizando el ancho de banda de Internet, la penetración de Internet y los minutos de llamadas por Internet. Además, en esos informes se intenta diferenciar los flujos de datos transfronterizos de otros flujos, como los financieros (McKinsey, 2014), aunque la banca esté vinculada a grandes flujos de datos. En general, se constata que la contribución de los datos al aumento del producto interno bruto (PIB) mundial superó a la del comercio de mercancías (McKinsey, 2016). No obstante, parece que incluso los operadores de telefonía móvil consideran que es bastante complicado medir estos flujos. En una publicación sobre los flujos de datos transfronterizos de su asociación sectorial, la GSMA, se abstienen de cuantificar los flujos de datos internacionales (GSMA, 2018a).

En otras publicaciones se hace referencia a estudios de casos para demostrar el creciente papel de los datos, sobre todo en las empresas, la sanidad y la investigación. Castro y McQuinn (2015) señalan que empresas como los fabricantes de aviones recogen *terabytes* de datos durante los vuelos internacionales que ayudan a sus servicios de mantenimiento y reparación. Asimismo, un fabricante de camiones y autobuses ha creado una sección específica para analizar los datos de conducción con el fin de optimizar el consumo de carburante, reducir el impacto ambiental del transporte y utilizar los datos agregados para supervisar la flota y detectar antes los problemas (Castro y McQuinn, 2015).

Dado que la medición del volumen de los flujos de datos es difícil y predominan las aproximaciones, en algunos análisis económicos se intenta medir esos flujos de manera indirecta. Los enfoques se dividen en tres grandes categorías: en primer lugar, las aproximaciones que utilizan componentes digitales en el comercio; en segundo lugar, las encuestas y observaciones sobre los cambios de comportamiento ante los cambios reglamentarios; y en tercer lugar, las evaluaciones del impacto de las restricciones al flujo de datos.

Uno de los enfoques adoptados para cuantificar el papel de los flujos de datos transfronterizos consiste en examinar la contribución del comercio digital de servicios al comercio global o al PIB. Nicholson y Noonan (2017) tratan de estimar la aportación máxima de ese tipo de servicios al conjunto del comercio internacional de servicios de los Estados Unidos de América entre 2002 y 2011. Definen cinco categorías de estadísticas comerciales de la Oficina de Análisis Económicos basadas en las tecnologías de la información y las comunicaciones (TIC) que, por tanto, es probable que entrañen flujos de datos. Se trata de una aproximación, ya que no se dispone de información acerca de qué proporción de esos servicios se prestó realmente por medios digitales. Los autores estiman que, en 2011, los servicios digitales registraron un superávit comercial de 136.000 millones de dólares de los Estados Unidos y las exportaciones digitales ascendieron a 357.000 millones de dólares, por lo que representaron el 60 % de todas las exportaciones de servicios. Además, calculan que esos servicios aportan un tercio del valor añadido de todas las exportaciones. Por consiguiente, su valor para la economía de los Estados Unidos es considerable. A su vez, los flujos de datos transfronterizos que entrañan esos servicios probablemente sean muy valiosos. El inconveniente de este enfoque es que solo puede medir los flujos que tienen un valor monetario asociado. No se pueden tener en cuenta los datos que cruzan las fronteras antes de su transformación en productos de valor comercial. Por consiguiente, es probable que este enfoque subestime la importancia de los flujos de datos transfronterizos, dado que muchos de ellos no figuran en las estadísticas comerciales oficiales.

Tomiura y otros (2019) realizaron una encuesta a medianas y grandes empresas del Japón sobre sus transferencias de datos al extranjero tras la introducción del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, relativo a la transferencia de datos personales, y de las leyes de ciberseguridad de China y la India. Estos autores evalúan los cambios en el comportamiento de las empresas en un análisis descriptivo. El 5 % de las empresas encuestadas se vio afectada negativamente por la introducción del RGPD, y el 8 % por las leyes de ciberseguridad. Un tercio de esas empresas afectadas cambió la ubicación de su sistema de almacenamiento y procesamiento de datos. Asimismo, el 40 % de las empresas reforzaron sus medidas de protección de datos en respuesta al RGPD, mientras que más de la mitad del 8 % de las

afectadas no tomaron medidas en respuesta a las leyes de ciberseguridad. En términos generales, solo el 1 % de las empresas encuestadas transformó o interrumpió sus negocios con la Unión Europea a raíz de la introducción del RGPD. En torno al 5% de las empresas modificaron sus prácticas de transferencia de datos a los países correspondientes en respuesta a las leyes de ciberseguridad. En el caso del RGPD, el impacto de esta nueva normativa sobre la circulación de los datos parece ser comparativamente menor que en otros estudios (Gupta y otros, 2020; Ferracane y van der Marel, 2020). Además, la encuesta revela que hay un porcentaje sorprendentemente bajo de empresas que transfieren datos diariamente a nivel internacional, lo que puede indicar un problema de medición.

Otra corriente de la bibliografía mide el valor de los flujos de datos transfronterizos de forma implícita mediante una simulación o estimación del impacto de las restricciones a los flujos de datos, como el RGPD o las leyes de localización de los datos[4] en otros lugares. Bauer y otros (2013) miden estos flujos indirectamente a través de la reducción en el comercio, el PIB y el bienestar general, utilizando un modelo de equilibrio general para simular el impacto del RGPD antes de su introducción. Sus estimaciones revelan que la limitación de la libre circulación de los datos, con la consiguiente pérdida de competitividad, provocaría una contracción del PIB de la Unión Europea de entre el 0,8 % y el 3,9 %. El impacto negativo en el ingreso per cápita podría ascender a entre 340 y 1.140 dólares. Los autores estiman que esta pérdida anularía cualquier ganancia comercial conseguida con el Acuerdo de Libre Comercio (ALC) entre la Unión Europea y los Estados Unidos, lo que implica un valor significativo de los flujos de datos transfronterizos en un contexto comercial.

Del mismo modo, Bauer y otros (2016) miden el impacto de la regulación de la circulación de datos de los países en la productividad de sus industrias mediante la creación de un índice conexo. Ese índice se basa en los subindicadores del Índice de Regulación de Productos de Mercado de la OCDE y en las políticas específicas de cada país, además de en las medidas de intensidad de datos en diversos sectores. Los autores descubren que la restricción de la circulación de los datos tiene un efecto cada vez más adverso en la productividad y los precios de las industrias que emplean un volumen relativamente grande de datos. Sus estimaciones muestran que las restricciones a los flujos de datos generarían una reducción del PIB real a medio y largo plazo de entre el 0,1 % y el 0,58 %, lo que ascendería a varios miles de millones de dólares en el caso de la Unión Europea. Por su parte, Badran (2018), Ferracane y van der Marel (2020), así como Ferracane y otros (2020), miden el valor que pierden los flujos de datos transfronterizos a causa de las restricciones analizando las reducciones en el potencial de innovación y la productividad de las empresas y los sectores de diferentes conjuntos de países. En un análisis de CUTS International (Gupta y otros, 2020) se concluye que las políticas de restricción de los flujos de datos limitarían las exportaciones de servicios digitales de la India de tal manera que el PIB podría disminuir entre un 0,2 % y un 0,34 %. En el caso del volumen objetivo de la economía de la India para 2025, esto implicaría un déficit de entre 9.000 millones y 17.000 millones de dólares.

Por otro lado, Spiezia y Tscheke (2020) analizan el impacto de la eliminación de las restricciones a través de pares de países que se convierten en signatarios de los mismos acuerdos sobre la privacidad de los datos. Constatan que ser signatario del Convenio 108 del Consejo de Europa o de los acuerdos de puerto seguro de los Estados Unidos con la Unión Europea y Suiza aumenta el comercio de mercancías entre un 6 % y un 8 %. La ratificación del Convenio 108 está vinculada a un crecimiento del comercio de servicios del 12 % para los pares de países. Sin embargo, no se estima ningún efecto significativo en el caso de los acuerdos de puerto seguro de los Estados Unidos[5]. Por tanto, el costo de unas normas de cumplimiento más estrictas se ve compensado por los beneficios de la facilitación de los flujos de datos entre las partes de los acuerdos; este impacto es significativo tanto a nivel estadístico como económico.

Además del reto que supone la medición cuantitativa de los flujos, también existe una cuestión jurídica sobre lo que constituyen los flujos de datos transfronterizos que puede afectar a su medición. Por ejemplo, una transferencia de la propiedad de los datos de una entidad de un país a otra entidad de otro país, sin

[4] Por "localización de los datos" se entiende una medida política adoptada en el contexto de la regulación de los flujos de datos transfronterizos que consiste en imponer requisitos para que los datos se mantengan en un territorio concreto.

[5] Para un análisis del Convenio 108, véase el capítulo VI. Los acuerdos de puerto seguro fueron reemplazados por el Escudo de Privacidad, que también se examina en el capítulo IV.

que los datos salgan del centro donde están almacenados, podría constituir un flujo de datos a través de las fronteras sin que se haya producido y medido un flujo real (Nguyen y Paczos, 2020).

Por el momento, los estudios dirigidos a cuantificar esos flujos están repletos de propuestas para comprender mejor este asunto. No obstante, dado que siguen existiendo grandes lagunas si lo que se desea es obtener una visión completa, hay que seguir trabajando en la medición de los flujos de datos transfronterizos para desarrollar diferentes opciones y, finalmente, determinar qué enfoques pueden contribuir a las correspondientes estadísticas nacionales.

D. TIPOS DE DATOS

Los datos pueden caracterizarse según múltiples dimensiones. Los tipos de datos contemplados en la mayoría de las investigaciones suelen clasificarse en tres categorías: comerciales, empresariales y personales. Una parte considerable de las publicaciones se centra en los datos comerciales. La investigación abarca el comercio de servicios, mercancías y servicios digitales, y a menudo trata de cuantificar los flujos de datos de alguna manera. La mayoría de los análisis pertenecen a las dos categorías siguientes: en primer lugar, las iniciativas para cuantificar los flujos actuales de datos en forma de componentes del comercio de servicios (McKinsey, 2014; Nicholson y Noonan, 2017); y, en segundo lugar, las estimaciones del impacto de las restricciones al flujo de datos o de su supresión (Badran, 2018; Bauer y otros, 2013, 2016; Gupta y otros, 2020; Ferracane y otros, 2020; Ferracane y van der Marel, 2020; Spiezia y Tscheke, 2020).

Otro tipo de datos que se utilizan en los ejercicios de cuantificación son el volumen de los flujos de comunicación en *bytes* (Bughin y Lund, 2017; McKinsey, 2014). Dado que el valor de esos flujos es difícil de determinar, lo que complica su comparación con los valores de los flujos de mercancías y otros flujos internacionales, estas comparaciones son relativamente escasas.

La investigación jurídica en este ámbito se divide en las siguientes tres grandes categorías de datos no excluyentes: datos comerciales, datos personales (frente a los no personales) y la comparación de los distintos regímenes aplicables a los flujos de datos. Los argumentos en contra de la libre circulación de los datos suelen basarse en que los datos personales no están bajo el control de las entidades responsables. En consecuencia, en una parte importante de las publicaciones se investigan diferentes regímenes de restricción de la circulación de los datos en todo el mundo (Chander y Lê, 2015). Varios estudios señalan que las normativas suelen distinguir entre datos personales y no personales (Chander y Lê, 2015; Aaronson, 2019a; Aaronson y Maxim, 2013; Meltzer, 2020; Casalini y López González, 2019; Daza Jaller y otros, 2020; Mattoo y Meltzer, 2018; WEF, 2020b). Otros estudios de la legislación investigan el papel de los datos en el comercio, especialmente en el contexto de la regulación de los flujos de datos en el marco del sistema comercial (Burri, 2016; Daza Jaller y otros, 2020; Mattoo y Meltzer, 2018; Hilbig, 2018; BDI, 2017; Aaronson y Maxim, 2013). No obstante, Aaronson (2019a) señala que una gran proporción de datos no está asociada a ningún tipo de comercio, lo que hace que la regulación de los datos en virtud de acuerdos comerciales resulte problemática.

En el contexto de los datos empresariales, Nguyen y Paczos (2020) analizan el uso de los datos para mejorar los modelos de negocio existentes con un mayor hincapié en los datos, además de su importancia en los nuevos modelos de negocio. Linden y Dahlberg (2016) evalúan el papel de la libre circulación de los datos empresariales en el contexto de la libertad de circulación en la Unión Europea.

Otro bloque de publicaciones investiga diferentes tipos de datos en el contexto de la gobernanza de los datos. Al macronivel, se examinan las cuestiones de regulación en el plano nacional e internacional, así como la compatibilidad e interoperabilidad de los diversos enfoques reguladores (Aaronson, 2019a; Ademuyiwa y Adeniran, 2020; GSMA, 2018b; Mattoo y Meltzer, 2018; Microsoft, 2018; WEF, 2020b). Al micronivel, la atención se centra en la gestión de los datos de las empresas y el valor de los datos (Engels, 2019; Krotova y Eppelsheimer, 2019).

El Banco Mundial (World Bank, 2021) caracteriza los datos utilizando dos dimensiones: datos públicos o privados y, en cuanto a sus métodos de recopilación, nuevos o tradicionales. Los datos públicos recopilados tradicionalmente suelen abarcar una amplia parte de la población, pero no son oportunos,

mientras que los nuevos datos privados pueden ser muy detallados y oportunos, pero rara vez son representativos de la población, especialmente de las minorías.

Además de estas amplias categorías, Coyle y otros (2020) mencionan otras dimensiones que pueden ayudar a diferenciar los distintos tipos de datos:

- Características: por ejemplo, según la sensibilidad o la finalidad.
- Origen: datos facilitados, observados, derivados o inferidos (OECD, 2013a).
- Uso: por ejemplo, con fines de recursos humanos, institucionales, de empresa a consumidor o técnicos (Rentzhog y Jonströmer, 2014).
- Naturaleza: por ejemplo, públicos o privados, exclusivos o abiertos, creados activa o pasivamente (Nguyen y Paczos, 2020).

Estas dimensiones ayudan a comprender mejor la naturaleza y la finalidad de los datos e ilustran que, según el tipo de datos utilizados, pueden describirse de múltiples maneras. Asimismo, esta multidimensionalidad pone de manifiesto que el establecimiento de reglas directas en relación con los datos constituye un reto, ya que es difícil definirlos de forma estricta (De La Chapelle y Porciuncula, 2021).

E. POSICIONES ANTE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Cuatro grandes grupos (la sociedad civil, el mundo universitario y los grupos de reflexión, el sector privado y las organizaciones internacionales) contribuyen a las publicaciones sobre los flujos de datos transfronterizos. Dentro de cada grupo, las posiciones generales ante estos flujos están ampliamente armonizadas.

En términos generales, los investigadores universitarios y los grupos de reflexión[6] tienden a apoyar la libre circulación de los datos, mientras que muchos también están a favor de reglas claras en esta esfera (Aaronson, 2014, 2019a; Aaronson y Maxim, 2013; Badran, 2018; Bauer y otros, 2013, 2016; Chander y Lê, 2015; Chen y otros, 2019; Ciuriak, 2020; Ferracane y otros, 2020; Ferracane y van der Marel, 2020; Kimura, 2020; Meltzer, 2020; Tomiura y otros, 2019). Los aspectos económicos motivan principalmente los estudios a favor de la libre circulación de los datos con argumentos en contra de la localización de los datos y de las normativas en materia de privacidad que obstaculizan los flujos internacionales. Estos estudios son partidarios de los flujos de datos transfronterizos, ya que reducen los costos de las empresas y mejoran el comercio internacional, el bienestar de los consumidores y el PIB (Bauer y otros, 2013; Badran, 2018; Hinrich Foundation, 2019; Tomiura y otros, 2019; Ferracane y otros, 2020; Ferracane y van der Marel, 2020). Otro argumento en contra de la localización de los datos se refiere a las posibles ineficiencias. En primer lugar, el mantenimiento de los datos dentro de las fronteras nacionales y el establecimiento de una industria de almacenamiento de datos no se asocian a un gran aumento del empleo, ya que los centros de datos están en su mayoría automatizados (Chander y Lê, 2015). Además, la localización de los datos no contribuye a su seguridad. El mantenimiento de los datos en un solo lugar aumenta su vulnerabilidad a la destrucción a causa de desastres (naturales), pero también de la piratería informática, cuando la seguridad no se adapta a los estándares más recientes (Chander y Lê, 2015). Además, Taylor (2020) señala que el costo de oportunidad de la localización de los datos es demasiado alto, incluso para los países en desarrollo, ya que una Internet fragmentada repercutirá negativamente en las tecnologías emergentes, por ejemplo, serán más sesgadas si dependen de un conjunto limitado y homogéneo de datos para transformar estos en información.

No obstante, aunque apoyan la libre circulación de los datos por el supuesto costo de su localización, los autores no consideran los efectos distributivos de los beneficios de esa libre circulación, que es un aspecto crítico para el desarrollo. Esos beneficios, por ejemplo del comercio electrónico, tienden a

[6] Varios grupos de reflexión (como el European Centre for International Political Economy, la Information Technology and Innovation Foundation y la Hinrich Foundation, entre otros) apoyan firmemente la libre circulación de los datos, motivados principalmente por argumentos económicos y comerciales.

favorecer especialmente a sectores y personas que ya son privilegiados en lo que respecta al acceso a los mercados internacionales o a las competencias. Esto podría agravar la desigualdad existente dentro de los países y entre ellos (Hill, 2018; Avila, 2020).

Aunque en general están a favor de la libre circulación de los datos, Mitchell y Mishra (2019) proponen una revisión del marco de la Organización Mundial del Comercio (OMC) con normas que permitan una aplicación gradual. De esta manera, los países en desarrollo podrían ampliar sus capacidades para aplicar las nuevas normas de regulación de datos y construir infraestructuras digitales antes de estar obligados por las normas de la OMC. Además, el marco que proponen obligaría a los países desarrollados a proporcionar asistencia técnica para subsanar ese déficit de capacidad. Por otro lado, algunas investigaciones abogan por la libre circulación de los datos como defensa de los derechos humanos, la libertad de expresión y la democracia (Bauer y otros, 2013; Chander y Lê, 2015).

Por su parte, algunas organizaciones internacionales (especialmente la OCDE, el Banco Mundial y el Foro Económico Mundial (FEM)) apoyan la libre circulación de los datos, haciendo especial hincapié en el comercio y como medio para crear valor (Casalini y López González, 2019; Daza Jaller y otros, 2020; Mattoo y Meltzer, 2018; Nguyen y Paczos, 2020; Spiezia y Tscheke, 2020; WEF, 2019; World Bank, 2021). La motivación para que los flujos de datos transfronterizos sean relativamente libres es su contribución al crecimiento económico y a la cooperación internacional (World Bank, 2021), que requieren un sistema de intercambio de datos lo menos trabado posible, y que idealmente no conduzca a una mayor fragmentación entre países. Aunque gran parte de los trabajos se centran relativamente en el comercio, Spiezia y Tscheke (2020) señalan que, al margen de los datos comerciales, no se dispone de mucha información sobre los tipos de datos que cruzan las fronteras. Tal vez habría que reconsiderar las posiciones ante la libre circulación de los datos no relacionados con el comercio.

Los agentes del sector privado con publicaciones sobre los flujos de datos transfronterizos son un grupo selecto. En su mayoría tienen intereses comerciales internacionales y, por tanto, suelen estar a favor de la libre circulación de los datos. Les incentiva el mantenimiento y crecimiento de sus negocios. Relacionan la limitación de los flujos de datos con las medidas proteccionistas (BDI, 2017). Otro elemento común es que apoyan en cierto modo la existencia de normas de seguridad y privacidad de los datos (BSA, 2017; Global Data Alliance[7], 2020; GSMA, 2018a, 2018b; Microsoft, 2018). Es probable que esto se deba a la necesidad de confianza, tanto de los consumidores como de los reguladores. Las publicaciones en este contexto consisten principalmente en declaraciones que subrayan la importancia de la libertad de los flujos de datos transfronterizos, con poco fondo analítico (BSA, 2017; Global Data Alliance, 2020; International Chamber of Commerce, 2021).

Las perspectivas de la sociedad civil presentan más matices en sus posiciones ante la libre circulación de los datos. Algunos autores radicados en los Estados Unidos defienden firmemente los flujos de datos transfronterizos como contribución a la economía, y abogan por la celebración de negociaciones comerciales para imponer normas vinculantes sobre los flujos de datos (Castro y McQuinn, 2015; Cory, 2017, 2019). Otros prestan una mayor atención a la necesidad de disponer de reglas y normativas que acompañen esos flujos. Esas reglas y normativas adoptan diferentes formas, como normas técnicas comunes para garantizar la seguridad (McLaughlin y Castro, 2019) o un entorno regulador adecuado que abarque la protección de datos, la ciberseguridad, la responsabilidad jurídica y la interoperabilidad entre países (WEF, 2020b). Por tanto, su objetivo es permitir el intercambio de datos en el marco de unas directrices claras para proteger a las personas.

Los agentes de la sociedad civil que se centran en los países en desarrollo se muestran más cautos ante la libre circulación de los datos. Si se impone esa libre circulación a los países a través de los acuerdos comerciales, los países en desarrollo podrían salir perdiendo (Hilbig, 2018). En consecuencia, estos acuerdos pueden limitar el alcance de las políticas nacionales y los enfoques específicos de cada país en materia de desarrollo (Our World is Not for Sale, 2019). Además, para que los países en desarrollo se beneficien de la economía digital, necesitan encontrar la manera de mantener en su territorio el valor

[7] La Global Data Alliance se creó a principios de 2020 para defender la libertad de los flujos de datos transfronterizos. Véase *Medianama*, 23 de enero de 2020, "Cross-industry global coalition launched to advocate for free flow of data across borders".

económico de los datos, lo que podría requerir medidas proteccionistas temporales o un mejor marco para la propiedad y remuneración de los datos (Gurumurthy y otros, 2017; Hill, 2018; James, 2020). A falta de mejores normas nacionales, en particular sobre la fiscalidad de las empresas tecnológicas internacionales, es probable que aumenten las diferencias de ingresos y los problemas de privacidad, por lo que se afianzarán las dependencias (Kilic y Avila, 2019; Raghavan, 2018). Por consiguiente, no precipitarse en la formulación de políticas podría garantizar una distribución más justa de los beneficios obtenidos gracias a los datos (Trade Justice Movement, 2020).

Mayer (2020) defiende un enfoque cauteloso ante la libre salida de los datos sobre las preferencias de los consumidores de los países en desarrollo. Desde la perspectiva de una política industrial basada en los datos, las empresas nacionales podrían utilizar los datos sobre las preferencias de los consumidores en materia de fabricación para crear productos novedosos destinados a nuevos segmentos del mercado interno. Este tipo de política industrial limitaría la salida del país de determinados datos y, en consecuencia, contribuiría al desarrollo económico con una menor dependencia de la industrialización orientada a la exportación. Asimismo, Singh (2019) destaca la necesidad de contar con una política industrial para que los datos nacionales contribuyan a la creación de valor dentro del país y así se fomente el desarrollo de la industria digital. Foster y Azmeh (2020) y Ciuriak (2018) destacan también la relevancia de la política industrial para el desarrollo en la economía digital impulsada por los datos.

Por el contrario, Mitchell y Mishra (2019) dudan que la brecha digital pueda cerrarse si los países en desarrollo no tienen acceso a servicios digitales internacionales y relativamente baratos. Reconocen, no obstante, la distribución asimétrica de la propiedad intelectual y las tecnologías instrumentales para beneficiarse de los datos, que pertenecen principalmente a empresas de los países desarrollados, por lo que contar con una política industrial en la esfera de los datos podría resultar atractivo.

F. ALCANCE DE LA INVESTIGACIÓN

Los intereses comerciales y empresariales ocupan un lugar destacado en una gran parte de las publicaciones actuales. En consecuencia, su enfoque y análisis son relativamente limitados, ya que no se tienen en cuenta otras dimensiones de los datos. Dado que estos estudios suelen posicionarse a favor del libre comercio y los mercados globales integrados, los argumentos relativos a los flujos de datos transfronterizos también están orientados a esos objetivos.

Spiezia y Tscheke (2020) analizan el efecto de la pertenencia conjunta a acuerdos internacionales sobre los datos en el comercio de servicios y mercancías. Los autores reconocen sus limitaciones, porque su análisis empírico se centra en el comercio pero los datos no están vinculados únicamente a esa esfera. Sopesan el reto de determinar el valor asociado a los flujos de datos y medirlo debidamente, al tiempo que reconocen la dificultad de valorar correctamente otros factores, como la privacidad. En consonancia con la preocupación por la privacidad, Mattoo y Meltzer (2018) analizan diferentes opciones de regulación para determinar cuál es la mejor para permitir la libre circulación de los datos y proteger, al mismo tiempo, la privacidad de los datos personales. Defienden que cada país apruebe una normativa específica en materia de privacidad. Por tanto, los autores no apoyan la inclusión de componentes relacionados con la privacidad de los datos en los acuerdos de libre comercio y defienden más bien la celebración de acuerdos específicos de cooperación internacional entre reguladores, como el ahora invalidado Escudo de la Privacidad Unión Europea-Estados Unidos. Asimismo, Nguyen y Paczos (2020) evalúan el valor económico de los flujos de datos, lo que orienta sus argumentos hacia los efectos positivos de estos flujos.

El informe de políticas de Think20 (T20) sobre la libre circulación de los datos se basa en la teoría microeconómica, donde la mano invisible del mercado contribuye a su equilibrio (Chen y otros, 2019). Por tanto, sin fallos de mercado, la libre circulación de los datos sería la mejor opción. Las intervenciones políticas que impiden la libre circulación de los datos solo están justificadas si su objetivo es solucionar los fallos de mercado, como la competencia imperfecta, o por motivos no económicos, como las cuestiones sociales, incluidas las relacionadas con la privacidad y la seguridad. En consecuencia, en el informe de políticas se indica primero que la libre circulación de los datos representa la mejor opción y que, como segunda opción, se podría estudiar la regulación.

Tomiura y otros (2019) llevaron a cabo una encuesta sobre el efecto de la regulación de los flujos de datos transfronterizos en las empresas japonesas. No parece que adoptasen ninguna posición con respecto a las restricciones. El objetivo de la encuesta era determinar la importancia de los flujos de datos para las empresas encuestadas. Sin embargo, la redacción del texto parece indicar una preferencia implícita por la libre circulación de los datos internacionales. Los autores solo evalúan las repercusiones negativas de la regulación en las transferencias de datos preguntando si los negocios con las regiones sometidas a la regulación se redujeron, se desviaron a otro lugar o se interrumpieron. Dada la decisión de adecuación adoptada por la Unión Europea con respecto al Japón, también se podría haber dado un mayor intercambio de datos, conforme a las conclusiones de Spiezia y Tscheke (2020).

Algunos análisis empíricos parecen asumir de entrada que la regulación de los flujos de datos afectan negativamente al comercio y al PIB, y que las medidas para limitar los flujos de datos constituyen una amenaza para la idea fundacional de Internet (Chander y Lê, 2015; McLaughlin y Castro, 2019). Varios estudios también rechazan la idea de que la restricción de los flujos de datos internacionales sirve para apoyar el desarrollo de una industria nacional de datos; en realidad, tendería a aumentar los costos para las empresas locales, en particular para las más pequeñas, limitaría las opciones para los consumidores y pondría en peligro la seguridad de los datos (Badran, 2018; Chander y Lê, 2015; Cory, 2017; McLaughlin y Castro, 2019; Castro y McQuinn, 2015). En general, los análisis se centran demasiado en destacar los efectos negativos.

Las asociaciones sectoriales y los agentes del sector privado centran su argumentos todavía más en dichos efectos negativos, presumiblemente para reforzar sus intereses. Su premisa es que hay que apoyar los flujos de datos transfronterizos de la mejor manera posible. En consecuencia, presentan informes de políticas, que suelen contener pruebas o análisis empíricos limitados, en lugar de sopesar las ventajas y desventajas. La Federación de Industrias Alemanas considera que los datos son el principal elemento impulsor de la cuarta revolución industrial (Industria 4.0) y, en ese sentido, la circulación fluida de los datos es esencial para mantener la competitividad de sus miembros. Por tanto, cualquier acuerdo de libre comercio debería limitar las restricciones a los flujos de datos, que la Federación considera una nueva forma de proteccionismo (BDI, 2017). Del mismo modo, la Global Data Alliance describe las esferas (ciberseguridad, privacidad y aplicación de la ley) que apoya para fomentar la confianza del consumidor y posibilitar la actividad empresarial, la innovación y el crecimiento en todos los sectores (Global Data Alliance, 2020). GSMA, la asociación de proveedores de redes móviles, deja clara su postura en el título de una de sus publicaciones, “Flujos de datos transfronterizos: aprovechamiento de los beneficios y eliminación de las barreras” (GSMA, 2018a). Sostiene que los flujos de datos brindan más posibilidades a las personas, las empresas y las organizaciones al aumentar las opciones de los consumidores y reducir los costos operacionales de los operadores de redes que trabajan a través de las fronteras. Sin embargo, los operadores móviles están sujetos a normas específicas que limitan sus posibilidades de utilizar estas economías de escala a través de las fronteras, debido a las medidas relacionadas con la localización de los datos en red (GSMA, 2018b). De manera análoga, Microsoft expone las razones por las que disponer de una sólida infraestructura en la nube es la mejor manera de responder a muchos de los principales retos actuales de carácter social, económico y ambiental, y establece una hoja de ruta (Microsoft, 2018). Estas perspectivas tienen en común que no examinan los efectos distributivos de los beneficios generados por los flujos de datos transfronterizos.

Mientras que gran parte de la investigación apoya la libertad de los flujos de datos transfronterizos para sustentar el comercio (y, a su vez, la productividad, la innovación y el PIB), Aaronson (2014, 2019a) adopta un enfoque más amplio y considera que la propia importancia de contar con una Internet abierta es pertinente para los derechos humanos, la política exterior y la seguridad (Aaronson, 2014). Además, Aaronson (2019a) examina el papel de los datos como recurso económico de forma más amplia que la analogía a menudo utilizada de “los datos son el nuevo petróleo”. Muestra también que la gobernanza de los flujos de datos sigue fragmentada, por lo que es necesario que los Gobiernos desarrollen un nuevo enfoque al respecto. Este podría proporcionar un marco para defender la libertad de Internet con directrices más claras, que hasta la fecha no abordan la mayoría de las normativas y acuerdos de libre comercio (Aaronson, 2014).

En conclusión, la mayor parte de las publicaciones no analizan ampliamente el papel de los flujos de datos transfronterizos en la economía y la sociedad, ni sus posibles ventajas y desventajas de forma equilibrada. Más bien, la mayoría de los estudios parecen inclinarse hacia un objetivo predeterminado, que a veces se indica de manera específica, pero que en la mayoría de los casos corresponde encontrar a quien los lee.

G. LA PERSPECTIVA DE DESARROLLO DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

La investigación sobre los flujos de datos transfronterizos está estrechamente vinculada al apoyo que prestan sus autores a empresas con grandes flujos de datos. Esto se refleja en el origen geográfico y lingüístico de los estudios más innovadores sobre la cuestión: están fuertemente dominados por autores anglófonos de países desarrollados. La regulación nace, en cierta medida, de la necesidad de mantener la ventaja competitiva de los agentes nacionales (Aaronson y Maxim, 2013). Las investigaciones se corresponden con esa necesidad.

Dado que los países desarrollados dominan la investigación, hay relativamente pocos ejemplos de publicaciones que se centren en la relación entre los flujos de datos y el desarrollo. Hasta la fecha, los países en desarrollo han sido más consumidores que productores en la economía impulsada por los datos (Aaronson, 2019a) o es probable que salgan perdiendo (Hilbig, 2018). Las brechas digitales que aún persisten, en particular con respecto a la capacidad de utilizar los datos para el desarrollo económico, dan a los países desarrollados ventaja en la creación de conocimientos y valor a partir de los datos mientras estos circulan libremente a través de las fronteras (Mayer, 2020).

Badran (2018) lleva a cabo una investigación en cinco países africanos y estima que el impacto de la localización de los datos es considerablemente menor que en los países de la Unión Europea. Aunque, en un principio, esto pueda parecer positivo, es probable que se deba a los menores vínculos y relaciones comerciales con otros países, lo que no es ideal para el desarrollo económico a largo plazo. Además, los efectos adversos de la localización de los datos en África podrían ser especialmente numerosos porque la escasa fiabilidad del suministro energético hace que el funcionamiento de los centros de datos locales sea costoso.

Aaronson (2019a) señala que contribuir al establecimiento de marcos de gobernanza de los datos a nivel mundial puede ser un reto para los países en desarrollo, ya que muchos todavía carecen de las normas, reglas, normativas e infraestructuras adecuadas para la economía impulsada por los datos. Sin un plan a nivel nacional, es difícil que los responsables políticos tomen partido en el debate internacional y, por ejemplo, apoyen el desarrollo de normas interoperables que permitan a los países seguir sus propias estrategias (Aaronson, 2014; Cory, 2017, 2019; Hill, 2018; Mattoo y Meltzer, 2018; Meltzer, 2020; Microsoft, 2018). Dado que los Estados Unidos y la Unión Europea han establecido normas estrictas sobre la libre circulación o la protección de los datos, respectivamente, los países en desarrollo pueden verse atrapados en el medio y sentirse obligados a inclinarse por uno de los dos enfoques, ya que cuentan con menor poder de negociación (Aaronson y Maxim, 2013). El Banco Mundial (World Bank, 2021) subraya la necesidad de que los países de ingreso bajo participen en mayor medida en las negociaciones sobre el comercio digital y la gobernanza de los datos. El resultado de esas negociaciones no debe suponer una carga excesiva de carácter reglamentario, financiero y de capacidad para los países con el fin de que estos puedan cumplir las nuevas normas.

A pesar de lo dicho, algunos estudios analizan las oportunidades que pueden aprovechar los países en desarrollo. La perspectiva de desarrollo implícita de Cory (2019) es que la innovación se ve impulsada por el intercambio de ideas y datos, así como por el acceso a soluciones más económicas, como la computación en nube. En consecuencia, los países en desarrollo saldrían ganando con una normativa que maximice el potencial de innovación al permitir la libre circulación de los datos. Este punto de vista coincide con el de Chen y otros (2019). Estos autores señalan que, a medida que los habitantes de los países en desarrollo utilizan cada vez más la tecnología de las comunicaciones con un gran volumen de datos, va aumentando la necesidad de esos países de contar con un marco regulador que les permita aprovechar ese potencial de crecimiento económico.

En el contexto de los países en desarrollo, la mayor parte del debate sobre los flujos de datos transfronterizos y el desarrollo se centra en la India, que cuenta con una industria de servicios digitales relativamente grande, con vínculos de gran importancia en el extranjero. Los estados de la India con los sectores de tecnología de la información más desarrollados tienen un nivel de vida superior y atraen más inversión extranjera directa. Asimismo, las exportaciones de servicios digitales más importantes se asocian a una mayor innovación en términos de patentes registradas y número de empresas emergentes. Por tanto, la India es un ejemplo de los beneficios que brinda la libre circulación de los datos. CUTS International (Gupta y otros, 2020) utiliza modelos de restricciones a los flujos de datos y concluye que son adversas para el desarrollo, pues provocan una caída considerable de las exportaciones de servicios digitales y del PIB. No obstante, la utilización de la India como ejemplo para obtener información sobre el desarrollo de otros países podría ser válida solo hasta cierto punto. El gran tamaño del país y su clase media con buena formación y anglófona son factores clave que impiden que la experiencia india se reproduzca en muchos otros países. Estos podrían verse limitados por su pequeño mercado interno, que les impide desarrollar una economía digital nacional moderna (Deardorff, 2017; World Bank, 2021).

Algunas investigaciones reconocen que el nivel de preparación de los países difiere, pero no entran a analizar los diferentes efectos que podrían tener en los países en desarrollo determinados enfoques de gobernanza de los flujos de datos, o si esos enfoques podrían impulsar eficazmente el desarrollo (BSA, 2017; McKinsey, 2014).

Mientras los países en desarrollo no puedan fomentar su propio desarrollo en la esfera digital, la limitación de sus capacidades y sus medios financieros genera en ellos una nueva dependencia. Este “colonialismo digital” se observa también en las medidas que aplican las principales empresas tecnológicas para inclinar el debate político a su favor mediante grupos de presión, inversiones en infraestructuras y donaciones de hardware y software a los países en desarrollo (Avila, 2020).

En consecuencia, la capacidad de los países para tomar sus propias decisiones y adoptar políticas sobre los datos y los flujos de datos (es decir, su soberanía sobre los datos) está cobrando importancia (Hilbig, 2018; McLaughlin y Castro, 2019; Avila, 2020; Taylor, 2020), aunque la definición y la motivación de la soberanía sobre los datos pueden variar mucho de un país a otro (De La Chapelle y Porciuncula, 2021). Varios autores proponen que, para poner en práctica esta independencia, se preparen hojas de ruta con el objetivo de mejorar la gobernanza de los datos y crear entornos propicios (Aaronson, 2019a; Ademuyiwa y Adeniran, 2020; Chen y otros, 2019; GSMA, 2018b; WEF, 2020b). Además, dentro de los países, sugieren enfoques multilaterales para configurar el marco de gobernanza según las prioridades de las empresas y otros agentes. En consecuencia, varias publicaciones centran sus hojas de ruta en los marcos de privacidad, los entornos compatibles con la nube y la facilitación global del flujo de datos a través de las fronteras (GSMA, 2018b; Microsoft, 2018; WEF, 2020b). Su perspectiva de desarrollo consiste en reconocer que cada país debe recorrer su propio camino hacia el mejor entorno regulador. Uno de los principales factores que impiden establecer reglas y normativas actuales y sacar provecho de ellas son los escasos conocimientos técnicos en la materia, como confirman los responsables políticos encuestados en Asia (GSMA, 2018b). Por su parte, el FEM (WEF, 2020b) propone una hoja de ruta de muy alto nivel pero omite los detalles acerca de su aplicación. Ademuyiwa y Adeniran (2020) analizan específicamente los problemas de gobernanza de los datos que los países africanos deben solucionar para desarrollar un sector digital, digitalizar su economía e integrarse en la cadena mundial de valor de los datos con el fin de aprovechar las ventajas de la economía digital. Destacan el papel de las reglas y normativas en materia de defensa de la competencia, fiscalidad, y privacidad y seguridad de los datos, así como de las aptitudes.

La cooperación internacional en lo que respecta a los flujos de datos transfronterizos también es clave. Aunque es importante que los países dispongan de margen para formular normas acordes a sus necesidades individuales, la cooperación es imprescindible debido al carácter internacional de los flujos de datos. Aaronson (2019a) recomienda la creación de una organización internacional que fomente los flujos de datos transfronterizos y contribuya a formular normas comunes que faciliten la circulación de esos datos entre los países. En ese mismo sentido, GSMA (2018a) señala que sería mejor legislar esos flujos a nivel regional para crear zonas con pocas limitaciones, como ocurre en la Unión Europea.

Prácticamente todas las escasas publicaciones que tienen en cuenta una perspectiva de desarrollo han sido escritas en inglés por especialistas de países avanzados, en su mayoría. Por ejemplo, en el caso de América Latina, las publicaciones que estudian los flujos de datos transfronterizos en el contexto de los análisis sobre el comercio digital han sido escritas por Cory y Castro (2018), Meltzer (2018) y Suominen (2018). Aguerre (2019) es una de las pocas excepciones, al tratarse de una experta latinoamericana. Las perspectivas de otras lenguas y esferas también podrían ser útiles para ampliar el alcance del debate. Por ejemplo, hay algunos trabajos interesantes en relación con la geografía de los datos en francés, como el de Cattaruzza (2019).

H. INCONVENIENTES DE LAS PUBLICACIONES ACTUALES

Aunque las publicaciones presentan tendencias positivas que pueden contribuir a los debates políticos, también contienen ciertas deficiencias. Preocupan las suposiciones implícitas que muchos autores hacen antes de argumentar su postura basándose en esas suposiciones. La principal suposición es que las restricciones de los flujos de datos no son deseables. Por ejemplo, Tomiura y otros (2019) estudian solo los efectos negativos de la regulación de los flujos de datos. Aunque eso sería correcto tomando como base la teoría económica, que da por sentado que el mercado conduce a resultados eficientes, no se tienen en cuenta las imperfecciones del mercado (como las tendencias monopolísticas o los valores sociales) que podrían generar otros resultados. Desde una perspectiva más técnica, las suposiciones que sustentan los modelos de equilibrio general y sus calibraciones pueden limitar la posibilidad de generalizar las conclusiones a muestras de países diferentes (Badran, 2018; Bauer y otros, 2013, 2016; Ferracane y van der Marel, 2020; Ferracane y otros, 2020).

Es importante definir mejor los datos (así como las economías, las sociedades y el entorno general que afectan) para avanzar en los debates sobre la medición y sobre sus implicaciones políticas. Uno de esos debates es el relativo a los flujos de datos como forma de comercio y a si los acuerdos de libre comercio deben legislar a nivel internacional la circulación de los datos a través de las fronteras. Una parte considerable de las publicaciones se centra en los datos y el comercio, especialmente en la configuración de las normas internacionales en las negociaciones comerciales (Aaronson, 2014; Bauer y otros, 2013; BDI, 2017; Castro y McQuinn, 2015; Cory, 2017; Microsoft, 2018; Nicholson y Noonan, 2017). No cabe duda de que este es un tema importante para los flujos de datos transfronterizos. Sin embargo, tanto Burri (2016) como Mattoo y Meltzer (2018) rechazan que la negociación de estos flujos deba tener lugar en el ámbito de las negociaciones comerciales, ya que estas últimas tienen un carácter demasiado unilateral o dejan de lado a agentes relevantes, como la comunidad de la gobernanza de Internet.

La definición de los derechos sobre los datos también es importante para que los datos y sus flujos resulten más manejables. Habida cuenta de la creciente importancia de los flujos de datos transfronterizos, Linden y Dahlberg (2016) analizan si la libre circulación de los datos debe convertirse en una de las esferas de "libre circulación" que ocupan un lugar central en el mercado interno de la Unión Europea. De esa manera, los datos estarían al mismo nivel que las mercancías, los servicios, los capitales y las personas en lo que respecta a la libre circulación. Aunque los autores concluyen que la libre circulación de los datos podría tratarse más bien de una libertad subsidiaria, hay que seguir debatiendo sobre la naturaleza de los flujos de datos para delimitar mejor esta cuestión.

Además, como se ha indicado, la perspectiva de desarrollo no se contempla debidamente en las publicaciones. Esto entraña el reto añadido de que tal vez ciertas propuestas de gobernanza de los datos no sean fácilmente aplicables en todos los países. McLaughlin y Castro (2019) y Hilbig (2018) postulan que los países deben ser soberanos para legislar en materia de datos, pero no proponen cómo lograrlo. Asimismo, quienes piden un nivel adecuado de protección de los datos no indican cómo se podría evaluar ese nivel (Global Data Alliance, 2020). Por último, algunas de las hojas de ruta podrían ser difíciles de aplicar, ya que requieren ideas sobre cómo subsanar el déficit de capacidad para introducir y orientar el proceso político (Ademuyiwa y Adeniran, 2020; Microsoft, 2018; WEF, 2020b).

I. CONCLUSIÓN Y PERSPECTIVAS

El repaso de las publicaciones que se presenta en este capítulo revela varias limitaciones y lagunas:

- Las publicaciones actuales todavía tienen dificultades para definir los datos y los flujos de datos transfronterizos, lo que obstaculiza el debate constructivo sobre su gobernanza.
- Existen importantes problemas en lo que respecta a la medición de los flujos de datos transfronterizos.
- Hay pocas publicaciones sobre los diferentes tipos de datos, y las taxonomías utilizadas no abordan debidamente las implicaciones de las diferentes categorizaciones para los flujos de datos transfronterizos.
- La mayoría de las publicaciones analizan los flujos de datos transfronterizos desde una perspectiva comercial. Algunas analizan los problemas transfronterizos de privacidad pero, en términos generales, no hay estudios multidimensionales de los flujos de datos transfronterizos.
- Hay muy pocos análisis equilibrados que sopesen las ventajas y desventajas de las diferentes opciones políticas en relación con los flujos de datos transfronterizos. Muchos estudios contienen una clara tendencia ideológica y suposiciones implícitas que sustentan sus argumentos. Los estudios tienden a partir de una posición predeterminada en favor de la libre circulación de los datos, por un lado, o de la localización de los datos, por otro. En esos casos, el objetivo de la investigación es básicamente justificar la posición adoptada.
- Desde una perspectiva de desarrollo, hay pocos datos empíricos que respalden las posiciones favorables a la libre circulación de los datos a través de las fronteras o a las políticas estrictas de localización de los datos. La mayoría de los estudios que defienden la libre circulación tratan de estimar el impacto negativo de las restricciones a la circulación de los datos en términos de costo de oportunidad. Sin embargo, es posible que ese enfoque no incorpore las cuestiones relacionadas con la equidad y la distribución, es decir, con quién se apropia de las ganancias. También es posible que no tenga en cuenta las dimensiones no económicas de los datos, como la privacidad y la seguridad.
- Asimismo, los argumentos de quienes defienden la aplicación de políticas estrictas de localización de los datos como contribución al desarrollo nacional son frágiles. No está claro que el mantenimiento de los datos dentro de las fronteras nacionales redunde en un desarrollo económico o social.
- La falta de pruebas que sustenten una u otra postura se debe, en parte, a los problemas de medición y, en parte, al hecho de que la economía digital impulsada por los datos y la explosión de los flujos de datos transfronterizos son fenómenos relativamente recientes.
- La bibliografía está compuesta principalmente por estudios anglófonos, publicados predominantemente en países desarrollados o, cuando se centran en el mundo en desarrollo, sobre todo dedicados a la India.
- Por último, pero no por ello menos importante, no se hace especial hincapié en la relación existente entre los flujos de datos transfronterizos y el desarrollo. Asimismo, es bastante frecuente que, cuando se introduce la perspectiva de desarrollo, la analicen especialistas de países desarrollados. Hay pocos estudios sobre el tema realizados en países en desarrollo distintos de la India.

En general, estas conclusiones indican la existencia de importantes lagunas en la bibliografía sobre los flujos de datos transfronterizos y el desarrollo, lo que también influye en los debates políticos. En este contexto, el siguiente capítulo da un paso atrás y trata de sentar algunas bases para analizar de manera más amplia e inclusiva los flujos de datos transfronterizos.

En vista de las lagunas en la bibliografía y los debates sobre los flujos de datos transfronterizos que se han subrayado en el capítulo II, en este capítulo se da un paso atrás para analizar los fundamentos de los datos y su circulación a través de las fronteras. Esto significa que se revisan sus definiciones, conceptos y características. Sin un entendimiento común de lo que son los datos y los flujos de datos transfronterizos, y de las complejas interconexiones existentes en la economía de los datos, es difícil ponerse de acuerdo sobre sus implicaciones, o sobre las políticas que deben ponerse en marcha con miras a aprovechar los datos para el desarrollo.

Este capítulo pone de relieve que los datos son multidimensionales, por lo que debe aplicarse un enfoque holístico en su gobernanza. Sobre la base del análisis de las tendencias expuesto en el capítulo I, se señala que los datos pueden generar valor tanto privado como social, pero que la creación de valor requiere el acceso a grandes cantidades de datos y las capacidades y habilidades necesarias para transformarlos en inteligencia digital. El resultado depende, entre otras cosas, del tipo de datos de que se trate y de la manera en que se recopilan, analizan y comparten. Los desequilibrios de poder y las desigualdades existentes en relación con los flujos de datos transfronterizos suscitan preocupación por las posibles consecuencias para los países en desarrollo.

VOLVER A LO FUNDAMENTAL: CUESTIONES CLAVE

III

CAPÍTULO III QUÉ SON LOS DATOS Y LOS FLUJOS DE DATOS TRANSFRONTERIZOS Y CUÁLES SON SUS IMPLICACIONES PARA EL DESARROLLO

Los datos son multidimensionales

Dimensión económica

Recopilación → Almacenamiento → Análisis

Valor privado
(por ejemplo, a través de la publicidad digital selectiva, las plataformas digitales y los servicios de datos

Valor social
(por ejemplo, cambio climático o salud)

Dimensión no económica

- Privacidad
- Otros derechos humanos
- Seguridad

Cuestiones clave

Los datos son **diferentes de los bienes y servicios**, y sus flujos son diferentes del comercio

Las repercusiones de los flujos de datos transfronterizos varían según el **tipo de datos**

Más que la propiedad de los datos, lo que importa son los **derechos de acceso, control y uso de los datos**

La **ubicación de los datos** depende de diversos factores que hay que tener en cuenta

El acceso a los datos y su uso son fundamentales para el **desarrollo**

Unas pocas **corporaciones digitales globales** tienen un **acceso privilegiado** a los datos y **capacidades únicas** para convertir los datos en inteligencia digital

La **preparación** de los países **difiere en lo que respecta** a su capacidad de aprovechamiento de los datos para el desarrollo

Los **países en desarrollo** corren el riesgo de convertirse en **meros proveedores de datos**, mientras que tienen que pagar por la inteligencia digital producida con sus datos

Se necesitan políticas públicas

Maximizar el beneficio de la economía de datos y minimizar los riesgos que entraña

Garantizar una distribución equitativa de los beneficios

Tener en cuenta las complejas concesiones que hay que realizar al elegir entre las distintas opciones políticas

La simplificación excesiva que representa la reivindicación de la libre circulación de los datos o de su localización estricta probablemente no sea útil: se necesitan soluciones intermedias

La gobernanza mundial de los datos debe regirse por un enfoque holístico, multidimensional, pangubernamental y multilateral

A. INTRODUCCIÓN

La relación entre los datos y el desarrollo puede entenderse de dos maneras diferentes, pero interconectadas e igual de importantes. En primer lugar, los datos se pueden utilizar para fundamentar las decisiones y los procesos encaminados a la consecución de objetivos económicos, sociales y ambientales. Desde esta perspectiva, la relación entre el uso de los datos y el desarrollo es bastante sencilla. La mayor disponibilidad de datos gracias a los avances en las tecnologías digitales puede contribuir significativamente a la consecución de los Objetivos de Desarrollo Sostenible al proporcionar mejores datos empíricos para tomar las decisiones. Esto se refleja en diferentes casos vinculados a la reducción de la pobreza, la salud, el medio ambiente y el cambio climático, el transporte, la energía o la agricultura (World Bank, 2021).

En segundo lugar, los datos pueden formar parte de los propios procesos de desarrollo económico, dentro de la cadena de valor de los datos, ya que se han convertido en un recurso económico clave. En este sentido, el desarrollo se produce como resultado de la adición de valor a los datos mediante el procesamiento de los datos brutos para convertirlos en inteligencia digital (producto de datos). El concepto de datos para el desarrollo corresponde, en este caso, al papel que pueden desempeñar como motor del desarrollo (en términos de valor añadido económico interno en los países en desarrollo, que es lo que constituye el desarrollo económico). En este contexto, garantizar los beneficios de los datos para el desarrollo se convierte en una tarea más complicada.

> En términos de desarrollo económico, es importante garantizar que los países en desarrollo puedan captar debidamente el valor de los datos extraídos de su ciudadanía y sus organizaciones.

Dado que los datos se han convertido en la savia de la economía digital, y que pueden generar importantes beneficios para el desarrollo de los distintos agentes económicos (pero, sobre todo, debido a su naturaleza de bien público, para la sociedad en su conjunto), la compartición de los datos es deseable para reforzar sus efectos positivos y abordar los posibles riesgos (OECD, 2019a). La compartición de datos facilitando el acceso para la mayoría de la ciudadanía con el fin de maximizar los beneficios potenciales en la medida de lo posible implica que los datos deben circular, no solo a nivel nacional, sino también internacional. En este contexto, es importante examinar los diversos tipos de datos que pueden tener diferentes implicaciones en lo relativo al acceso, incluidos los datos que cruzan fronteras.

En términos de desarrollo económico, es importante garantizar que los países en desarrollo puedan captar debidamente el valor de los datos extraídos de su ciudadanía y sus organizaciones. Los beneficios económicos de los datos y los flujos de datos transfronterizos no son automáticos, ni se distribuyen uniformemente entre los países y dentro de ellos (UNCTAD, 2019a); el libre juego de las fuerzas del mercado no conduce a resultados eficientes y equitativos. Por tanto, las políticas públicas desempeñan un importante papel. Sin un sistema internacional adecuado de regulación de los flujos de datos transfronterizos, las plataformas digitales globales y las empresas líderes de las cadenas mundiales de valor disfrutan de un acceso privilegiado a los datos, controlan enormes cantidades de ellos y están en una posición especialmente buena para apropiarse de las ganancias potenciales. También pueden obstaculizar la generación de posibles beneficios sociales limitando el acceso a los datos. Esto repercute considerablemente en la desigualdad y afecta a las perspectivas de desarrollo. En consecuencia, desde un punto de vista económico, es importante examinar el valor privado y social de los datos, además de la distribución del valor creado a partir de los datos, dentro de los países y entre ellos, para que sea equitativa.

Los datos tienen un impacto significativo no solo en términos de valor económico; también hay que examinar los aspectos no económicos de los datos que tienen importantes efectos en las personas y la sociedad y no pueden desvincularse de la economía debido a la naturaleza particular de los datos. Los flujos de datos transfronterizos presentan muchas implicaciones complejas en diversos ámbitos que

se deben estudiar y comprender en profundidad para poder utilizarlos con fines de desarrollo. Puede haber razones legítimas para que los datos permanezcan dentro de las fronteras nacionales, aparte de garantizar que la economía nacional pueda beneficiarse debidamente de esos flujos, como la protección de la privacidad y otros derechos humanos y las cuestiones de seguridad. También hay que tener en cuenta los importantes desafíos que plantea el abuso y el uso indebido de los datos. La necesidad de minimizar esos riesgos y desafíos, que afectan en gran medida a la confianza de los usuarios, apunta hacia la protección de los datos mediante diferentes salvaguardias y políticas con el fin de controlar los flujos de datos transfronterizos.

En consecuencia, los datos y los flujos de datos, tanto nacionales como internacionales, pueden aportar muchos beneficios, que deberían promoverse y distribuirse de forma equitativa, en lugar de que sean acaparados por unas pocas empresas y países. Al mismo tiempo, hay muchos riesgos y desafíos que deben abordarse detenidamente. Todos ellos afectan a las personas, que cada vez más son el origen de los datos, y a las empresas privadas, tanto grandes como pequeñas, además de a los Gobiernos y a la sociedad civil. En consecuencia, es importante que todo el mundo reflexione detenidamente sobre cuáles son las principales cuestiones en juego en relación con los datos y los flujos de datos transfronterizos desde la perspectiva del desarrollo, y cuáles son las implicaciones para la formulación de políticas. Es indispensable estudiar las múltiples interconexiones y los vínculos subyacentes entre los datos y el desarrollo para comprender mejor los flujos de datos transfronterizos desde el punto de vista de las políticas.

> Los datos y los flujos de datos transfronterizos pueden aportar muchos beneficios, que deberían distribuirse de forma equitativa y no ser acaparados por unas pocas empresas y países, mientras que hay muchos riesgos y desafíos que deben abordarse detenidamente.

En este contexto, y en vista de las lagunas en la bibliografía y los debates sobre los flujos de datos transfronterizos que se han puesto de manifiesto en el capítulo II, en el presente capítulo se da un paso atrás con el fin de comprender mejor las principales cuestiones pertinentes para los flujos de datos transfronterizos y el desarrollo partiendo de los elementos fundamentales. De hecho, el punto de partida es la definición y las características de los datos introducidos en el capítulo I, que en el presente capítulo se desarrollan más exhaustivamente. En la sección B se examinan las formas de recopilación y uso de los datos. A continuación, en la sección C se analizan las diferentes dimensiones de los datos que añaden importantes complejidades al análisis de los datos y los flujos de datos transfronterizos. Las cuestiones relacionadas con la propiedad, el acceso al control y los derechos sobre los datos se estudian en la sección D. En la sección E se analiza la forma en que circulan los datos y la relevancia de la ubicación de su almacenamiento, mientras que en la sección F se examinan los diferentes tipos de datos y sus implicaciones para los flujos de datos transfronterizos. En la sección G se analizan los desequilibrios de poder y las desigualdades resultantes de los flujos de datos transfronterizos. La posición de los países en desarrollo en la cadena internacional de valor de los datos se examina en la sección H. Las cuestiones de soberanía relacionadas con estos flujos, a diferentes niveles, se abordan en la sección I. En la sección J se ponen de relieve los conflictos de intereses y las concesiones que hay que realizar al elegir entre las distintas opciones políticas que surgen en este contexto. A continuación, en la sección K se examinan las capacidades necesarias para aprovechar los datos y, por último, se presentan las conclusiones en la sección L.

B. RECOPILACIÓN DE DATOS, ELABORACIÓN DE PERFILES Y USO DE LA INFORMACIÓN

Cualquier dato que circule por Internet puede ser recopilado. Como se ha comentado en el capítulo I, los datos pueden recopilarse a través de diferentes canales, como los navegadores, las aplicaciones móviles o los dispositivos de la Internet de las cosas. Esos datos pueden ser personales, pero también

geoespaciales, meteorológicos, de sensores (entre máquinas) y de tráfico, entre otros. Pueden suministrarse de manera voluntaria, como en el caso de la información personal para registrarse en un servicio web o los datos obtenidos con una encuesta realizada en línea. Sin embargo, a menudo los datos recopilados y analizados son datos observados, como las visitas de páginas web, la ubicación o la dirección del protocolo de Internet (IP), pero también pueden incluir información técnica sobre el dispositivo conectado, como su sistema operativo o la dirección de control de acceso a los medios. Con el acceso adecuado, también es posible interceptar cualquier dato enviado a través de Internet, como correos electrónicos u otros mensajes de texto, voz o vídeo, o la comunicación de los dispositivos de la Internet de las cosas, como los refrigeradores o los timbres conectados a Internet[1].

Para algunos fines, es importante recopilar datos que puedan utilizarse como identificadores (que vinculen la información a una persona concreta). Los identificadores son datos que apuntan a una persona o un dispositivo específico (únicos), no cambian fácilmente (persistentes) y son fácilmente accesibles (disponibles)[2]. No todos los identificadores presentarán las tres características, pero algunos que sí lo hacen son los nombres, las direcciones de correo electrónico o los números de teléfono. La identificación es fundamental para determinar el grado de anonimización de los datos, que es relevante para distinguir entre datos personales y no personales. Sin embargo, aunque la tecnología de anonimización de los datos está evolucionando, el grado de anonimización sigue siendo una cuestión controvertida, como se comenta a continuación.

Los datos pueden recopilarse por diferentes motivos (como el desarrollo de productos y servicios, la publicidad selectiva y la vigilancia) y su autorización puede basarse en acuerdos de servicio, políticas de uso, requisitos legales o solicitudes. Las entidades que poseen, controlan o tienen acceso a la infraestructura clave de Internet (por ejemplo, los puntos de intercambio de tráfico de Internet (IXP)), los sitios web, los servidores web o los programas informáticos (sistemas operativos y aplicaciones) pueden recopilar datos sin depender de terceros. Entre estas entidades se encuentran los propietarios de sitios web, las plataformas de comercio electrónico o de medios sociales, los desarrolladores de aplicaciones, los desarrolladores de sistemas operativos, los proveedores de servicios de Internet (PSI), los Gobiernos y los piratas informáticos. Los datos también pueden obtenerse indirectamente, por ejemplo, por conducto de corredores de datos, órdenes judiciales u otros requerimientos legales, o comprarse en la web oscura.

En el contexto de la economía de los datos, surgen nuevos términos y un gran número de nuevos agentes pertinentes. Entre esos agentes se encuentran los titulares de los datos, que pueden definirse como la persona viva (o entidad) identificada o identificable a la que se refieren los datos personales[3]; y los corredores de datos, a saber, empresas que agregan información de diversas fuentes, la procesan para enriquecerla, limpiarla o analizarla, y transmiten las correspondientes licencias a otras organizaciones[4]. Otros agentes relacionados con los datos son los agregadores, los analistas y los controladores de datos, que determinan los fines y los medios del tratamiento de los datos personales[5].

> Una cuestión relevante que se plantea con respecto a la recopilación y el rastreo de los datos es si las ingentes cantidades de datos recopilados son necesarias para el funcionamiento de los servicios, o si existe una recopilación excesiva de datos.

1 Por ese motivo, las transferencias de datos están cada vez más encriptadas, por ejemplo, con el paso del inseguro HTTP (protocolo de transporte de hipertexto) al más seguro HTTPS (protocolo seguro de transporte de hipertexto).

2 Véase Electronic Frontier Foundation, 2 de diciembre de 2019, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, disponible en www.eff.org/wp/behind-the-one-way-mirror.

3 Este concepto se ha generalizado con el RGPD. En otros reglamentos tal vez utilicen términos diferentes. Por ejemplo, en la India, el titular de los datos es la persona a la que se refieren los datos.

4 Véanse las definiciones, disponibles en https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/#subject y www.gartner.com/en/information-technology/glossary/data-broker.

5 Véase Comisión Europea, "¿Qué es un responsable o encargado del tratamiento?", disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_es.

En cuanto a la recopilación de datos con fines comerciales, cabe distinguir entre la recopilación y el rastreo de datos de origen y por parte de terceros. Las plataformas en línea más grandes recopilan enormes cantidades de datos cada vez que se utilizan sus servicios. La recopilación de datos por las empresas a través de sus propios productos y servicios se denomina "rastreo de origen". Estos datos pueden recopilarse con arreglo a un consentimiento implícito o explícito. Sin embargo, también pueden recopilar datos partes distintas del sitio web o del servicio con el que el usuario interactúa directamente, lo que se conoce como "rastreo de terceros". Por ejemplo, Facebook también recopila información sobre los usuarios de otros sitios web y aplicaciones con sus "píxeles de conversión" invisibles, y Google utiliza datos de ubicación para rastrear las visitas de los usuarios a las tiendas físicas[6]. De hecho, hay muchos corredores de datos y agencias de publicidad en línea que rastrean la navegación por la web y el uso de los dispositivos que se realizan cada día. La mayor parte del rastreo de terceros está diseñado para crear perfiles de personas y entidades que puedan utilizarse en la publicidad selectiva. En el recuadro III.1 se detallan algunas de las formas más habituales de rastreo en Internet. Determinadas plataformas digitales importantes están revisando las prácticas de rastreo, lo que podría tener implicaciones en la privacidad y la competencia. Está por ver el impacto positivo de esos cambios en la privacidad.

Recuadro III.1. Rastreo en Internet

El rastreo del comportamiento en línea puede realizarse de múltiples formas, y las herramientas y técnicas evolucionan constantemente. A continuación se indican algunos de los métodos más comunes que se utilizan actualmente:

Cookies de rastreo

Una *cookie* es la información que guarda un navegador cuando alguien visita un sitio web con el fin de poder reconocer el dispositivo en el futuro. Las *cookies* pueden tener diferentes propósitos, entre ellos rastrear el comportamiento en línea de un usuario, por ejemplo, para personalizar la navegación o para ofrecer publicidad selectiva. Las cookies de rastreo pueden ser colocadas por el sitio web de destino (*cookies* de origen) o por sus asociados (*cookies* de terceros), y contienen identificaciones que permiten determinar quiénes son los usuarios y rastrearlos en Internet. Cada vez que un usuario vuelve a conectarse a un sitio web, el navegador envía la información de la cookie, como los clics, las preferencias de compra, las especificaciones del dispositivo, las ubicaciones y el historial de búsqueda. En los últimos años se ha intensificado el debate sobre el uso de *cookies* de terceros, que actualmente bloquean algunos de los navegadores más utilizados, como Mozilla Firefox, Safari y pronto también Google Chrome.

Balizas web

Las balizas web son imágenes diminutas de un solo píxel que rastrean el comportamiento del usuario en los sitios web o los correos electrónicos. Al abrir una página web o un correo electrónico que contenga esas balizas, el navegador o el lector de correo electrónico descarga la imagen, para lo cual el dispositivo debe enviar una solicitud al servidor donde se almacena esa imagen. Esta solicitud automática proporciona información que permite obtener datos sobre el dispositivo del usuario, como su dirección IP, la hora de la solicitud, el tipo de navegador o lector de correo electrónico que realizó la solicitud y la existencia de *cookies* enviadas anteriormente por el servidor anfitrión. El servidor anfitrión puede almacenar toda esta información y asociarla a la de otros rastreadores o identificadores.

Registro de la huella digital del dispositivo

Una forma aún más intrusiva de rastreo es el registro de la huella digital del navegador o el dispositivo. Consiste en la recopilación de información sobre el *hardware* y el *software* de un dispositivo concreto a través de un *script* (una lista de comandos que ejecuta un determinado programa) activado en segundo plano cuando se visita un sitio web. Esos *scripts* pueden determinar el sistema operativo del dispositivo, el navegador u otros programas instalados, el uso de un bloqueador de anuncios, el huso horario, el idioma, la resolución y la profundidad de color de la pantalla, las extensiones instaladas en el navegador e incluso especificaciones técnicas más detalladas sobre la tarjeta gráfica y los controladores *(drivers)*. Todos estos diferentes atributos, en su conjunto, proporcionan una huella digital única con la que el dispositivo puede ser identificado y rastreado, incluso sin utilizar *cookies* o cuando la dirección IP está oculta.

Dispositivos móviles

Se utilizan técnicas similares para rastrear el uso de las aplicaciones en los dispositivos móviles. Aunque las aplicaciones móviles no pueden acceder a las cookies de la misma manera que los rastreadores web, pueden

[6] Véase la nota 58.

aprovechar la forma en que funcionan los sistemas operativos móviles y acceder a identificadores únicos que les permiten vincular la actividad a un dispositivo específico. Además, en las aplicaciones móviles no es posible conceder un privilegio sin conceder el mismo privilegio a todo el código de terceros que se ejecuta dentro de ella. Algunos sistemas operativos móviles, como la actualización iOS 14.5 de Apple, han empezado a incluir recientemente una opción para que los usuarios bloqueen el rastreo de las aplicaciones.

Rastreo por los proveedores de servicios de Internet

Aparte del rastreo por los sitios web de origen y de terceros, los proveedores de servicios de Internet también pueden controlar las actividades en línea, ya que todo el tráfico de un usuario se dirige a través de los servidores de su proveedor. Analizando la información de NetFlow, un proveedor de servicios de Internet puede recopilar información sobre el sitio web que se está visitando, el tiempo que se pasa en ese sitio web y otra información básica sobre la conexión y el tipo de datos que se transfieren. La inspección profunda de paquetes puede proporcionar al proveedor aún más información. Siempre que el sitio web de que se trate no utilice una comunicación cifrada, el proveedor puede controlar básicamente todo, desde el nombre de usuario y las contraseñas hasta los productos que se compran y los números y direcciones de las tarjetas de crédito cuando se introducen para pagar y seleccionar el modo de entrega. Incluso cuando se visita un sitio web utilizando una comunicación cifrada, el proveedor puede conocer el sitio web de destino. Además, los proveedores pueden analizar el tráfico de Internet y sus metadatos, como el tamaño, el tipo, la hora de envío y el destino de los paquetes de datos. Esto significa que los proveedores de servicios de Internet pueden llegar a recopilar más datos personales que Facebook o Google.

Fuente: UNCTAD, con información obtenida de Electronic Frontier Foundation, 2 de diciembre de 2019, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, disponible en www.eff.org/wp/behind-the-one-way-mirror; TechCrunch, 19 de junio de 2020, Oracle's BlueKai tracks you across the web. That data spilled online, disponible en https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/; Avast, 14 de mayo de 2021, Corredores de datos: todo lo que necesita saber, disponible en https://www.avast.com/es-es/c-data-brokers?redirect=1; Información para consumidores de la Comisión Federal de Comercio de los Estados Unidos, mayo de 2021, Cómo proteger su privacidad en línea, disponible en https://www.consumidor.ftc.gov/articulos/como-proteger-su-privacidad-en-linea; Goodwill Community Foundation, Understanding browser tracking, disponible en https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/; Proton Technologies AG, How to protect your data from your ISP, disponible en https://protonvpn.com/blog/is-your-isp-selling-your-data/; StackExchange, My ISP uses deep packet inspection; what can they observe?, disponible en https://security.stackexchange.com/questions/155057/my-isp-uses-deep-packet-inspection-what-can-they-observe.

Una cuestión relevante que se plantea con respecto a la recopilación y el rastreo de los datos es si las ingentes cantidades de datos recopilados son necesarias para el funcionamiento de los servicios, o si existe una recopilación excesiva de datos. Esto es importante porque una gran parte de los datos son observados, y a menudo se recopilan sin el consentimiento ni el conocimiento del usuario. Podría argumentarse que, al aceptar las condiciones del servicio, el usuario ha aceptado esa recopilación de datos. Sin embargo, este consentimiento supuestamente "informado" es muy discutible, puesto que las condiciones de los servicios se suelen presentar de manera opaca, muy a menudo en un lenguaje largo y complejo. Además, el consentimiento se presenta en forma de "tómalo o déjalo", por lo que el usuario no tiene más opción que aceptar las condiciones. En principio, las condiciones de servicio deberían ser más sencillas y claras para que los usuarios sepan qué han aceptado, y no debería haber una recopilación excesiva de datos innecesarios. Sin embargo, esto último es bastante difícil, ya que los datos tienen un valor de "opción" o potencial, que solo se materializa una vez que son procesados y utilizados. Por ello, la recopilación de algunos datos es especulativa y se realiza sin conocer exactamente su uso posterior. Siempre habrá que llegar a una solución intermedia para conjugar las prácticas de consentimiento con la innovación en los servicios basados en datos.

Aunque la recopilación y el rastreo de datos son objeto de preocupación en sí mismos, lo más importante es su finalidad (para qué se utilizan los datos), que es lo que determinará su valor, así como sus efectos positivos y negativos en las personas y la sociedad. Como ya se ha mencionado, los datos pueden utilizarse con fines de desarrollo, como el aumento general de la eficiencia y la productividad. Los datos son un ingrediente esencial para nutrir la inteligencia artificial, y se utilizan para crear perfiles de personas o entidades. Las empresas y las organizaciones pueden emplear los datos, la información generada por ellos y los perfiles creados para mejorar sus productos y personalizar sus servicios, facilitando así

la interacción de sus clientes y usuarios con ellos, así como con fines publicitarios. De este modo, las empresas que recopilan los datos pueden generar importantes beneficios mediante su monetización. En cuanto a los efectos negativos, las empresas y los Gobiernos que controlan los datos pueden manipular las interacciones y las opiniones mediante el uso de herramientas de economía de la atención y economía conductual, lo que puede generar efectos no deseados para la sociedad. De este modo, esos perfiles pueden constituir un abuso y un uso indebido de los datos que pueden provocar, por ejemplo, discriminaciones, ya que pueden utilizarse para diferentes actividades (como la contratación de personal, los seguros, los préstamos bancarios y los servicios sociales) de manera muy opaca. También pueden darse discriminaciones por motivos de género y raza, ya que los datos y los algoritmos pueden presentar sesgos. La disponibilidad de grandes cantidades de datos es clave para producir inteligencia digital valiosa, pero la calidad de esa inteligencia también depende de la calidad de los datos utilizados.

En general, las personas se convierten en el producto al "transformarse" en datos a medida que se digitalizan cada vez más sus actividades y acontecimientos en lo que se ha denominado la "economía de la vigilancia" (Clarke, 2019). La inteligencia digital derivada de los datos se convierte en mercancía y, como los datos reflejan las actividades y los comportamientos de las personas, estas también se asimilan en cierto modo a la mercancía. Así, en todo el mundo la economía de mercado está dejando paso a la sociedad de mercado a causa de la digitalización, que permite que el mercado domine cada vez más aspectos de la vida.

C. EL CARÁCTER MULTIDIMENSIONAL DE LOS DATOS

Para comprender debidamente el papel de los datos en la economía y la sociedad, así como sus propiedades fundamentales, hay que examinar sus diferentes dimensiones. Esta sección pone de relieve el carácter multidimensional de los datos, no solo como recurso económico por su valor privado y social, sino también en relación con aspectos no económicos, como la privacidad y otros derechos humanos, y la seguridad. En todas sus dimensiones, que están interconectadas y deben considerarse como un todo, los datos se han convertido en un recurso estratégico para las personas, las empresas y los países. Dado que esas dimensiones no pueden disociarse, para formular políticas adecuadas no se pueden abordar las cuestiones relativas a los datos con un planteamiento compartimentado, aunque se puede hacer hincapié en cada una de las dimensiones en función de las preferencias y tener en cuenta las repercusiones interdimensionales.

1. La dimensión económica de los datos

Una idea clave que subyace en gran parte del debate sobre los datos es que estos se han convertido en un *recurso económico* clave. La economía digital se define cada vez más por los activos intangibles, donde nuevos aspectos de las organizaciones (como los conocimientos, la propiedad intelectual y el código digital) son ahora fundamentales para adquirir una ventaja competitiva (Haskel y Westlake, 2017). Esto alienta a las organizaciones a recopilar, combinar y procesar cada vez más datos para generar valor económico (UNCTAD, 2019a; Mayer-Schönberger y Cukier, 2013). Los datos han surgido como un recurso especialmente importante para los principales modelos de negocio en la economía digital. Por ejemplo, los modelos de negocio de las plataformas se basan en los datos y, mediante los análisis, dan lugar a un círculo virtuoso de mejoras basadas en los datos y una mayor producción de estos (Gawer, 2014). Los modelos de negocio que giran en torno a la inteligencia artificial y los algoritmos son inviables sin datos que alimenten los modelos y sistemas.

Desde esta perspectiva, se puede hacer hincapié en diferentes aspectos económicos fundamentales de los datos. Los datos pueden considerarse una *mercancía* con la que se puede comerciar; no obstante, la posible comerciabilidad de los datos es muy discutible, sobre todo en lo que se refiere a los datos brutos. Es difícil establecer los derechos de propiedad o la titularidad de los datos, entre otras cosas, porque son bienes no rivales, lo que implica que muchas personas pueden utilizarlos simultáneamente, y suelen ser un reflejo de las personas y sus comportamientos (véase más adelante). Además, como los datos brutos individuales solo tienen un valor de "opción" potencial —ya que el valor económico en la economía

digital impulsada por los datos se materializa solo después de la agregación de los datos brutos, su transformación en productos de datos y su monetización—, no existe un mecanismo adecuado de formación de los precios del mercado de datos brutos. Asimismo, el valor de los datos cuando se utilizan —una vez procesados— es muy contextual. En consecuencia, no existen mercados de datos brutos debidamente desarrollados y formalizados, lo que implica que estos datos no se pueden comprar ni vender directamente y no existe una demanda y una oferta adecuadas. Como señala el Banco Mundial (World Bank, 2021:32), "aunque los intercambios bilaterales privados de datos están consolidados en determinados segmentos (concretamente, el comercio de datos personales para la publicidad selectiva), hasta ahora no existen mercados multilaterales abiertos de datos, y muchos intentos de crear ese tipo de mercados de datos han fracasado". La inteligencia digital resultante del procesamiento de los datos es la que se puede monetizar y comercializar; en consecuencia, las referencias a los mercados de datos suelen corresponder sobre todo a los mercados de esos productos de datos.

> Más allá del valor económico privado de los datos, desde la perspectiva de desarrollo, también es crucial examinar el valor social de los datos.

Los datos también se pueden considerar *capital* (Sadowski, 2019; Tang, 2021), pero, de nuevo, es principalmente la inteligencia digital la que se puede considerar capital, un activo que puede mejorar el funcionamiento de una empresa y generar riqueza. Habida cuenta del papel que los datos están desempeñando como aspecto central de la toma de decisiones en las organizaciones y la sociedad, los datos también se pueden considerar una *infraestructura*, que es cada vez más crucial para las operaciones a nivel organizacional, sectorial, regional o nacional (OECD, 2015); esto está muy relacionado con el valor social de los datos, que se analiza más adelante (Kawalek y Bayat, 2017). Los datos también se pueden considerar *trabajo*, ya que representan frecuentemente actividades realizadas por humanos (Arrieta-Ibarra y otros, 2018). Aunque las personas generan muchos datos, son las empresas privadas las que los suelen recopilar, agregar y procesar. Este desajuste entre la creación individual y el control de la empresa ha dado lugar a un debate sobre si las personas reciben una compensación justa por su "trabajo gratuito" de creación de datos. Esos debates se han intensificado a medida que los datos de los usuarios se han convertido en la base de la rentabilidad de muchas de las mayores corporaciones digitales globales. La perspectiva laboral de los datos podría entonces conducir a un estudio más detenido de los individuos/productores de datos, por ejemplo, examinando si tienen suficiente poder de negociación para obtener una parte justa del valor de su trabajo (Aaronson, 2019a). Esto también tiene implicaciones para la tributación en la economía digital en lo que respecta a la determinación del lugar de creación y tributación del valor, porque la digitalización complica la tributación de las actividades al no ser necesaria la presencia física para su ejecución.

Más allá del valor económico privado de los datos, desde la perspectiva de desarrollo, también es crucial examinar el valor social de los datos[7]. Como se ha comentado en el capítulo I, los datos tienen características especiales porque son bienes no rivales, aunque pueden tener distintos grados de excluibilidad. Los datos suelen entrañar externalidades positivas o negativas. La mayor parte del valor de los datos es relacional, derivado de la comparación o agregación de datos; los datos tomados individualmente no tienen ningún valor. Debido a las externalidades de los datos, los mercados suelen proporcionar muy pocos datos con efectos positivos y demasiados datos con efectos perjudiciales para la sociedad. Además, los datos son coproducidos entre la persona o entidad que los origina y el propietario de la tecnología que los recopila. Así, el valor de los datos para la economía y la sociedad en su conjunto es diferente del valor comercial para las empresas privadas que los recopilan y explotan: algunos tipos de datos presentan características de bien público. El tratamiento de los datos como bien público también se justificaría por el hecho de que una gran parte de la tecnología que utilizan las corporaciones digitales fue resultado de la investigación

[7] Para un examen más detallado del valor social de los datos, véase el proyecto de la Nuffield Foundation titulado "Valuing data: foundations for data policy", disponible en www.nuffieldfoundation.org/project/valuing-data-foundations-for-data-policy. En cuanto al carácter de bien público de los datos, véase también MacFeely (2020a).

pública, y por los efectos de la red, que son colectivos. Ese tratamiento permitiría configurar la economía digital de una manera que atienda las necesidades públicas (Mazzucato, 2018).

Además, como se analiza más adelante, los datos proporcionan ventajas competitivas y un gran poder de mercado a las corporaciones digitales, lo que provoca desequilibrios de poder y desigualdad. En consecuencia, no es probable que los mecanismos de mercado generen resultados eficientes o equitativos para la sociedad, lo que lleva a la necesidad de formular políticas públicas. Esas políticas deben tener como objetivo garantizar que la creación de valor (privado y social) a partir de los datos se maximice y se distribuya equitativamente en la sociedad, tanto a nivel nacional como internacional, y evitar al mismo tiempo los posibles riesgos que pueda entrañar.

> Los datos proporcionan ventajas competitivas y un gran poder de mercado a las corporaciones digitales, lo que provoca desequilibrios de poder y desigualdad.

Si bien para maximizar el valor social de los datos es necesario que se compartan más como resultado de las políticas públicas, los datos favorables al bien o interés público pueden ser recopilados o generados tanto por el sector privado como por el público. Los datos generados por el sector público se comparten normalmente con la sociedad en general, mediante múltiples iniciativas de datos abiertos en todo el mundo. Al formular políticas para la compartición de los datos, así como al regular los flujos de datos transfronterizos, será importante distinguir si es el sector privado o el público el que los recopila, porque su tratamiento y las consecuencias difieren.

En cuanto a los flujos de datos transfronterizos, lo que importa es si el carácter de bien público de los datos tiene implicaciones fuera de las fronteras nacionales. Esto entraña que los datos generados en un país también pueden aportar valor social en otros países, para lo que habría que compartir los datos a nivel internacional. En este contexto, se pueden señalar diferentes ejemplos de desafíos para el desarrollo que son de carácter mundial. La situación creada por la pandemia de COVID-19 ha demostrado claramente la importancia de compartir los datos sanitarios a nivel mundial para hacer frente a sus consecuencias e investigar una vacuna. La compartición internacional de datos también puede ser útil para el medio ambiente[8]. El uso de los datos para abordar este tipo de desafíos mundiales requiere permitir los flujos de datos transfronterizos. Sin embargo, hay que tener en cuenta que, a nivel internacional, afrontar los riesgos asociados a la compartición de datos puede resultar aún más complicado. Además, a nivel internacional, es necesario que las políticas públicas aborden los desequilibrios entre los países que se derivan de los flujos de datos transfronterizos.

2. Las dimensiones no económicas de los datos

Las dimensiones no económicas de los datos se refieren principalmente al respeto de los derechos humanos, así como a cuestiones de seguridad nacional. La *dimensión de derechos humanos* de los datos surge al examinar el origen de los datos y vincularlos a los derechos y las protecciones fundamentales, ya que los datos suelen representar actividades y comportamientos de usuarios o entidades. Cuando las organizaciones tienen grandes cantidades de datos, la cuestión importante es su interacción con los derechos humanos fundamentales y la protección de las personas (Singh y Vipra, 2019). En concreto, hay declaraciones generales sobre los derechos humanos, como la Declaración Universal de Derechos Humanos de las Naciones Unidas, que abarcan el derecho a la privacidad (artículo 12), entre otros relevantes para la esfera de los datos (Heeks y Renken, 2018). Además de la protección de la privacidad, la Hoja de Ruta del Secretario General para la Cooperación Digital (United Nations, 2020a) incluye la vigilancia, la represión, la censura y el acoso en línea como aspectos importantes relacionados con los

[8] Véase, por ejemplo, Jha y Germann (2020) y Royal Society (2021) para los datos sanitarios, y UNEP (2020) para los datos ambientales.

derechos humanos en lo que respecta a las tecnologías digitales basadas en los datos[9]. Otros derechos humanos pertinentes son la libertad de opinión y de expresión (artículo 19).

A medida que se generan datos cada vez más detallados sobre las personas, pueden surgir tensiones entre esos derechos fundamentales y los datos que se tienen sobre las personas. La privacidad también debe analizarse desde una perspectiva colectiva, ya que los datos de una persona pueden revelar información sobre otras[10]. El análisis de los datos desde el punto de vista de los derechos se centraría entonces en esas cuestiones de derechos humanos de forma más destacada y estudiaría la protección de los derechos humanos fundamentales dentro del tratamiento de los datos de una persona, así como el ejercicio de los derechos y el control de los procesos por parte de las personas. Esta perspectiva de derechos humanos también se refleja en las discriminaciones (por ejemplo, por motivos de género y raza) que pueden surgir a causa de la inteligencia artificial, la vigilancia y la manipulación de las técnicas de datos. Además, la vigilancia y la manipulación de datos pueden afectar a los derechos humanos democráticos e incluso influir en los sistemas políticos. La influencia en la política puede afectar a su vez a la economía, ya que las políticas económicas aplicadas dependen de las autoridades políticas elegidas y de los regímenes políticos[11].

El abuso y uso indebido de los datos por las organizaciones que los controlan (ya sea el sector privado o los Gobiernos) y su impacto en los derechos humanos afectan a la confianza de los usuarios y limita los posibles beneficios que puedan derivarse de la economía digital impulsada por los datos. Por ejemplo, las dudas en relación con el respeto de los derechos humanos han limitado el uso de las aplicaciones digitales de rastreo de contactos para ayudar a evitar los contagios de COVID-19[12]. Sería bueno que las políticas garantizaran el respeto de los derechos humanos para aumentar la confianza. Además, desde la perspectiva del sector privado, tratar los datos con el respeto de los derechos humanos en mente puede presentar una ventaja competitiva por sus efectos en la reputación de la empresa.

> El carácter multidimensional de los datos, desde el punto de vista económico y no económico, pone de relieve importantes aspectos y puntos de vista sobre los datos y los flujos de datos que no pueden abordarse de manera inconexa.

Los datos también tienen una *dimensión de seguridad* que hay que tener en cuenta. Los datos pueden representar actividades de interés para la seguridad nacional y el orden público, así como para la cultura y los valores nacionales. A medida que se codifican cada vez más actividades dentro de los datos, la naturaleza de los flujos de datos adquiere interés para los encargados de la seguridad y el cumplimiento de la ley. Garantizar la seguridad y la protección de los datos producidos por las organizaciones clave (como las fuerzas armadas o las pertenecientes a las infraestructuras críticas) es cada vez más importante para la seguridad nacional. Esta perspectiva sobre los datos puede solaparse a menudo con la perspectiva económica. Por ejemplo, las normas de seguridad nacional de los países con un mayor enfoque geopolítico podrían centrarse tanto en la protección de los secretos comerciales y la propiedad intelectual de las organizaciones nacionales como en las actividades nacionales críticas.

A medida que los datos se han ido generalizando, también sirven para controlar la delincuencia y el cumplimiento de la ley. Por tanto, la accesibilidad y la jurisdicción de los datos son cada vez más importantes

9 Véase el trabajo de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) sobre "el derecho a la privacidad en la era digital", disponible en https://www.ohchr.org/SP/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Para otros instrumentos internacionales y regionales importantes de derechos humanos en los que se reconoce el derecho a la privacidad, véase Privacy International, 23 de octubre de 2017, What is Privacy?, disponible en https://privacyinternational.org/explainer/56/what-privacy. Véanse también los informes anuales del ACNUDH sobre la libertad de opinión y de expresión, disponibles en www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx.

10 Véase, por ejemplo, Véliz (2019) y Viljoen (2020), para más información sobre la naturaleza colectiva de la privacidad.

11 Para una descripción exhaustiva de la relación entre los datos y los derechos humanos, véase Ebert, Busch y Wettstein (2020).

12 Véase, por ejemplo, Lewis (2020); Algorithm Watch, Digital contact tracing apps: do they actually work? A review of early evidence, disponible en https://algorithmwatch.org/en/analysis-digital-contact-tracing-apps-2021/; y Back y otros (2021).

para las fuerzas del orden. Los datos también pueden ser relevantes en las cuestiones de seguridad nacional. En algunos países, los flujos de datos (por ejemplo, los que incorporan determinados medios o aplicaciones) pueden contravenir las normas culturales o morales, o tener un carácter políticamente conflictivo que lleve a su censura.

En resumen, el carácter multidimensional de los datos, desde el punto de vista económico y no económico, pone de relieve importantes aspectos y puntos de vista sobre los datos y los flujos de datos que no pueden abordarse de manera inconexa. Por consiguiente, los responsables políticos deben enfocar los flujos de datos transfronterizos de forma holística, teniendo en cuenta todas las diferentes dimensiones. No cabe duda de que se puede hacer más o menos hincapié en una u otra dimensión según las prioridades políticas, pero es importante reconocer los efectos que cualquier medida puede tener en cada una de las dimensiones. Por ejemplo, la regulación de los flujos de datos transfronterizos solo desde la perspectiva del comercio no tendrá en cuenta otros factores relacionados con la privacidad o la seguridad, lo que muy probablemente puede dar lugar a una normativa inadecuada. Para analizar holísticamente los datos y las políticas conexas, en particular en el caso de los flujos de datos transfronterizos, es indispensable entender cómo se complementan o entran en conflicto las diferentes dimensiones de los datos. Al mismo tiempo que se tiene en cuenta la naturaleza multidimensional de los datos, es importante garantizar que las dimensiones no económicas no se utilicen como excusa para aplicar políticas que tengan repercusiones económicas y afecten a las perspectivas de desarrollo de los países en desarrollo.

El carácter multidimensional de los datos también pone de manifiesto que es difícil concluir con claridad si los flujos de datos transfronterizos tienen un efecto neto positivo o negativo para los países en desarrollo. Los datos se copian, trasladan, agregan y reutilizan rápidamente en diferentes entornos, y tienen múltiples usos simultáneos. Los datos generados por un dispositivo médico, por ejemplo, se podrían utilizar tanto para mejorar el tratamiento de una persona como para contribuir a los observatorios mundiales de la salud que apoyan el desarrollo; no obstante, los mismos datos también pueden ayudar a una empresa a crear modelos de riesgo que excluyan de la cobertura sanitaria a las personas marginadas.

D. PROPIEDAD, ACCESO, CONTROL Y DERECHOS SOBRE LOS DATOS

Para entender la naturaleza particular de los datos, también es importante analizar las cuestiones de la propiedad, el acceso, el control y los derechos sobre los datos. Aunque existe un amplio debate sobre la "propiedad" de los datos, este no es el concepto realmente importante en este ámbito. El establecimiento de los regímenes jurídicos aplicables a los datos presenta importantes complicaciones (Correa, 2020)[13] dadas las características específicas de estos, entre ellas que son bienes intangibles, no rivales, coproducidos y con un valor relacional. En términos económicos, esto implica que no se debe pensar directamente que los datos son semejantes a los bienes económicos convencionales y recurrir a ciegas a los modelos de escasez económica, oferta y demanda. De hecho, como ya se ha mencionado, no existen mercados multilaterales propiamente dichos en el caso de los datos (brutos). Esas propiedades también son fundamentales para la definición de los datos; como representación de un hecho o idea en el mundo, los datos no deben considerarse un bien económico convencional que pueda poseerse. Sin embargo, los datos pueden incorporarse en un conjunto de derechos (de uso, distribución y modificación) que deben ser conformados por las normas y políticas (Heverly, 2003).

> Más que la propiedad, lo que importa son los derechos sobre los datos, es decir, el derecho a acceder, controlar y utilizar los datos.

Además, en relación con su carácter personal o colectivo, los datos representan las acciones y los comportamientos de la persona (o de la comunidad en el caso de los datos colectivos). En consecuencia, tal vez sea más importante estudiar los derechos sobre los datos, que son inalienables o intrínsecos a la persona (o a la comunidad). Así pues, más que la propiedad, lo que importa son los derechos sobre

[13] Véase también Cofone (2020) y Scassa (2018).

los datos, es decir, el derecho a acceder, controlar y utilizar los datos (UNCTAD, 2019a). Esos derechos abarcan el "derecho a acceder, modificar, trasladar o eliminar los datos; y el derecho a saber quién los recopila, dónde están, a dónde van, quién tiene acceso a ellos y con qué fines"[14]. Además, las dificultades que entraña el aplicar el modelo de la propiedad o la titularidad a los datos entrañan que no se pueden comercializar ni intercambiar, solo compartir.

Los principales marcos suelen exponer a grandes rasgos tres principales dominios de datos que se solapan y que están asociados a diferentes tipos de derechos y control (Correa, 2020; OECD, 2020a): los *datos públicos*, utilizados con fines públicos, abarcan los datos que se pretenden utilizar de forma más abierta y, por tanto, pueden estar sujetos a menos derechos y control para apoyar su uso y compartición[15]; los *datos personales*, como representación de hechos o comportamientos sobre las personas, se entrelazan con los derechos humanos fundamentales, por lo que los marcos para los datos personales buscan determinar de qué manera las personas pueden controlar y acceder a los datos recopilados sobre ellas (Duch-Brown y otros, 2017); y los *datos privados de las empresas*, que son datos amparados por un derecho de propiedad intelectual, están menos definidos por los derechos y más por el control. Normalmente, las empresas pueden controlar los datos restringiendo el correspondiente acceso o uso y preservando así la escasez de este recurso económico. Cuando las empresas comercian, compran o utilizan productos de datos de otras empresas, estos pueden estar sujetos a licencias o contratos comerciales. A medida que los datos se han convertido más en un recurso esencial de las empresas y forman parte de las grandes inversiones en capital relacionado con los datos, también se han ejercido presiones para que se instauren normas más estrictas sobre la "propiedad" de los datos con el fin de proteger las inversiones privadas.

Pueden surgir tensiones en la intersección de estos tres dominios básicos de los datos (OECD, 2015). Los datos personales recopilados por el sector privado resultan especialmente complicados. Por un lado, grandes cantidades de datos en línea incorporan información identificativa, y muchas personas se preocupan por la privacidad y por la falta de consentimiento para la recopilación de esos datos (Floridi, 2020). Por otro lado, dado que los datos amparados por un derecho de propiedad intelectual son fundamentales para que las empresas adquieran una ventaja competitiva, estas desean controlar los datos en los que han invertido. Asimismo, podrían surgir tensiones a causa de los datos sobre el medio ambiente recopilados por empresas privadas, y se han levantado voces pidiendo que esos datos sean de dominio público, dado que representan hechos sobre el mundo.

E. LOS FLUJOS DE DATOS TRANSFRONTERIZOS, EL COMERCIO Y LA UBICACIÓN DE LOS DATOS

Cuando hablamos de "flujos de datos transfronterizos" nos referimos a la transmisión de datos de un país a otro. Para que esta transmisión se produzca, los datos se dividen en paquetes, que siguen diferentes rutas dentro de las redes que forman Internet. Como Internet es una red global de redes, estos paquetes de datos fluyen por una infraestructura global y distribuida, es decir, la transferencia de paquetes de datos es de carácter "transfronterizo" (Mishra, 2019). Lo que determina que un flujo de datos sea transfronterizo es el origen donde se encuentra el usuario o cliente y el servidor de destino. Por ejemplo, en el caso de una búsqueda en Google (solicitud) realizada por cualquier usuario fuera de los Estados Unidos, el origen es el lugar donde este se encuentre, y el destino los Estados Unidos. Comprender bien lo que conllevan los flujos de datos transfronterizos es muchas veces complicado, a causa de su carácter global y distribuido; por ejemplo, aunque los datos se transfieran entre dos dispositivos digitales dentro del mismo país, pueden transitar por servidores extranjeros por razones de eficiencia económica o tecnológica. Entender cómo funciona Internet es, por tanto, esencial para analizar la relación entre los flujos de datos transfronterizos y el desarrollo, así como sus implicaciones para las políticas. En el anexo de este capítulo se explica mejor cómo circulan los datos a través de las fronteras.

[14] Véase Privacy International, 6 de febrero de 2019, We don't want to sell our data, we want data rights!, disponible en https://privacyinternational.org/news-analysis/2683/we-dont-want-sell-our-data-we-want-data-rights.

[15] Parece que, en las publicaciones, no está demasiado claro el término "datos públicos". Puede referirse a los datos producidos por el sector público para el uso exclusivo de los responsables políticos o para la sociedad en su conjunto, de manera que se convierten en datos abiertos. Además, según se ha mencionado en la sección sobre los datos como bien público, los datos recopilados por el sector privado también pueden compartirse con la población y utilizarse para el interés público.

Con el fin de comprender mejor los flujos de datos transfronterizos, en esta sección también se analizan dos aspectos clave: las similitudes y las diferencias entre los flujos de datos transfronterizos y el comercio internacional, y las cuestiones relacionadas con la ubicación de los datos.

1. Similitudes y diferencias entre los flujos de datos transfronterizos y el comercio internacional

El marco conceptual para medir el comercio digital de la Organización de Cooperación y Desarrollo Económicos (OCDE), la Organización Mundial del Comercio (OMC) y el Fondo Monetario Internacional (FMI) pone de manifiesto los elementos comunes y divergentes entre el comercio y los datos. En el se señala que "los flujos de datos que no se monetizan directamente no suelen considerarse flujos comerciales en las normas estadísticas actuales; se trata, por ejemplo, de la información personal proporcionada en las redes sociales o los datos recopilados por las empresas en el marco de la 'Internet de las cosas'" (OECD, WTO e IMF, 2020:24); en consecuencia, la información y los datos no monetizados no se consideran comercio digital.

Debido a las características particulares que se han examinado más arriba, los datos requieren un tratamiento diferente al de los bienes y servicios convencionales, en particular en lo que se refiere al flujo internacional de datos. Los datos pueden entenderse mejor como bienes compartidos, más que poseídos o intercambiados (Coyle y otros, 2020), o comercializados. El comercio tradicional puede llevarse a cabo sin flujos de datos significativos, pero el comercio de mercancías o servicios está cada vez más vinculado a los flujos de datos transfronterizos en algunos aspectos. En el comercio de mercancías, el pedido y el pago de los bienes o servicios pueden realizarse digitalmente. En el caso de los bienes y servicios que se digitalizan, estos se pueden tanto pedir como entregar en línea. No obstante, los flujos de datos transfronterizos no pueden relacionarse tan fácilmente con el comercio. Los flujos de datos pueden no estar claramente vinculados a una transacción o monetizarse de forma más indirecta. Los usuarios tal vez utilicen un servicio en línea extranjero de forma gratuita (como los motores de búsqueda, los medios sociales, la emisión de vídeo en directo y la navegación web), pero durante ese proceso se extraen, procesan y monetizan los datos generados sobre ellos, por ejemplo, mediante la publicidad selectiva. Además, a medida que aumenta la integración de los productos y servicios, los flujos de datos transfronterizos duraderos también pueden facilitar los servicios que se prestan en dispositivos como los teléfonos y los sensores.

Independientemente de si están vinculados a flujos comerciales o no, los flujos de datos transfronterizos difieren enormemente en su carácter, velocidad, regularidad y capacidad de seguimiento. Los flujos de datos transfronterizos suelen estar mucho menos asociados de manera clara a una transacción comercial, y en muchos casos no lo están. Un dispositivo móvil, por ejemplo, puede transmitir o recibir flujos de datos sobre su usuario durante un largo período de tiempo simplemente por estar encendido. La velocidad y la regularidad de los flujos de datos transfronterizos también dan lugar a un carácter muy diferente al del comercio internacional. Una sola interacción del usuario en una aplicación puede generar un torrente de diferentes flujos de datos transfronterizos, como los datos de usuario recopilados, los datos solicitados al almacenamiento en la nube y los flujos de datos relacionados con la publicidad y otros usos, a veces entre un conjunto de organizaciones y servicios intermedios. Como los flujos de datos son "fluidos y frecuentes, y la ubicación es difícil de determinar en una red sin fronteras…, el comercio del mismo conjunto de datos puede repetirse en nanosegundos. Los investigadores y los responsables políticos tal vez tengan dificultades para determinar qué es una importación o una exportación, así como cuándo están sujetos los datos a la legislación nacional… y qué tipo de legislación transfronteriza es aplicable" (Aaronson, 2019b:546-547).

> Dadas las diferentes características de los datos en comparación con los bienes y servicios y su carácter multidimensional, los flujos de datos transfronterizos requieren un tratamiento regulador diferente al del comercio.

El comercio internacional y otros flujos económicos internacionales forman parte de sistemas de control y medición consolidados. Sin embargo, no hay una forma clara de aplicar los enfoques del comercio a esos flujos. Las normas que rigen el comercio internacional se basan en las estadísticas correspondientes

a los tipos, valores y ubicaciones de los intercambios (origen y destino) como forma fundamental de regular los flujos. Estos enfoques son difíciles, si no imposibles, de adoptar cuando se quiere seguir la pista de flujos de datos sobre los que no existen estadísticas oficiales. Es complicado determinar el origen y destino de los flujos de datos debido a sus características técnicas, a saber, su frecuencia, su envío como paquetes a través de Internet y el papel de los intermediarios (como las plataformas) que participan en la facilitación de los flujos de datos. Asimismo, la evaluación del valor de los datos y de los flujos de datos es una tarea sumamente complicada, dado que es principalmente un valor "de opción" potencial, que solo se materializa en el momento del uso y es sumamente contextual. Además, los datos suelen ser el subproducto no valorado de la producción y el consumo de bienes y servicios, por lo que es difícil determinar dónde se crea y captura el valor (Slaughter y McCormick, 2021). Por tanto, los enfoques consolidados que se aplican al comercio internacional (por ejemplo, las normas de origen) en diferentes territorios no encajarían en este caso por la naturaleza de los datos y los flujos de datos transfronterizos.

Dadas las diferentes características de los datos en comparación con los bienes y servicios y su carácter multidimensional, los flujos de datos transfronterizos requieren un tratamiento regulador diferente al del comercio internacional. A diferencia del comercio, en muchos países, ciertos tipos de datos (como los datos no personales o no sensibles, que se verán en la siguiente sección) pueden enviarse a través de Internet sin necesidad de registro, aprobación o permiso. La transmisión de otros tipos de datos, incluidos los personales, está sujeta a los regímenes jurídicos de rendición de cuentas. En este caso, no hay obstáculos técnicos a la libre circulación, pero las organizaciones deben cumplir las normas y son responsables si surgen problemas. Por ejemplo, las normativas recientes sobre los datos personales suelen exigir a las organizaciones que se registren oficialmente ante los reguladores (véase también el capítulo V).

2. La ubicación de los datos

La ubicación de los datos viene determinada por una serie de factores, que pueden ser técnicos, económicos, de seguridad, de jurisdicción o de privacidad; también depende de la disponibilidad y fiabilidad de la infraestructura relacionada con los datos y de la energía necesaria para que pueda funcionar[16]. En muchos casos, los flujos de datos son transfronterizos o no según donde se almacenen los datos. Al interactuar con un sitio web o una aplicación, el servidor donde se aloja el contenido o la aplicación puede encontrarse en cualquier parte del mundo. Algunos servicios en línea poseen y operan sus propios centros de datos; otros alquilan espacio en un servidor de otras empresas, como Amazon Web Services, Microsoft Azure o Google. Los servidores también pueden estar situados en un proveedor de servicios de Internet, en una pequeña empresa o en un domicilio particular. A su vez, el servidor de Internet puede almacenar los datos en sus unidades de disco locales o enviarlos a otro servidor que normalmente, aunque no siempre, se encuentra en la misma ubicación. Como se ha comentado en el capítulo I, cada vez se almacenan mayores volúmenes de datos en un número limitado de centros de datos de hiperescala (vinculados a la concentración de importantes servidores, infraestructura y almacenamiento de datos en la nube), una gran parte de ellos en países desarrollados y China.

Técnicamente, los datos viajan a través de la fibra a la velocidad de la luz y para muchas aplicaciones, y no es necesario que el almacenamiento se realice en un lugar específico. Dentro de las aplicaciones o los servicios puede haber peticiones de datos que se transmiten rápidamente. Los modelos de negocio de las grandes empresas tecnológicas tienden a aprovechar esta independencia en lo que respecta a la ubicación del almacenamiento. Las infraestructuras de datos fundamentales prestan servicios a nivel mundial o a una amplia región, con un fuerte predominio de los centros de datos situados en América del Norte y Europa Occidental, que juntos representan casi dos tercios de todos los centros de datos de ubicación conjunta (véase el capítulo I)[17].

[16] Hay que distinguir entre la ubicación de los datos, que es el lugar real donde están los datos, y la localización de los datos, que es una política en el contexto de la regulación de los flujos de datos transfronterizos que impone requisitos para ubicar los datos en un territorio concreto.

[17] La computación en nube y el almacenamiento de datos de bajo costo dependen de las economías de escala, y las decisiones de las empresas sobre la ubicación de estas instalaciones de datos están muy estructuradas en función de diferentes razones, como la situación de riesgo y la disponibilidad de infraestructuras, en particular energía, y las consideraciones relativas a los costos y las cuestiones políticas y reguladoras (Azmeh y otros, 2021).

Aunque el almacenamiento de datos no tiene por qué ser específico de una ubicación, hay argumentos técnicos a favor de una mayor expansión global de las infraestructuras de datos y de almacenamiento. Disponer de una fuente de datos más local puede resultar más económico para las empresas locales. Además, la menor latencia, o tiempo de respuesta a la solicitud, favorece la ubicación de los datos más cerca de su origen (World Bank, 2021). Otros riesgos técnicos, como los cortes esporádicos de fibra y la falta de redundancia, se reducen con una mayor diversidad de centros de datos. Estos argumentos son menos importantes para los datos de bajo ancho de banda o que no se transmiten en tiempo real, pero se convierten en un desafío para una nueva generación de aplicaciones en tiempo real en las que los usuarios requieren flujos de datos muy sensibles a los retrasos o muy interactivos (como las aplicaciones en la nube o la supervisión en tiempo real en la industria).

En estos casos, la proximidad cobra importancia para garantizar la viabilidad de los flujos de datos a gran escala. Esto no implica necesariamente que haya que establecer requisitos de localización de los datos a nivel nacional, pero pone de manifiesto que existen barreras potencialmente sutiles en los flujos de datos transfronterizos en algunas regiones que pueden repercutir en el desarrollo económico. La infraestructura de las grandes empresas tecnológicas, por ejemplo, ha pasado por alto determinadas regiones, como África, que carece de infraestructuras de datos, es decir, de servidores de aplicaciones clave, centros de datos y redes de distribución de contenido (Fanou y otros, 2017; Weller y Woodcock, 2013). Aunque la situación ha mejorado en los últimos años, puede tener repercusiones, por ejemplo, al disminuir el rendimiento de aplicaciones específicas en la nube o aumentar los costos generales para los proveedores de datos (Chetty y otros, 2013). Este argumento a favor del almacenamiento local de los datos se ha examinado con menos frecuencia en el ámbito de las políticas en los países en desarrollo. Más bien se lo justifica como contribución a la seguridad y la economía.

Uno de los argumentos más comunes a favor del almacenamiento local de los datos está vinculado con las cuestiones de jurisdicción y seguridad. Cuando los datos se almacenan fuera de las fronteras de un Estado, se afirma que puede resultar difícil acceder a esos datos por razones legales. Existen tratados de asistencia judicial recíproca que permiten a las naciones acceder a los datos fuera de una jurisdicción, pero no están vigentes entre todos los países. Además, se ha informado de que esas solicitudes tardan entre seis semanas y diez meses, incluso cuando el solicitante son los Estados Unidos (Brehmer, 2018). Hay ejemplos muy destacados en los que el acceso a los datos por razones de seguridad no fue muy fluido. Cabe destacar, en relación con los flujos transfronterizos, el mediático caso de los *Estados Unidos contra Microsoft* de 2017, en el que los tribunales estadounidenses fallaron a favor de Microsoft, que denegaba el acceso del Gobierno de los Estados Unidos a los datos que tenía almacenados en sus centros de datos de Dublín (Irlanda) (Daskal, 2017).

Las implicaciones en términos de ciberseguridad también podrían utilizarse para justificar el almacenamiento local de los datos. Los flujos transfronterizos y el almacenamiento internacional se han vinculado a lo que se percibe como riesgos, ya que las naciones temen la vigilancia de otros Estados o la extracción injustificada de datos nacionales (Meltzer, 2015). Sin embargo, esos argumentos relacionados con la seguridad son muy discutidos. Aunque hay pruebas de que esa vigilancia existe, es poco probable que la localización del almacenamiento de datos ofrezca mejores resultados de ciberseguridad. De hecho, el almacenamiento nacional de datos en muchos países plantea el riesgo de que se establezcan muchos centros de datos pequeños, mal gestionados y costosos (Chander y Lê, 2014). Además, para los ciudadanos preocupados por la seguridad de sus datos personales, el almacenamiento localizado en países con gobiernos autocráticos también puede plantear mayores riesgos de vigilancia que el almacenamiento internacional (Meltzer, 2015). En cuanto a la seguridad, las empresas suelen guardar los datos en ubicaciones diversificadas para minimizar los riesgos.

El almacenamiento local de los datos también se justifica en ocasiones por razones económicas. Estos argumentos son un reflejo de los que se exponen en los debates comerciales convencionales, que sostienen que la producción local contribuye sobremanera al fomento de competencias, la creación de empresas nacionales y el desarrollo en general (Foster y Azmeh, 2020). Siguiendo una línea argumental similar, se ha afirmado que el almacenamiento local de los datos (y la reducción de los flujos de datos transfronterizos) puede contribuir al desarrollo de las infraestructuras y capacidades de datos locales e impulsar la economía digital. La salvedad que cabe anteponer a esos argumentos es que, a diferencia de

la localización de la producción de bienes o servicios, aunque los centros de datos estén ubicados en el país, las actividades asociadas a esos datos pueden seguir realizándose fuera de él. En consecuencia, los beneficios locales directos de los centros de datos nacionales son la creación de un número relativamente pequeño de puestos de trabajo directos, principalmente vinculados a la construcción inicial de los edificios, además de un número reducido de especialistas en ingeniería de redes, personal técnico y personal de seguridad necesarios sobre el terreno (Chander y Lê, 2014).

> La decisión acerca de la ubicación de los datos depende de diferentes factores técnicos, económicos, de seguridad, jurisdiccionales y de privacidad, así como de la disponibilidad de infraestructuras y energía y de su fiabilidad, que pueden incidir en diferentes direcciones y deben evaluarse de manera integral.

Sin embargo, hay quienes sostienen que los efectos indirectos de las inversiones en centros de datos pueden ser más significativos y destacan que, con la presencia de esos centros, surgen otros tipos de capital y capacidad relacionados con los datos. No se han investigado demasiado esos argumentos en los países en desarrollo, pero lo observado en los países desarrollados indica que los centros de datos pueden complementar otras inversiones en infraestructuras de datos y tener importantes efectos indirectos en la economía, por ejemplo, al apoyar la mejora conjunta entre el sector público y el privado de la infraestructura de energía y transporte (NVTC, 2020; Washington State Department of Commerce, 2018; UNCTAD, 2019a). Por tanto, aunque los beneficios económicos directos de la localización de los centros de datos son limitados, en algunos casos la presencia de esos centros de datos podría constituir un elemento importante de un paquete más amplio de inversiones planificadas para desarrollar el capital y la capacidad de un país en materia de datos. Además, aunque los argumentos a favor de la localización nacional de los datos están ganando terreno, las pruebas de esa relación son limitadas.

La estrategia consistente en exigir que los datos se almacenen en el país solo puede funcionar en los grandes países que pueden alcanzar la masa crítica y la escala necesarias para crear valor a partir de los datos. Además, el mantenimiento de los datos dentro de las fronteras únicamente puede conducir al desarrollo económico cuando el país cuenta con capacidad para transformar los datos en inteligencia digital y monetizarlos, como se verá más adelante. Los conocimientos sobre el uso de los datos son más importantes (y pueden desarrollarse localmente) aunque el centro de datos se encuentre en otro lugar; la infraestructura de conectividad también es más pertinente que los propios centros de datos. En el caso de los países más pequeños, se puede generar poco valor a partir de los datos cuando no circulan a través de las fronteras, dado que ese valor se obtiene con su agregación.

Por ello, es más importante centrarse en la ubicación del valor creado a partir de los datos (y su captura), mediante la transformación de los datos en productos de datos, que no coincide necesariamente con el lugar donde se generan los datos. Es en el lugar en que se utilizan los datos donde se agrega el verdadero valor económico; por tanto, lo que importa es el flujo del valor de los datos más que el propio flujo de los datos. En este sentido, la ubicación física del almacenamiento de los datos tal vez no sea un factor tan importante para el desarrollo. No obstante, esto también puede depender de las necesidades de procesamiento de datos, ya que la mayor capacidad de procesamiento se encuentra en los centros internacionales de datos de hiperescala, que no suelen estar situados en países en desarrollo, a excepción de China.

Cabe argumentar que, mientras se garantice el acceso a los datos, no debería haber ninguna relación entre la ubicación donde se almacenan y el desarrollo económico, ya que, con el acceso garantizado, los agentes nacionales pueden utilizar los datos con fines económicos. Así ocurriría en el caso de una empresa que almacena sus datos en un centro fuera de su país (lo que da lugar a un flujo de datos transfronterizo) y que, mientras pueda utilizar los datos para sus fines, se beneficiará de ellos.

Otro caso sería el de una plataforma digital mundial que extrae los datos de los usuarios de un país concreto y los utiliza para su beneficio privado, sin ninguna compensación y sin la posibilidad de que las empresas nacionales utilicen esos datos de forma productiva. En efecto, las entidades globales disfrutan a menudo de la ventaja de ser las primeras en el mercado del análisis y el procesamiento de datos, ventaja que difícilmente pueden superar los países en desarrollo que se incorporan tardíamente, incluso teniendo acceso a sus datos. Para que un marco internacional regulador de los flujos de datos transfronterizos sea adecuado, debe asegurar el acceso a los datos y, cuando este sea restringido, garantizar que las ganancias obtenidas a partir de esos datos se distribuyan equitativamente. Esto debería complementarse con la mejora de la capacidad de procesamiento de los datos en los países en desarrollo. En general, la decisión acerca de la ubicación de los datos depende de diferentes factores técnicos, económicos, de seguridad, jurisdiccionales y de privacidad, así como de la disponibilidad de infraestructuras y energía y de su fiabilidad, que pueden incidir en diferentes direcciones y deben evaluarse de manera integral. Los responsables políticos de los países en desarrollo tendrán que evaluar los diferentes costos y beneficios que entraña la decisión sobre la ubicación física de los datos, teniendo en cuenta las características específicas del país y las necesidades de su estrategia de desarrollo.

F. DIFERENTES TIPOS DE DATOS: IMPLICACIONES PARA LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Los datos pueden clasificarse en diferentes tipos según diversas taxonomías. Ya se han introducido diferentes tipos de datos en secciones anteriores de este Informe, como los datos proporcionados voluntariamente y los observados; los datos estructurados y no estructurados; y los datos personales, públicos y privados. Otras categorizaciones posibles son los datos recopilados con fines comerciales u oficiales; los datos utilizados por las empresas, que incluyen los datos institucionales, los datos de recursos humanos, los datos técnicos y los datos mercantiles; los datos presentes e históricos; los datos sensibles o no sensibles; y los datos entre empresas (B2B), de empresa a consumidor (B2C), de Gobierno a consumidor (G2C) o de consumidor a consumidor (C2C). Es importante distinguir entre los diferentes tipos de datos, porque puede repercutir en el acceso que habría que dar a cada tipo, tanto a nivel nacional como internacional, así como en la forma de manejar los datos.

En esta sección se analizan algunas categorías clave de flujos de datos. Estas categorizaciones son importantes, ya que pueden servir de base para un tratamiento diferenciado de los datos cuando circulan a través de las fronteras. Además, pueden dar ideas que permitan regular de manera más detallada los flujos de datos transfronterizos. Sin embargo, dadas las importantes dificultades que existen para medir y diferenciar esos flujos, su aplicación práctica puede presentar limitaciones.

Es importante distinguir entre quiénes son los productores y los consumidores de los datos. Para ello se debe explorar si los flujos de datos transfronterizos están asociados a intercambios B2B, G2C, B2C o C2C. También es pertinente analizar otras cuestiones transversales que pueden implicar un tratamiento diferente de los datos personales y sensibles.

1. Tipos de productores y usuarios de datos

a) Datos comerciales

Como se ha señalado anteriormente, los flujos de datos amparados por derechos de propiedad intelectual resultantes de las interacciones B2B y B2C están a menudo sujetos a acuerdos jurídicos de las empresas que determinan qué datos se transmiten y cómo circulan a través de las fronteras. Cuando los flujos no abarcan datos personales, muchas veces vienen determinados por normas internas de las empresas, acuerdos entre empresas o contratos.

En el caso de los datos organizativos transfronterizos asociados a la transferencia entre empresas internas o en cadenas globales de valor o intercambios B2B, preocupa especialmente la preservación del control y la confidencialidad de los datos como elemento central de la ventaja competitiva en la economía de datos. Por ejemplo, garantizar que los datos entre máquinas o los procedentes de la Internet de las cosas puedan intercambiarse de forma segura y rápida es un aspecto cada vez más importante del funcionamiento de las cadenas globales de valor (Foster y otros, 2018).

b) Datos oficiales y abiertos

Los Gobiernos suelen integrar sus servicios de datos con el sector privado cuando utilizan fuentes, servicios y almacenamiento de datos. Por tanto, los flujos de datos transfronterizos iniciados por los Gobiernos también pueden depender de los contratos y acuerdos que configuran el correspondiente flujo. Los datos oficiales suelen tener un carácter más reservado que otros datos, especialmente si forman parte de la infraestructura nacional crítica. Así pues, los flujos transfronterizos de ese tipo de datos pueden estar sujetos a requisitos adicionales, como una normativa nacional. Por ejemplo, puede ocurrir que determinados datos oficiales solo puedan atravesar las fronteras si se cumplen ciertos requisitos (por ejemplo, que se utilicen solo estándares o normas de cifrado específicas o los datos sean almacenados en una nube privada, a diferencia de la nube pública, por seguridad). En algunos casos, se pueden prohibir los flujos de datos transfronterizos cuando los datos son especialmente sensibles, como se explica más adelante con mayor detalle.

Aunque los datos oficiales internos pueden estar sujetos a un tratamiento más estricto, las administraciones y otras organizaciones sin fines de lucro también tienden a compartir datos para generar valor económico y social. Si se hace adecuadamente, compartiendo los datos se puede impulsar la cooperación regional o internacional. A nivel gubernamental, cada vez son más frecuentes los flujos de datos transfronterizos en ámbitos como la armonización comercial, las bases de datos empresariales, las plataformas de gobernanza regional y los sistemas nacionales de seguridad y lucha contra la delincuencia.

Además, los flujos de datos pueden integrarse con más recursos abiertos, que también pueden considerarse una categoría de datos con el objetivo de utilizarse y compartirse de forma abierta. Las esferas o agrupaciones organizativas específicas pueden reunirse para acordar la manera de compartir los datos a nivel nacional o internacional. Un ejemplo de éxito en este ámbito son las actividades que han promovido la creación de normas y plataformas y el fomento de la compartición de datos sobre la ayuda. Dirigidas por la Iniciativa Internacional para la Transparencia de la Ayuda, estas actividades han ayudado a los Gobiernos y las organizaciones no gubernamentales a difundir sus datos sobre la ayuda, que luego pueden combinarse a nivel global y utilizarse para comprender mejor este sector (Pamment, 2019).

c) Datos de los consumidores

Los flujos de datos transfronterizos relativos a los consumidores pueden recibir un tratamiento específico. En ese sentido, cabe destacar ante todo que los datos de los consumidores suelen incluir datos personales y, por tanto, sus flujos pueden estar sujetos a normas adicionales. Dado que los datos personales también pueden estar asociados a otras fuentes de datos, esto se aborda como una cuestión transversal más adelante. La interacción transfronteriza entre los consumidores y las empresas extranjeras, o entre un consumidor nacional y otro extranjero, ha surgido principalmente a escala como resultado de las tecnologías digitales. El tratamiento de estos flujos de datos plantea una serie de interrogantes. Dado que las empresas extranjeras están fuera de la jurisdicción de los Gobiernos, los flujos significativos de datos B2C extranjeros plantean riesgos en relación con el cumplimiento en el país de una serie de reglas internacionales y nacionales, por ejemplo, con respecto a los estándares, las normas laborales y la tributación (Aaronson, 2019a). El crecimiento de los flujos de datos C2C a través de las fronteras también plantea interrogantes sobre el tratamiento y la jurisdicción pertinentes. Por ejemplo, las interacciones C2C a gran escala en el comercio electrónico y los flujos de datos C2C vinculados a la economía del trabajo esporádico han sido facilitados por las plataformas en línea. Estas permiten la ejecución de determinadas actividades al margen de los marcos reguladores existentes, que tal vez deban revisarse.

2. Cuestiones transversales en la esfera de los datos personales sensibles

a) Datos personales

Los datos personales son una categoría importante de datos cuyos flujos deben ser objeto de una regulación adicional. Distintos tipos y fuentes de datos pueden incluir datos personales. Los datos que implican interacciones con los consumidores suelen contener información personal asociada a un

individuo, pero también la pueden contener otros flujos de datos. En ocasiones, las empresas y otras organizaciones intercambian, por ejemplo, información sobre los usuarios que tal vez forme parte de flujos de datos transfronterizos relacionados con procesos B2B u organizativos internos.

El tipo de datos personales presentes en esos flujos de datos es diverso. Puede tratarse de datos que los usuarios proporcionan voluntariamente cuando interactúan con las aplicaciones y los servicios, como información sobre el grupo demográfico al que pertenecen o los datos de su tarjeta de crédito. También pueden incluir una variedad más amplia de datos observados a partir del uso de productos o servicios; por ejemplo, las aplicaciones de comercio electrónico pueden conservar información sobre los productos que un usuario ha mirado y recopilar datos más detallados sobre su ubicación o sus interacciones, entre otros (OECD, 2020a). Asimismo, se pueden generar otros tipos de datos inferidos[18] sobre personas concretas, incluidas las inferencias basadas en los datos recopilados (como las calificaciones de riesgo y crédito), y combinarse también con otras fuentes de datos externas, tanto personales como no personales. Por ejemplo, una empresa de seguros puede combinar los datos personales proporcionados por una persona con otros datos sobre esa misma persona procedentes de fuentes externas, además de otros datos, como la ubicación y el riesgo demográfico, para determinar los niveles de riesgo (GSMA, 2018c).

Los flujos transfronterizos de datos personales suelen estar sometidos a una serie de acuerdos y normativas. Por ejemplo, lo normal es que el emisor y el receptor de los datos tengan que cumplir determinadas normas y acuerdos comerciales sobre la recopilación, transmisión y reutilización de los datos. En términos más generales, esas actividades se rigen por la normativa de protección de datos. En la actualidad están surgiendo en todo el mundo diferentes enfoques básicos de la protección de los datos personales que no son muy compatibles, como se analizará en los capítulos IV y V.

A este respecto es importante determinar qué tipos de flujos de datos se clasifican como flujos que contienen datos personales. Mientras que los datos personales ofrecidos voluntariamente, como la información demográfica, son claramente personales, puede no estar claro si los datos observados son de carácter personal o no cuando no identifiquen directamente a un individuo específico. Las normas más estrictas sobre los datos personales que han ido surgiendo han tratado de mejorar la protección de los datos incluyendo definiciones más amplias de "datos personales", también cuándo los datos anónimos y voluntarios podrían identificar indirectamente a una persona, por ejemplo, en el caso de los datos asociados a la dirección IP o a las *cookies* utilizadas por los sitios web (Bird y Bird, 2017).

Habida cuenta de los riesgos y la posible carga reguladora que supone recopilar y volver a compartir los datos personales, las empresas suelen utilizar técnicas para anonimizar los datos que permitan una mayor flexibilidad en los flujos. Las técnicas más comunes son las que permiten desvincular los datos observados de una persona concreta, utilizar la pseudoanonimización o compartir los datos solo cuando están agregados. Esas técnicas pueden ser eficaces pero, a medida que aumenta el volumen de datos sobre las personas, no está claro que sirvan realmente para anonimizar los datos. En el contexto actual de fortalecimiento de la protección de datos en todo el mundo, se están investigando nuevas técnicas que permitan que los datos sean más anónimos sin dejar de ser útiles. Algunos ejemplos de técnicas recientes son la perturbación de datos, en la que se añade ruido aleatorio a los datos para que la persona sea anónima aunque se mantiene la estructura; y los datos sintéticos, es decir, mediante algoritmos se generan datos artificiales para reflejar el carácter de los datos reales, pero sin representar a personas (PDPC, 2018). En la era del aprendizaje automático, es probable que los modelos y algoritmos de datos entrenados también se impongan como alternativa a los datos personales. Una vez que los modelos han sido entrenados satisfactoriamente, los datos del modelo pueden compartirse para ser usados en aplicaciones con menores riesgos. Esos enfoques de anonimización de los datos podrían ser importantes desde el punto de vista de los derechos humanos, al reducir el riesgo de que los datos identifiquen a los usuarios. También podrían apoyar la compartición de datos derivados de las personas como bienes públicos digitales en el futuro.

[18] Según la OCDE (OECD, 2019a), "los datos derivados (o inferidos o imputados) se generan a partir de los análisis de datos, incluidos los datos creados de manera bastante 'mecánica' utilizando un razonamiento simple y matemáticas básicas para detectar patrones". Por consiguiente, deben considerarse un "producto de datos", ya que implica el procesamiento de los datos brutos.

b) Datos sensibles

Cuando los datos se clasifican como "sensibles" surge una importante segmentación, pues sus flujos están sujetos a normas o regulaciones adicionales, en particular sobre la forma en que pueden transmitirse a través de las fronteras. Las principales tensiones en los flujos de datos transfronterizos aparecen en las diferentes formas de clasificar los datos sensibles: lo que se considera datos sensibles varía según el país y el momento.

Los datos asociados a sectores específicos pueden estar sujetos a normas adicionales a la regulación de datos general. Por ejemplo, sectores como los servicios financieros o de telecomunicaciones pueden tener normas de datos más estrictas que no permitan los flujos de datos transfronterizos, o requisitos específicos sobre el almacenamiento o los flujos. En ocasiones, la categorización de los flujos de datos sensibles puede crear confusión y contradecir otras normas, ya que surgen de un conjunto más amplio de ministerios, como los de sanidad, comercio e industria y finanzas. En otros países, las normas sobre los datos definen "niveles" más amplios de flujos de datos que se consideran sensibles.

3. Aspectos técnicos de los flujos de datos

Los datos también pueden clasificarse en función de características técnicas y ser objeto de un tratamiento diferente. El formato de los datos es un aspecto técnico que podría dar lugar a un tratamiento distinto de los flujos de datos transfronterizos. Los flujos de datos transfronterizos asociados a determinados tipos de aplicaciones (como el audio, el vídeo, la mensajería, los protocolos de telecomunicaciones IP y los datos cifrados) pueden entrañar un tratamiento diferenciado. Por ejemplo, se puede realizar un bloqueo técnico de determinados flujos de datos en las pasarelas nacionales de Internet, o solicitar a todos los proveedores de servicios de Internet nacionales que bloqueen esos formatos. Ese tratamiento técnico no siempre consiste en el bloqueo de los flujos de datos; los países pueden simplemente no dar prioridad a esos flujos. Por ejemplo, si no se da prioridad a los flujos transfronterizos de audio o vídeo podría disminuir la calidad de un servicio internacional. Esto se ha utilizado a menudo extraoficialmente para dar prioridad a los productores de contenidos y empresas nacionales. Otras posibles categorizaciones técnicas de los flujos de datos podrían recibir un tratamiento diferenciado, aunque hay menos pruebas de que sean habituales. Por ejemplo, los tratamientos que diferencian entre datos brutos o procesados (por ende, posiblemente con elementos amparados por derechos de propiedad intelectual) o datos cifrados (por ende, con protocolos de ciberseguridad más estrictos) podrían ser categorías importantes en el futuro.

En resumen, esta sección ha proporcionado algunos ejemplos para destacar que existe una amplia gama de categorías de datos, lo que podría implicar un tratamiento diferente de los flujos de datos transfronterizos según el tipo de datos. En la práctica, la identificación y diferenciación de estas distintas categorías puede plantear importantes dificultades. Resulta muy complicado diferenciar los flujos de datos en función de servicios o bienes específicos, o destacar los casos en que la información contiene datos personales, sin una cooperación considerable de los productores y los consumidores de los datos. También es difícil identificar a los productores y usuarios de los flujos de datos, ya que en los flujos de datos transfronterizos existen muchos intermediarios, como las plataformas, las redes privadas virtuales y las redes de distribución de contenidos. Estos desempeñan un papel esencial en la infraestructura de Internet, pero también pueden complicar la identificación del origen y el destino de los flujos de datos. Sin embargo, una cuestión que se plantea en este contexto, en el que sofisticados algoritmos pueden crear perfiles altamente personalizados para la publicidad selectiva, es si sería posible diseñar de forma similar sofisticados algoritmos para rastrear los diferentes tipos de datos.

Además de las dificultades técnicas que plantea su identificación, en el contexto de los flujos de datos transfronterizos también son importantes las dificultades políticas y culturales. Para muchas de las categorizaciones señaladas (como los servicios, los datos personales y los datos sensibles) no existe una definición acordada a nivel mundial, sino que esta varía entre las distintas regiones e incluso entre los países de una misma región. Esto dificulta la tarea de decidir cómo tratar los flujos transfronterizos. Como se ha demostrado en relación con los datos personales, no se trata de un asunto menor. Las distintas definiciones pueden dar lugar a diferencias muy grandes en el volumen de flujos de datos categorizados como datos personales.

Pese a lo difícil que resulta lograr una categorización adecuada de los datos, presenta claras ventajas, dado que los distintos tipos de datos tienen diferentes implicaciones en lo que respecta a su circulación,

también cuando es de carácter transfronterizo. Una categorización adecuada permitiría establecer el tipo de acceso necesario para cada tipo de datos y facilitaría la compartición de datos con las garantías necesarias. Por ejemplo, se podrían aplicar condiciones de acceso para cada tipo de agente, a nivel nacional o internacional. Por tanto, es necesario intensificar los esfuerzos y la investigación para llegar a cierto consenso sobre una taxonomía de datos que pueda ser útil en el contexto de los flujos de datos transfronterizos y su regulación internacional.

G. LOS DESEQUILIBRIOS DE PODER Y LA DESIGUALDAD QUE GENERAN LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Como ha señalado la UNCTAD (2019a), la dinámica del mercado en la economía digital impulsada por los datos conduce a asimetrías de información, concentración del mercado y desequilibrios de poder que agravan las desigualdades entre los países y dentro de ellos. Aunque se ha generado una riqueza enorme en un tiempo récord, esta se ha concentrado en un número reducido de personas, empresas y países. La captura del valor de los datos mediante la transformación de los datos brutos en inteligencia digital (la cadena de valor de los datos) está cada vez más en manos de unas pocas plataformas digitales globales (véase también el capítulo I). Esto también se refleja en los intercambios desiguales en los flujos de datos transfronterizos. Además, con las políticas y normativas vigentes, es probable que se mantenga esta trayectoria, lo que contribuirá a aumentar aún más la desigualdad y los desequilibrios de poder. En la presente sección se revisan estas cuestiones en relación con el dominio del sector privado y la justicia de datos. Estos elementos tienen implicaciones significativas para las políticas de desarrollo, ya que es importante garantizar la distribución equitativa de los mayores ingresos derivados de la economía digital impulsada por los datos, en particular a través de los flujos de datos transfronterizos, además de la justicia de datos.

1. Concentración del poder de mercado

La cadena de valor de los datos está dominada por las empresas y las corporaciones digitales globales que controlan las cadenas globales de valor. Desde el punto de vista de la producción, aunque los Gobiernos, las pequeñas empresas o los ciudadanos desarrollen su capacidad de recopilación o aplicación de datos, la mayoría de los flujos de datos son captados por empresas privadas o tienen lugar entre ellas, a menudo entre filiales, servicios y asociados conectados a las pocas grandes empresas tecnológicas que dominan las distintas partes de la cadena de valor de los datos. Desde la perspectiva del desarrollo, la manera en que estas grandes empresas extraen y controlan los datos, lo que les permite crear y acaparar el correspondiente valor, es problemática. A medida que esas empresas crecen e invierten, disminuye la capacidad de otras empresas nuevas para competir con ellas, debido a los retos que plantea la inversión en capacidad y capital humanos para competir a escala. Existe el riesgo de que se generen "divisiones de aprendizaje" muy desiguales y que, en consecuencia, un pequeño número de especialistas de las empresas tecnológicas —con acceso a los datos y con una infraestructura informática y de procesamiento de datos adecuada— sean fundamentales para la creación de valor.

> La captura del valor de los datos mediante la transformación de los datos brutos en inteligencia digital (la cadena de valor de los datos) está cada vez más en manos de unas pocas plataformas digitales globales, lo cual también se refleja en los intercambios desiguales en los flujos de datos transfronterizos.

Las empresas de los distintos países se encuentran en diferentes estados de preparación para crear valor en la economía digital impulsada por los datos. La ventaja competitiva que proporcionan los datos a los precursores provoca asimetrías de información. Aunque alrededor del 20 % de todas las empresas de los países de la OCDE realizaron transacciones de comercio electrónico en 2017, en la mayoría de los países las grandes empresas participan en el comercio electrónico más del doble que las pequeñas y medianas

empresas, y esta brecha se está ampliando en términos absolutos en muchos países (OECD, 2019b). En general, las empresas más pequeñas de la mayoría de los países en desarrollo utilizan el comercio electrónico mucho menos. Además, enormes plataformas digitales como Google, Alibaba, Amazon y Tencent ya disponen de grandes cantidades de datos, que pueden transformar en nuevos productos y servicios de datos de valor añadido. Estas empresas también disponen de fondos para adquirir una importante potencia computacional y cantidades considerables de conocimientos especializados en datos (Ciuriak, 2018). Los nuevos productos y servicios desarrollados a partir de datos generan a su vez todavía más datos, lo que acentúa el poder de mercado de los gigantes digitales (Weber, 2017). Las empresas que se benefician de estas asimetrías de información suelen ser grandes y, en general, se concentran en los Estados Unidos y China (UNCTAD, 2019a). Existen algunas plataformas digitales de éxito a nivel regional en los países en desarrollo, como Mercado Libre en América Latina y Jumia en África, pero suelen seguir prácticas de datos similares a las de las corporaciones digitales globales, aunque a menor escala.

El dominio de los datos comporta ventajas de información, que se suman a las fuentes de posibles fallos del mercado en las economías conseguidas basándose en datos, en particular las economías de escala y de alcance, así como efectos de red. Todo ello tiende a promover la concentración del mercado (y, en consecuencia, que las empresas líderes ganen cuota de mercado). La asimetría de la información inherente a la economía de los datos parece irreductible, ya que no existen soluciones de mercado para corregirla. Debido a la explotación de esas asimetrías de información —y al hecho de que la inversión en la recopilación y la limpieza de datos suele tener un costo inicial elevado, pero un costo marginal bajo o nulo (como otros bienes y activos digitales o intangibles)—, las grandes empresas que controlan los datos pueden obtener importantes rentas por su extracción[19].

La economía mundial de los datos también presenta importantes problemas estructurales para el desarrollo. A diferencia de otras tecnologías en las que se ha registrado una difusión global de la innovación, las necesidades interrelacionadas de una alta cualificación, recursos intensivos en capital y una cantidad ingente de datos dificultan mucho más que el mercado resuelva esos problemas estructurales en torno a los datos. Las plataformas y los dispositivos clave que mejoran las cadenas de valor de los datos están avanzando hacia una situación en la que "el ganador se lo lleva todo". Las grandes empresas tecnológicas de éxito también tienden a crecer mediante la integración en las diferentes etapas de las cadenas de valor de los datos y pueden expandirse en diferentes sectores. También invierten más en infraestructuras de recopilación de datos, así como en investigación y desarrollo de inteligencia artificial, y consolidan así su dominio (UNCTAD, 2019a; Srnicek, 2016; véase también el capítulo I).

> El dominio de los datos comporta ventajas de información, que se suman a las fuentes de posibles fallos del mercado en las economías conseguidas basándose en datos, en particular las economías de escala y de alcance, así como efectos de red, y refuerzan la concentración del mercado y las desigualdades.

Dada la excluibilidad parcial de los datos, los propietarios de datos privados tienen fuertes incentivos para acumular datos que refuercen sus rentas económicas actuales y futuras, utilizando los datos como barrera de entrada. En consecuencia, pueden reforzar su poder de mercado y las desigualdades; surgen así importantes desequilibrios de poder entre las grandes corporaciones digitales y los particulares, las empresas más pequeñas y los Gobiernos. Esto también se refleja en las asimetrías entre los países cuando los datos circulan a través de las fronteras. En vista del enorme tamaño y poder que han alcanzado esas empresas, es probable que ningún país por sí solo, en particular si es un país en desarrollo, pueda hacer frente a su poder. A medida que aumentan el alcance y la influencia de esas corporaciones digitales globales en el plano internacional, crece la necesidad de cooperación entre los países para lograr resultados de desarrollo equitativos en beneficio de las personas y el planeta.

[19] Para un análisis más amplio sobre la obtención de rentas en la economía digital impulsada por los datos, véase Mazzucato y otros (2020), Ciuriak (2020) y Rikap (2021).

2. Justicia de datos e inclusión

Una reflexión más amplia sobre los datos y el desarrollo implica también considerar las economías de datos en desequilibrio dentro de los países. Es importante no subestimar las tensiones más amplias en torno a los signos de los impactos desiguales de los datos en las economías que tienden a concentrar los beneficios entre la élite educada (IDC y OpenEvidence, 2017). Si se mira más allá de los indicadores económicos de desarrollo y se presta atención al desarrollo social y la justicia en un sentido más amplio, será importante detectar las injusticias de datos —la diferente dimensión de la recopilación, el tratamiento, el procesamiento y la estructura social de los datos que podría conducir a la desigualdad— para garantizar que la política de datos ayude a fomentar la inclusión y el desarrollo sostenible (Heeks y Renken, 2018). Las posibles discriminaciones basadas en los datos por diferentes motivos —como el género o la raza— que afectan a los derechos humanos son ejemplos de injusticia de datos[20].

En el caso de los países en desarrollo, preocupa, por ejemplo, la forma en que se están introduciendo las infraestructuras de datos, ya que se están generando datos sobre grupos y comunidades de bajos ingresos, lo que puede conducir a la explotación y a nuevas fronteras de exclusión económica y social (Arora, 2016; Flyverbom y otros, 2017). Para crear inteligencia digital sobre los usuarios de bajos ingresos en esos mercados, los usuarios se convierten en el objetivo de los sistemas e infraestructuras de datos (Arora, 2016). Por ejemplo, el suministro de acceso gratuito a Internet en los países en desarrollo con sistemas como Free Basics o Discover de Facebook puede proporcionar a los grupos de bajos ingresos acceso a Internet a un bajo costo, pero sus críticos argumentan que sirve como fuente de datos acerca de su comportamiento en línea y puede contribuir así a la expansión de esas empresas y conducir a futuras injusticias de datos para los pobres. En Kenya, las aplicaciones de tecnofinanzas, a menudo de empresas domiciliadas en los Estados Unidos, no solo ofrecen aplicaciones para la gestión de pagos y seguros, entre otros, sino que también forman parte de una infraestructura de recopilación de datos que permite a las empresas construir modelos de riesgo social de los participantes, que pueden ser un elemento tan importante de los beneficios como las comisiones directas que obtienen con sus productos financieros (Donovan y Park, 2019; Iazzolino y Mann, 2019)[21].

Las políticas específicas sobre los flujos de datos transfronterizos deberían entonces tener en cuenta los objetivos relacionados con la reducción de las injusticias y los riesgos vinculados a los datos, y el aprovechamiento del entorno digital y los datos para lograr un desarrollo más inclusivo (Foster y Azmeh, 2020; Singh, 2018a; Singh y Vipra, 2019). Además, los Gobiernos pueden centrarse en crear y fomentar bienes públicos digitales como los datos para generar valor social, tal y como se ha comentado, y en desarrollar infraestructuras y plataformas más abiertas para apoyar el desarrollo.

H. LOS PAÍSES EN DESARROLLO EN LA CADENA INTERNACIONAL DE VALOR DE LOS DATOS

Los desequilibrios de poder y las desigualdades comentadas en la sección anterior dan lugar a un desequilibrio en las geografías de datos. Aunque parece haber un creciente potencial de actividades de las cadenas de valor de los datos en los márgenes, están surgiendo muy pocos líderes digitales en los países en desarrollo, y solo en determinados lugares, como China, la India, Indonesia y Sudáfrica (David-West y Evans, 2016a; Evans, 2016). Algunos países en desarrollo (sobre todo China, pero también otros, como la India e Indonesia) presentan una creciente capacidad digital. Pero no puede decirse lo mismo de muchos otros países en desarrollo, que están muy atrasados en cuanto a la preparación para la economía digital impulsada por los datos.

En el contexto de la cadena internacional de valor de los datos, las diferentes etapas de recopilación, almacenamiento, análisis y transformación en inteligencia digital de los datos se suelen desarrollar en distintos países. Cada vez se reconoce más que los flujos de datos transfronterizos están desequilibrados. Para los países en desarrollo, los flujos de datos extraídos están firmemente definidos por los flujos

[20] Para un análisis más detallado de la justicia de datos, véase Global Data Justice, "A globally inclusive dialogue about the future of data", disponible en https://globaldatajustice.org/.

[21] Véase también el análisis de las estrategias de expansión de las principales esferas de influencia en la economía mundial de los datos en el capítulo IV.

"Sur-Norte" (McKinsey, 2014), que son en su mayoría datos brutos. Habida cuenta del dominio de las empresas de datos en los países desarrollados, los datos transformados en inteligencia digital se caracterizan por concentrarse en un número limitado de países avanzados (Mueller y Grindal, 2019; Weber, 2017), sobre todo en los Estados Unidos, además de en China. Estos países tienden a captar la ventaja competitiva de la generación de datos y su uso con fines productivos.

> Los países en desarrollo corren el riesgo de convertirse en meros proveedores de datos brutos para las plataformas digitales globales y de tener que pagar por la inteligencia digital obtenida a partir de sus datos.

Como advirtió la UNCTAD (2019a), las empresas de muchos países en desarrollo pueden encontrarse en posiciones subordinadas, ya que los datos y la captura de su valor asociado se concentran en unas pocas plataformas digitales globales y otras empresas multinacionales que controlan los datos. En consecuencia, los países en desarrollo corren el riesgo de convertirse en meros proveedores de datos brutos para las plataformas digitales globales y de tener que pagar por la inteligencia digital obtenida a partir de sus datos. Esto apunta a un nuevo modelo de relaciones internacionales centro-periferia en la economía digital impulsada por los datos, en el que los Estados Unidos y China están en el centro y el resto del mundo en la periferia. Esta configuración se aleja de la tradicional separación entre países desarrollados y en desarrollo; un país en desarrollo ocupa el centro, mientras que varios países desarrollados están en la periferia. Sin embargo, los países desarrollados de la periferia están mucho más preparados que los países en desarrollo para afrontar los retos que presenta esta situación.

En consecuencia, el surgimiento de los datos como recurso económico ha dado lugar a una nueva categoría en la división internacional del trabajo (Rikap, 2021; Coyle y Li, 2021; Feijóo y otros, 2020), tal y como se refleja en la tipología de flujos de datos presentada en el cuadro III.1. En este cuadro se muestran diferentes tipos de países según varios criterios: a) si son mayoritariamente el destino de flujos de entrada o salida de datos; b) si son países desarrollados o en desarrollo; c) el tamaño del país; d) si tienen plataformas internacionales en línea dominantes; y e) si cuentan con industrias líderes en alta tecnología y profesionales competentes. Se presentan algunos ejemplos para cada categoría.

Cuadro III.1. Clasificación de los países/grupos de países según sus flujos de datos transfronterizos, por nivel de desarrollo

	Entradas de datos	Salidas de datos
Países desarrollados	Países grandes con plataformas internacionales dominantes en línea e industrias líderes en alta tecnología y profesionales competentes: - *Estados Unidos*	Países y regiones sin plataformas internacionales dominantes en línea pero con industrias líderes en alta tecnología y profesionales competentes: - *Unión Europea* - *Japón* - *Reino Unido*
Países en desarrollo	Países grandes con plataformas internacionales dominantes en línea e industrias líderes en alta tecnología y profesionales competentes: - *China*	Países grandes sin plataformas internacionales dominantes en línea pero con industrias líderes en alta tecnología y profesionales competentes: - *India* Países grandes sin plataformas internacionales dominantes en línea ni industrias líderes en alta tecnología y profesionales competentes: - *Indonesia* Países pequeños sin plataformas internacionales dominantes en línea ni industrias líderes en alta tecnología y profesionales competentes: - *Países de África Subsahariana*

Fuente: UNCTAD, a partir de Coyle y Li (2021).

Se ha examinado si este desequilibrio en los flujos de datos es problemático, utilizando modelos económicos de comercio adaptados para analizar los flujos de datos transfronterizos (Mueller y Grindal, 2019). Los enfoques económicos que asocian el desarrollo con el comercio de libre mercado se basan en el supuesto de que el libre comercio a través de las fronteras reduce el precio de los bienes para los consumidores de los países en desarrollo. Los mercados abiertos también impulsan la competencia y la innovación, y favorecen la especialización, ya que las empresas nacionales buscan ventajas comparativas (Hunt y Morgan, 1995). Se ha argumentado que, en la economía digital, la libre circulación de los datos sigue este paradigma más amplio, y que una Internet abierta impulsaría considerablemente el desarrollo y el comercio (Bauer y otros, 2014; Meltzer, 2015). Desde esta perspectiva, un desequilibrio en el flujo de datos no sería necesariamente un problema, sino que formaría parte de un proceso económico continuo en el que las diferencias en los flujos estarían relacionadas con las diferencias de costos. El mercado resolvería los desequilibrios. De hecho, dado que la economía digital se nutre de los rápidos flujos de datos transfronterizos, es probable que los intentos de restringirlos reduzcan sus beneficios (Aaronson, 2019a).

> Los flujos de datos transfronterizos no pueden beneficiar a las personas y al planeta si solo un reducido número de corporaciones digitales globales de unos pocos países acaparan la mayor parte de las ganancias que generan los datos.

En la esfera comercial, algunos observadores se han opuesto a estas ideas de comercio abierto sin restricciones. Esta apertura comercial tiende a beneficiar a los países desarrollados poderosos y es problemática para los países en desarrollo, ya que las importaciones crecen y las empresas nacionales se ven desplazadas (Stiglitz, 2012). Las reflexiones sobre la desigualdad en los flujos de datos transfronterizos indican que también pueden generar problemas en cuanto a la ubicación de la producción de valor añadido en la economía digital (Weber, 2017). Desde este punto de vista, los desequilibrios derivados de los flujos de datos transfronterizos pueden justificar la adopción de intervenciones estratégicas y políticas en los países en desarrollo para garantizar que una mayor parte del valor añadido resultante de los datos permanezca dentro de sus fronteras.

Los flujos de datos transfronterizos no pueden beneficiar a las personas y al planeta si solo un reducido número de corporaciones digitales globales de unos pocos países acaparan la mayor parte de las ganancias que generan los datos. A efectos de desarrollo, adoptándose un sistema internacional para regular correctamente esos flujos podría contribuirse en gran medida a que los países en desarrollo se apropien de una parte más equitativa del valor de los datos.

I. LA SOBERANÍA Y LOS DIFERENTES NIVELES DE GOBERNANZA DE LOS DATOS

Los flujos de datos transfronterizos plantean problemas en relación con la soberanía sobre los datos y su uso. Se suele hablar de soberanía para designar a los agentes o grupos que tienen la legitimidad, la autoridad y el poder para controlar una sociedad e influir en ella. Diferentes agentes han tratado de controlar los flujos de datos mediante diversas actividades, normas y políticas (Couture y Toupin, 2019). No obstante, como en el caso de la propiedad de los datos, en la economía digital impulsada por los datos la noción de soberanía se ve ampliamente alterada, ya que surgen nuevos matices y significados. Tradicionalmente, la soberanía se ha asociado a los territorios nacionales y a las fronteras físicas. Sin embargo, la economía digital impulsada por los datos cuestiona este concepto, ya que los datos se transmiten a través de Internet, que originalmente se concibió como un espacio abierto, donde las fronteras nacionales se difuminan.

Otro factor que afecta a la soberanía es que, con el aumento de su poder de mercado y su tamaño, las poderosas plataformas digitales globales pueden comportarse de manera similar a un Estado-nación y autorregular sus enormes ecosistemas digitales, que incluyen cada vez más aspectos de la vida y la sociedad, y afectan a la soberanía de los verdaderos Estados-nación. En esta sección se examinan los

diferentes niveles y escalas de control, aplicando el concepto de soberanía a los datos y las tecnologías digitales. Se analiza la soberanía en la economía digital impulsada por los datos a nivel nacional e individual (así como en los ámbitos de las comunidades y los grupos), y en términos de geografía.

1. Soberanía nacional

Convencionalmente, se habla de soberanía para referirse al Estado-nación, ya que este es el que tiene la legitimidad, el poder y la capacidad de establecer normas y gobernar (que normalmente le otorga la voluntad soberana de su pueblo por conducto de elecciones democráticas). A medida que los datos adquieren mayor importancia económica y que los Estados perciben una pérdida de control —en favor de otros países o de las plataformas digitales globales— a raíz de los flujos de datos transfronterizos, crece la preocupación por la soberanía nacional sobre los datos.

Los términos "soberanía digital" y "soberanía sobre los datos" han cobrado un gran protagonismo recientemente[22]. La noción de "soberanía sobre los datos", que prácticamente no existía antes de 2011 en el mundo de la investigación ni en el discurso público (Couture, 2020), ha adoptado varios significados que reflejan diferentes valores culturales y preferencias políticas en distintas regiones (Couture y Toupin, 2019); el significado también puede evolucionar con el tiempo a medida que cambian las prioridades nacionales (véase el capítulo IV). Por ejemplo, en la Unión Europea se habla cada vez más de la soberanía digital en relación con sus valores, que se centran en la protección de los derechos fundamentales. También guarda relación con la idea de que la Unión Europea necesita crear capacidad y "recuperar terreno" en la esfera de la economía digital impulsada por los datos, frente a las plataformas digitales globales dominantes de los Estados Unidos y China (European Parliament, 2020).

Pero parece que últimamente se está haciendo más hincapié en el concepto de "autonomía estratégica"[23]. El enfoque de China con respecto a la soberanía digital sitúa a las tecnologías digitales e Internet como un activo geopolítico más amplio. En consecuencia, hace hincapié en los planes nacionales para fomentar el liderazgo tecnológico mundial y en la protección de los datos como un activo central y estratégico para el Estado (Budnitsky y Jia, 2018), prestando especial atención a la seguridad (Creemers, 2020). En los Estados Unidos, la soberanía sobre los datos se confía principalmente al sector privado. En el capítulo IV se analizan con cierto detalle los principales enfoques mundiales en materia de gobernanza de los datos, que guardan una estrecha relación con las diferentes concepciones de la soberanía sobre los datos.

Cuando otros países en desarrollo se han referido a la soberanía nacional, a menudo han combinado estas diferentes ideas. En el Brasil e Indonesia, por ejemplo, se ha prestado más atención a la creación de capacidades y se ha aludido a las infraestructuras críticas que las naciones necesitan controlar en el marco de la idea de soberanía (Azmeh y Foster, 2018). En los países en desarrollo también se destacan más las ideas sociales y culturales de la soberanía digital que antes eran más comunes en los movimientos sociales y las comunidades de código abierto. Dichas ideas se derivan de historias más enraizadas de dominación y desigualdades poscoloniales, y del deseo de que los grupos tomen colectivamente el control de sus propios bienes y de su propio destino (Avila, 2018; Couture y Toupin, 2019; Kwet, 2019). En el contexto de las economías basadas en los datos, se entiende que el colonialismo digital y el colonialismo de los datos tienen un alcance más amplio que el colonialismo histórico de los países sobre los países. El colonialismo en el contexto digital remite a la explotación de seres humanos por empresas o Estados a causa de los datos, y puede darse en todos los países (Couldry y Mejias, 2018, 2021).

Sin embargo, la aparición de la soberanía nacional en todos estos casos puede entrar en conflicto con el carácter global de Internet y con la dificultad de asignar territorialidad a los flujos de datos transfronterizos. El enfoque de un control más estratégico de los activos digitales clave también puede ser viable

[22] Existe un amplio debate acerca de la soberanía digital y la soberanía sobre los datos que muestra las importantes diferencias y complicaciones que surgen en relación con estos conceptos. Para análisis detallados, véase Hummel y otros (2021), Pohle y Thiel (2020), Aydın y Bensghir (2019), Couture (2020) y Coyer y Higgott (2020).

[23] Véase, por ejemplo, "Digital sovereignty is central to European strategic autonomy", discurso del Presidente del Consejo Europeo, Charles Michel, en el evento en línea Masters of Digital 2021, disponible en www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/; y Aktoudianakis (2020).

únicamente en las grandes naciones con un poder centralizado que estén dispuestas a aplicar políticas muy intervencionistas. Incluso en este caso, cabe preguntarse si esos enfoques merecen la pena ante la fragmentación de las redes mundiales de producción y de la innovación.

La soberanía digital nacional se asocia a menudo con la necesidad de almacenar los datos dentro de las fronteras de un país. Sin embargo, como ya se ha comentado, la relación entre el almacenamiento nacional de los datos y el desarrollo no es tan evidente. Contar con un marco internacional de gobernanza de los datos bien definido y que funcione correctamente, también en el caso de los flujos de datos transfronterizos, podría permitir cierto consenso y aportar claridad acerca de los derechos soberanos sobre los datos.

2. Personas, comunidades y grupos

Las cuestiones relacionadas con los flujos de datos transfronterizos van más allá de las empresas y los Gobiernos, y afectan a las personas (en relación con sus derechos individuales); en consecuencia, la soberanía sobre los datos individuales también es clave en el contexto de la economía digital impulsada por los datos. Los derechos en materia de datos individuales son importantes para controlar el uso de los datos de las personas y evitar su abuso o uso indebido. Tanto las empresas como los Gobiernos deben respetar esos derechos en los planos nacional e internacional.

Habida cuenta de la capacidad del sector privado para controlar los datos y las tecnologías digitales, así como del control que pueden ejercer los Gobiernos, los debates sobre la soberanía digital individual suelen girar en torno a los derechos en materia de datos, como ya se ha comentado, y a la forma en que las personas pueden reivindicar el acceso, el control, la propiedad o el uso de sus datos privados (Floridi, 2020), así como la protección de estos frente al abuso y el uso indebido. En este sentido, la noción de soberanía digital en la Unión Europea hace hincapié en el papel de las personas con respecto al control de sus datos (European Parliament, 2020).

Como señala Bria (2020), la soberanía digital en manos del pueblo puede abarcar la capacidad de las tecnologías digitales para facilitar la transición de la actual economía digital del capitalismo de la vigilancia (donde unas cuantas corporaciones con sede en los Estados Unidos y China luchan por la supremacía digital mundial) a un futuro digital centrado en las personas y basado en mejores derechos para los trabajadores y trabajadoras, el medio ambiente y la ciudadanía con el fin de aportar una innovación social a largo plazo y acabar con la lógica binaria que siempre nos presenta solo dos posibilidades para el futuro del entorno digital:… El Gran Estado despoja a las personas de sus libertades individuales, mientras que la Gran Tecnología (las grandes empresas del sector) crea monopolios de datos que acabarán gestionando infraestructuras críticas como la sanidad o la educación; ninguna de las dos opciones es válida para un mundo democrático". Se puede plantear "una tercera vía: la Gran Democracia, es decir, una democratización de los datos, la participación ciudadana y la tecnología al servicio de la sociedad y la transición ecológica".

Hay señales que revelan que las personas pueden tomar el control de sus datos. Hay indicios de que algunos usuarios están contemplando una "soberanía sobre los datos personales", en el sentido de que las decisiones de los consumidores sobre el uso de las tecnologías digitales se basan en cómo se utilizan sus datos, especialmente cuando perciben que esos datos son objeto de un tratamiento problemático (Kesan y otros, 2016). Últimamente, los activistas también han comenzado a desarrollar herramientas destinadas a favorecer la soberanía sobre los datos personales utilizando dispositivos o programas informáticos específicos para mantener el control de sus datos (Couture y Toupin, 2019). Los programas de código abierto orientados a la privacidad, como ownCloud y nextCloud, permiten a los usuarios alojar sus propios servicios en la nube sin extraer datos personales. Otro ejemplo es Signal, un competidor de WhatsApp que utiliza el cifrado de extremo a extremo para mantener la seguridad de las conversaciones. En el marco de la economía de los datos personales también han surgido varias empresas emergentes, como digi.me y Meeco, que permiten a los usuarios compartir sus datos o sacar provecho de ellos. Hasta el momento, esas actividades no han representado un gran volumen, pero podrían influir en los flujos de datos en el futuro.

Muchas comunidades han participado en actividades relacionadas con la soberanía sobre los datos para hacer valer sus derechos colectivos en materia de datos. Por ejemplo, algunas comunidades indígenas han intentado reivindicar los derechos que les corresponden sobre sus datos (Kukutai y Taylor, 2016). En los países en desarrollo, también se han hecho llamamientos para que otros grupos y comunidades

a diferentes niveles ejerzan sus derechos en materia de datos, como los comerciantes o conjuntos más amplios de trabajadoras y trabajadores (Singh y Vipra, 2019). En términos más generales, los crecientes argumentos en torno a la discriminación y los sesgos raciales en la esfera de los datos (Arora, 2016; Noble, 2018) podrían impulsar en el futuro demandas de comunidades más grandes y grupos marginados o discriminados para ejercer sus derechos comunitarios en materia de datos como un aspecto de la justicia de datos (Heeks y Renken, 2018). A diferencia de lo que ocurre con los datos personales, las reivindicaciones para ejercer la soberanía sobre los datos colectivos son más recientes y suelen tener una base menos sólida en lo que respecta a los derechos subyacentes. Sin embargo, no hay que restarles importancia, pues hay comunidades, grupos o conjuntos de trabajadores y trabajadoras que perciben que la propiedad de sus propios espacios y prácticas, y su capacidad para controlar de forma independiente su condición, están disminuyendo debido a la extracción de datos (Singh y Vipra, 2019).

3. Geografía

Las reivindicaciones en cuanto a la soberanía digital se han dado en diferentes niveles geográficos. A nivel subnacional, suelen centrarse en la obtención de acceso a los datos recopilados de forma privada en espacios de interés público, como los datos locales sobre el tráfico, la población o la contaminación en manos de empresas privadas que pueden mejorar el análisis, la gestión y la planificación espaciales. Mediante la negociación o en momentos concretos, empresas tecnológicas como Uber, Siemens, Airbnb y Orange han compartido datos para respaldar proyectos urbanos (véase, por ejemplo, OECD, 2020a; Villani, 2018). En algunos países en desarrollo, la soberanía también ha surgido en proyectos estratégicos conjuntos de construcción de infraestructuras de datos y captura y análisis de datos entre proveedores de datos y el sector público, como se ha visto, por ejemplo, en distintos proyectos de ciudades inteligentes en la India (Heeks y otros, 2021). También hay propuestas en el sentido de ampliar la soberanía sobre los datos, como las relativas a los datos abiertos o a la creación de fideicomisos de datos, cooperativas de datos u otras entidades de gestión de datos (González-Zapata y Heeks, 2015; Open Data Institute, 2019a; O'Hara, 2019). Estas reivindicaciones de soberanía suelen tener menos fuerza y su aplicación práctica es por el momento limitada. En los ejemplos mencionados, las ciudades rara vez han intentado controlar los datos o impedir los flujos de datos transfronterizos; simplemente exigen acceder a los datos y utilizarlos para sus propios fines.

> Existen importantes dificultades para compaginar la noción de soberanía nacional, tradicionalmente asociada a los territorios de los países, y la naturaleza no territorial, la globalidad y la apertura del espacio digital en el que circulan los datos.

En resumen, existen distintas nociones de soberanía cuando se reivindican los derechos sobre los datos, y en diferentes capas y niveles geográficos; el significado de la soberanía digital o la soberanía sobre los datos (y, en consecuencia, de los correspondientes derechos soberanos) sigue siendo confuso (Christakis, 2020; De La Chapelle y Porciuncula, 2021). Existen importantes dificultades para compaginar la noción de soberanía nacional, tradicionalmente asociada a los territorios de los países, y la naturaleza no territorial, la globalidad y la apertura del espacio digital en el que circulan los datos. Además, en la economía digital impulsada por los datos no solo preocupa la soberanía nacional; la soberanía sobre los datos individuales (o comunitarios) también cobra especial relevancia en vista de la naturaleza de los datos. Esto implica que tal vez sea necesario proteger la soberanía sobre los datos individuales de las personas o comunidades frente a las empresas privadas y los Gobiernos para garantizar que las personas (y las comunidades) tengan el control de sus datos y evitar que estos sean objeto de abuso y uso indebido. De ahí la necesidad de regular debidamente los datos en un amplio marco internacional de gobernanza. Es importante que los países puedan reclamar su derecho a la soberanía sobre los datos generados a nivel nacional para poder tomar decisiones autónomas basadas en esos datos y beneficiarse de ellos, así como para conservar su independencia frente a las plataformas digitales globales y los Gobiernos extranjeros. No obstante, esto no debe dar lugar a estrategias de autosuficiencia o aislacionismo, que probablemente no den resultado por el carácter de red de Internet y la gran interdependencia en la economía digital impulsada por los datos.

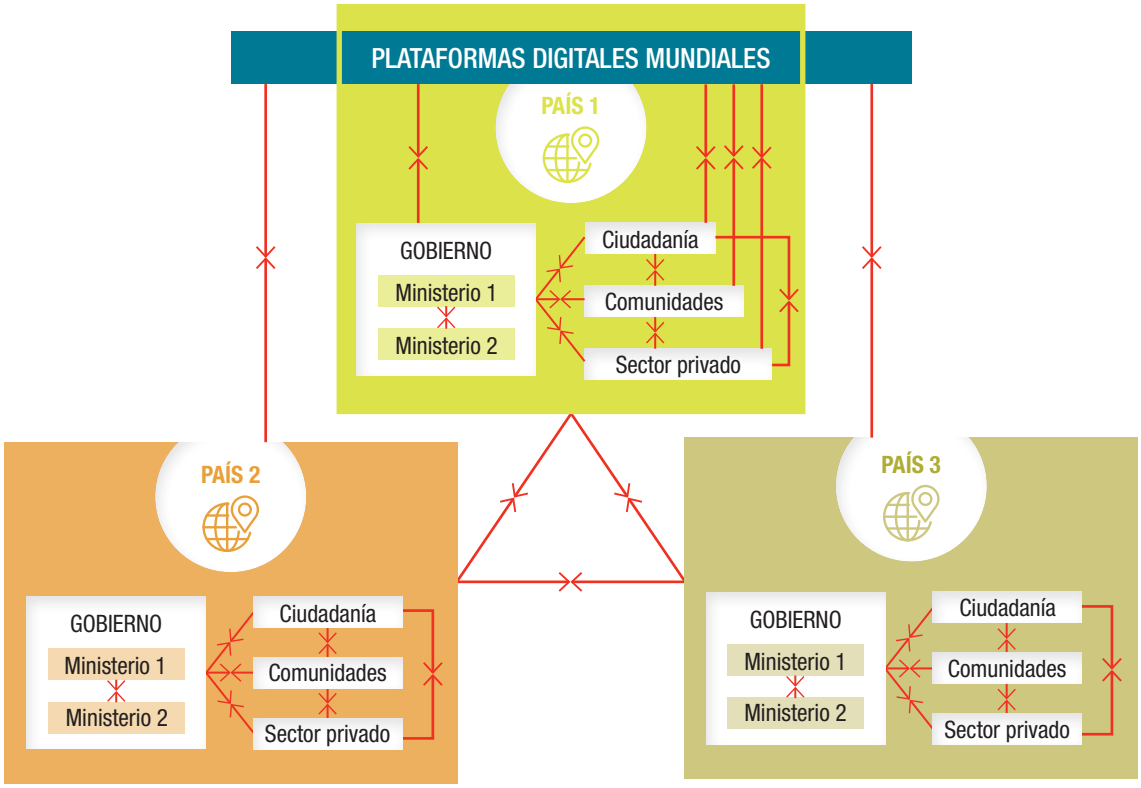
J. CONFLICTOS DE INTERESES EN LOS FLUJOS DE DATOS TRANSFRONTERIZOS Y CONCESIONES POLÍTICAS

Las diferencias económicas, políticas y culturales entre los países pueden dar lugar a opiniones divergentes acerca de los datos, la privacidad, Internet, la economía digital y la vigilancia, entre otras cuestiones. Los conflictos de intereses de los distintos países pueden generar tensiones entre ellos. También pueden surgir tensiones dentro de los países entre los distintos agentes de la economía digital (como las personas, las comunidades, las grandes y pequeñas empresas privadas del sector digital o de otros sectores, la sociedad civil y los Gobiernos), ya que sus intereses también difieren.

En este contexto, surgen grandes dilemas entre los distintos objetivos políticos a nivel nacional y entre los países, así como diferentes intereses entre los diversos agentes en relación con los flujos de datos transfronterizos. Algunos ejemplos de esos dilemas son la seguridad nacional frente a la privacidad, la innovación frente a la protección de los datos, la vigilancia frente a la privacidad, y la distribución de las ganancias por país o por agente económico. Incluso dentro de esos dilemas pueden surgir otros; por ejemplo, en la esfera de la innovación, ¿cuál es su objetivo? ¿La innovación va a servir únicamente a los intereses de las plataformas digitales globales que se benefician del control de los datos y aumentan su poder mediante el control de la IA? ¿O va a servir al interés público? Las diferentes culturas y valores de los países con respecto a las cuestiones relacionadas con los datos, la privacidad y la soberanía, por ejemplo, pueden dar lugar a puntos de vista opuestos sobre las formas de abordarlos y las políticas necesarias para regular los flujos de datos transfronterizos.

En la figura III.1 se presenta una ilustración sencilla de la posible incidencia de esas tensiones en un contexto de tres países (que podría proyectarse a múltiples países). Muestra la complejidad de las relaciones entre los diferentes actores de la economía digital a nivel nacional e internacional. Las líneas entre países y actores representan las distintas tensiones que pueden surgir.

Figura III.1. Los diferentes actores y la complejidad de las relaciones en el contexto de los flujos de datos transfronterizos



Fuente: UNCTAD.

Las reflexiones sobre los flujos de datos transfronterizos ponen de manifiesto que la formulación de normas depende del contexto, según las diferentes categorías de datos y flujos de datos y sobre la base de diversas perspectivas. Por tanto, es probable que los países en desarrollo tengan que estudiar las posibles consecuencias de sus decisiones sobre sus políticas relativas a los datos para esos flujos, los costos de las empresas, la privacidad de los datos, la seguridad nacional, la innovación y la competencia, entre otras cuestiones. Los países tendrán que hacer concesiones entre esos intereses, en función de sus objetivos de desarrollo.

Por tanto, para formular políticas en este ámbito hay que tener en cuenta la complejidad de los distintos intereses en juego, los dilemas existentes y las concesiones que deben hacerse, y evaluarlos debidamente. Esto implica elegir determinadas opciones por encima de otras, ya que los intereses pueden ir en diferentes direcciones. Por consiguiente, los responsables políticos tendrán que asignar un valor a los diferentes intereses y objetivos, y encontrar el equilibrio necesario que satisfaga sus necesidades específicas y favorezca sus objetivos de desarrollo. El resultado final será fruto de las decisiones políticas y sociales.

Este análisis también pone de manifiesto que la gobernanza de los datos requiere un enfoque holístico y pangubernamental donde se alcance un equilibrio entre los diferentes objetivos políticos. También es importante tener en cuenta los intereses de todas las partes. Por último, para resolver los conflictos de intereses entre los países en relación con los flujos de datos transfronterizos, los órganos decisorios a nivel internacional y multilateral son claves para reflejar debidamente las voces y opiniones de los países en desarrollo en la gobernanza mundial de los datos.

K. LA CAPACIDAD PARA BENEFICIARSE DE LOS DATOS

El análisis expuesto en las secciones anteriores ha puesto de manifiesto la importancia del acceso a los datos y de su uso con fines productivos y de desarrollo. Sin embargo, los datos también pueden ser objeto de abuso y uso indebido, lo que plantea importantes desafíos. Aunque el acceso a los datos es una condición necesaria para beneficiarse de ellos, no es suficiente. El valor de los datos proviene de su agregación, análisis y transformación en inteligencia digital. Por tanto, es fundamental tener, además del acceso, la capacidad de transformar los datos en una inteligencia digital que se pueda monetizar o utilizar con fines de bien público. En consecuencia, es importante examinar cuáles son las capacidades necesarias para poder aprovechar los datos con fines productivos y de desarrollo. Para crear y capturar valor a partir de los datos se necesita de una infraestructura asequible que permita su circulación, además de competencias, recursos, vínculos con el resto de la economía y apoyo mediante normativas y políticas adecuadas (UNCTAD, 2019a).

> Aunque el acceso a los datos es una condición necesaria para beneficiarse de ellos, no es suficiente. Se necesita además la capacidad de transformar los datos en una inteligencia digital que se pueda monetizar o utilizar con fines de bien público.

La preparación de los países para participar y beneficiarse de la economía digital impulsada por los datos difiere en términos de conectividad e infraestructura de datos, emprendimiento digital y competencias; recursos financieros; y capacidad institucional. La mayoría de los países en desarrollo no tienen una gran capacidad digital. Además, el tamaño reducido de sus mercados limita su posibilidad de lograr economías de escala y de alcance en la economía de los datos. Asimismo, en la mayoría de esos países el electorado no ejerce una gran presión sobre los responsables políticos para que formulen normas que regulen los datos (Weber, 2017).

Por consiguiente, muchos países en desarrollo temen que no podrán ponerse al día en este nuevo contexto y obtener una ventaja comparativa en otros bienes o servicios derivados del uso de los datos. La UNCTAD (2017) informó de que la posición de los países en desarrollo en el comercio de mercancías como los productos básicos se vería afectada negativamente por los escasos conocimientos especializados en datos. Estos países deberían utilizar los análisis de datos para mejorar sus procesos de producción y sus productos, y mantener la competitividad.

Desde el punto de vista laboral, en lo que respecta al trabajo realizado en la producción y el procesamiento de los datos, una premisa común es que esa producción está muy automatizada y en ella participan especialistas en sistemas y datos. Sin embargo, al desgranar la producción de datos se descubre que el proceso entraña otro tipo de tareas. Ciertos tipos de datos valiosos (como los datos en línea, el vídeo y el audio) suelen requerir la intervención humana para recopilar, categorizar, filtrar y limpiar los datos con el fin de procesarlos eficazmente (Gray y Suri, 2019). Así, una visión laboral prestaría más atención al hecho de que, detrás de los complejos sistemas y algoritmos basados en datos, suele haber ejércitos de "peones digitales" mal remunerados, muchos de ellos en el mundo en desarrollo.

Las competencias necesarias para tratar los datos almacenados están vinculadas con la administración, la gestión y el análisis de las bases de datos, que a menudo necesitan administradores de sistemas y especialistas en bases de datos cualificados. Sin embargo, la mayoría de estas actividades se pueden llevar a cabo a distancia desde cualquier lugar del mundo, usando herramientas en línea. Por consiguiente, en muchos casos los profesionales y los analistas de bases de datos están situados lejos del emplazamiento de los centros de datos (Azmeh y otros, 2021).

El análisis y la transformación de los datos se asocian principalmente a los profesionales de la tecnología de la información y la ciencia de los datos. Los analistas se caracterizan por estar altamente cualificados, a menudo con formación universitaria. Ante la gran demanda de este tipo de competencias en el mercado mundial, los países en desarrollo suelen tener dificultades para retener a los especialistas en datos (Huang y Arnold, 2020). Además, los análisis de datos requieren cada vez más tareas de media y baja cualificación. Este tipo de trabajo puede necesitar de menores conocimientos de procesamiento de datos, y algunas funciones brindan oportunidades a las personas que tienen conocimientos básicos de computación. El trabajo menos cualificado corresponde a los trabajadores y trabajadoras que participan en la extracción, la selección, la corrección, el filtrado y el etiquetado de datos, que son esenciales para la eficacia de las grandes organizaciones basadas en los datos. Los principales centros de externalización y trámites comerciales en línea, como la India y Filipinas, se han convertido en centros de análisis digitales de baja cualificación (Graham y otros, 2017; Gray y Suri, 2019). También se ha registrado un crecimiento en otros países en desarrollo, como en las regiones rurales más conectadas (Malik y otros, 2016) y en los centros urbanos de África, ya que la conectividad permite a las trabajadoras y trabajadores mal remunerados convertirse en "peones digitales" (Anwar y Graham, 2020).

En términos más generales, como esfera emergente en los países en desarrollo, los organismos públicos y los reguladores deberán contar con la capacidad necesaria para poder beneficiarse de los datos. En concreto, deberán ser capaces de analizar técnicamente los flujos de datos y desarrollar su capacidad, así como de comprender la relación de los datos con el resto de los sectores e industrias. Además, los responsables políticos deberán prestar más atención a la necesidad de contar con personal competente en la esfera de la ciencia de los datos y la IA, no solo para desarrollar el espíritu empresarial, sino sobre todo para crear capacidad institucional en los propios órganos decisorios. Muchas administraciones públicas no cuentan con los recursos humanos necesarios para diseñar, aplicar y supervisar las políticas pertinentes porque la mayor parte del personal competente es atraído por el sector privado.

> Ello significa que existen importantes retos de capacidad a nivel individual, empresarial y público para garantizar que los países en desarrollo no sean solo lugares de recopilación de datos, sino que también puedan captar el valor de esos datos.

Asimismo, cuando se analiza cómo aprovechar los datos de forma más amplia es crucial centrarse en el desarrollo. Como se ilustra en el presente capítulo, el carácter multidimensional de los datos y la prevalencia de los flujos de datos transfronterizos obligan a los reguladores de estos a lograr un equilibrio entre los distintos intereses opuestos comprendiendo claramente los beneficios y los desafíos.

En resumen, el crecimiento de la cadena de valor de los datos brinda oportunidades de fomento de la capacidad en los países en desarrollo, pero es importante destacar que la mayor parte de las infraestructuras de datos y de recopilación de datos son de carácter privado y están controladas por grandes empresas que, en su mayoría, no se encuentran en los países en desarrollo, con la notable excepción de China. Ello significa que existen importantes retos de capacidad a nivel individual, empresarial y público para garantizar que los países en desarrollo no sean solo lugares de recopilación de datos, sino que también puedan captar el valor de esos datos.

L. CONCLUSIÓN

En el presente capítulo se han explorado con cierta profundidad las complejidades de la relación entre los flujos de datos transfronterizos y el desarrollo, que se derivan en gran parte de la naturaleza particular de los datos. En el contexto de los datos y sus flujos transfronterizos, hay diversas opiniones sobre qué implican y quién puede reivindicar los derechos sobre los datos, las categorías de flujos transfronterizos según el tipo de datos y los enfoques de la soberanía digital. Estas diferentes opiniones son el resultado de las diversas concepciones y situaciones políticas, sociales y económicas de los distintos países, e influyen en la orientación de sus políticas.

Debido a sus características particulares, sobre todo su carácter de bien público, los datos pueden generar importantes ganancias privadas, pero también un valor social y beneficios para el desarrollo. El valor de los datos depende en último término de su uso. Los datos por separado no son de gran utilidad, pero tienen un valor potencial porque son el ingrediente para obtener una inteligencia digital que se pueda monetizar, o utilizar para generar valor privado y social. Para que los beneficios de la economía digital se materialicen, es necesario que los datos se compartan y utilicen, lo que a menudo entraña que estos circulen a través de las fronteras. En este sentido, el acceso a los datos es esencial. No obstante, las implicaciones del uso de los datos tienen dimensiones tanto económicas como de otros tipos.

> Los responsables políticos, tanto a nivel nacional como internacional, pueden actuar para maximizar las ganancias que generan los datos y los flujos de datos transfronterizos y minimizar los riesgos que conllevan, garantizando al mismo tiempo una distribución equitativa de los beneficios que generan los flujos de datos transfronterizos.

Además, desde el punto de vista económico, la necesidad de permitir los flujos de datos no debe entrañar que los datos puedan cruzar gratuitamente las fronteras. Al no existir actualmente un sistema internacional que regule los flujos de datos transfronterizos, las plataformas digitales globales pueden extraer los datos brutos de los países en desarrollo y apropiarse de la mayor parte del valor creado, lo que se traduce en un volumen creciente de desequilibrios de poder y desigualdades. Los flujos de datos transfronterizos no pueden beneficiar a las personas y el planeta si solo un reducido número de corporaciones digitales globales de unos pocos países pueden obtener la mayor parte de las ganancias.

Los mecanismos de mercado por sí solos no conducen a resultados eficientes o equitativos. En consecuencia, los responsables políticos, tanto a nivel nacional como internacional, pueden actuar para maximizar las ganancias que generan los datos y los flujos de datos transfronterizos y minimizar los riesgos que conllevan, garantizando al mismo tiempo una distribución equitativa de los beneficios que generan los flujos de datos transfronterizos. Habida cuenta del alcance mundial de esos flujos, esto implicará tanto la adopción de políticas nacionales como internacionales.

Las principales cuestiones destacadas en este capítulo son las siguientes:

- Debido a sus características particulares, la naturaleza de los datos es muy diferente a la de los bienes y servicios. Los datos son bienes intangibles, no rivales, parcialmente excluibles y de naturaleza relacional y multidimensional.

- Por su naturaleza especial, los flujos de datos transfronterizos deben recibir un tratamiento diferente al del comercio internacional de bienes y servicios.
- No existe un vínculo claro entre la localización de los datos dentro de las fronteras nacionales y el desarrollo económico; al decidir si se localizan los datos se deben tener en cuenta diferentes factores, que dependen en gran medida de la situación específica del país.
- Los distintos tipos de datos pueden tener diferentes implicaciones en cuanto a los flujos de datos transfronterizos y las correspondientes políticas.
- El acceso a los datos y su uso (incluso su posible uso negativo) son fundamentales para el desarrollo, junto con la capacidad de crear y capturar valor a partir de los datos, es decir, de transformar los datos en inteligencia digital (productos de datos).
- Existe una compleja combinación de intereses opuestos entre los agentes de la economía digital mundial basada en los datos, y para formular políticas sobre los flujos de datos transfronterizos que beneficien al desarrollo deben tomarse decisiones en favor de unos u otros.
- Las políticas destinadas a instaurar una gobernanza mundial de los datos deben adoptar un enfoque holístico, multidimensional, pangubernamental y multilateral, tanto a nivel nacional como internacional.

Al explorar los posibles retos y oportunidades de los flujos de datos transfronterizos, este capítulo proporciona conocimientos pertinentes que pueden ayudar a los responsables políticos. En ese sentido, la aparición de elementos clave en esferas como la protección de los datos, la creación de capacidad y las normas que impulsan el crecimiento económico pone de manifiesto las oportunidades que tienen los países en desarrollo de capturar valor en la cadena de valor de los datos.

El establecimiento de normas adecuadas en materia de flujos de datos fronterizos en su justa medida puede ayudar a garantizar los derechos en materia de datos, reducir los problemas estructurales y favorecer el desarrollo económico. Es importante estudiar otros delicados equilibrios que deben lograrse en relación con la ética de los datos, como crear valor a partir de los datos sin llegar a vigilar a la población, o los vínculos entre el filtrado de datos y la censura.

Los países tal vez deseen controlar el acceso a los datos por motivos técnicos, económicos, de privacidad y relacionados con otros derechos humanos. Mientras no exista un sistema internacional de regulación de los flujos de datos transfronterizos que funcione correctamente y garantice la maximización del valor de los datos, privados y públicos, además de su protección frente a los perjuicios y la distribución equitativa de las ganancias derivadas dentro de los países y entre ellos, la única opción que tendrán los países que quieran que la economía nacional se beneficie de las ganancias obtenidas a partir de los datos en materia de desarrollo será tratar de mantener sus datos dentro de las fronteras nacionales. Sin embargo, es importante tener en cuenta que, aunque no se puede generar valor sin los datos brutos, el acceso a los datos sin la capacidad de procesarlos y monetizarlos, o de crear valor social, no sirve de nada. En este contexto, la imposición de restricciones a los flujos de datos transfronterizos tal vez no reporte ningún beneficio y generará obstáculos e incertidumbre a las empresas y los particulares que deseen intercambiar datos a través de las fronteras.

Las diversas opiniones y dimensiones sobre las características clave de los datos y los flujos de datos transfronterizos, así como las complejidades conexas, señalan la necesidad de evaluar detenidamente todos los elementos presentes al formular las políticas. Puesto que diferentes factores pueden afectar al proceso de diferentes maneras, hay que tener en cuenta la diversidad de interconexiones e intereses que entran en juego. La combinación de las diferentes cuestiones abordadas en este capítulo puede dar lugar a múltiples combinaciones de políticas que requerirán las consiguientes elecciones en función de las decisiones políticas y sociales, así como de los objetivos de desarrollo. En términos generales, no hay una solución sencilla. Los enfoques simplificadores, ya sea pidiendo la libre circulación de los datos sin traba alguna (o la prohibición de la localización de los datos), en un extremo, o la localización absoluta de los datos como regla general, en el otro extremo, no ayudan mucho. Hay que evaluar exhaustivamente las implicaciones de los flujos de datos transfronterizos, teniendo en cuenta las diferencias entre países, tipos de datos, intereses y objetivos políticos. Como suele decirse, es necesario “hilar muy fino”.

En general, los datos se han convertido en un recurso estratégico clave que origina tensiones geopolíticas entre los distintos países del mundo, como se analizará en el próximo capítulo. Básicamente, la cuestión es quién gana en la carrera por el control de los datos y las tecnologías digitales, que permiten influir y controlar la sociedad. Los flujos de datos transfronterizos son clave en este contexto.

> Los enfoques simplificadores, ya sea pidiendo la libre circulación de los datos sin traba alguna (o la prohibición de la localización de los datos), en un extremo, o la localización absoluta de los datos como regla general, en el otro extremo, no ayudan mucho.

El análisis de este capítulo también pone de manifiesto que se puede producir una fragmentación de enfoques nacionales de la regulación, con diferencias significativas entre los países que podrían no conducir a un desarrollo global. Por consiguiente, es necesario examinar más detalladamente los marcos de gobernanza apropiados y las iniciativas emergentes de cooperación internacional en torno a los flujos de datos transfronterizos que pueden favorecer trayectorias de desarrollo más amplias. En el resto del Informe se analizan exhaustivamente las políticas en vigor sobre los flujos de datos transfronterizos a diferentes niveles, primero a nivel nacional (en el capítulo IV, que se centra en las tendencias de la gobernanza de datos a nivel mundial relacionadas con los flujos de datos transfronterizos, y en el capítulo V, donde se exponen las normativas nacionales sobre los flujos de datos transfronterizos). Las políticas a nivel regional e internacional se analizan en el capítulo VI. Por último, en el capítulo VII se exploran posibles caminos en relación con las políticas sobre los flujos de datos transfronterizos.

ANEXO DEL CAPÍTULO III: LA CIRCULACIÓN DE LOS DATOS A TRAVÉS DE LAS FRONTERAS

1. La circulación de los datos

a) El "modelo cliente-servidor"

La mayor parte de la circulación de datos actual en Internet se basa en el "modelo cliente-servidor". Este modelo hace referencia a la estructura de aplicación distribuida que divide las tareas o cargas de trabajo entre los servidores (proveedores de servicios) y los clientes (consumidores de servicios). En el lugar de hospedaje web se ejecutan una o más aplicaciones del servidor, que comparten contenidos o recursos con los clientes. El cliente no comparte ninguno de sus recursos, pero solicita un contenido o un servicio a un servidor.

Los clientes y los servidores intercambian mensajes (paquetes de datos) siguiendo un patrón de solicitud-respuesta. Para la comunicación, el dispositivo del cliente y los servidores situados en el hospedaje web utilizan lenguajes y reglas comunes de transmisión de datos. Actualmente, la mayoría de las comunicaciones siguen el modelo TCP/IP. El protocolo de control de transmisión (TCP) proporciona paquetes de datos fiables, ordenados y a prueba de fallos entre las aplicaciones del servidor y del cliente (conexión a tres bandas). El protocolo de Internet (IP) es el principal protocolo de comunicaciones para la retransmisión (enrutamiento) de paquetes de datos a través de las redes.

b) El modelo de tres niveles de proveedores de servicios de Internet

La propia Internet es un conjunto de redes separadas pero interconectadas, cada una de las cuales es un sistema autónomo. Las redes de sistemas autónomos están controladas por los proveedores de servicios de Internet (PSI). Cada uno de esos PSI cuenta con sus propias políticas, topologías de red internas, servicios y perfiles de clientes. Además del sistema de direccionamiento IP, los sistemas autónomos también comparten un marco de enrutamiento global basado en el protocolo de puerta de enlace de borde (BGP) para conectar las diferentes redes.

Todas esas redes están conectadas a través de puntos de intercambio de tráfico de Internet (IXP), que son ubicaciones físicas a través de las cuales las empresas de infraestructuras de Internet (como los PSI, las redes de distribución de contenidos, las empresas web, los proveedores de servicios de comunicación y los proveedores de servicios en la nube y de *software* como servicio) se conectan para intercambiar el tráfico de Internet. Esas ubicaciones de intercambio de Internet alojan conjuntamente diferentes redes y permiten a los proveedores de red compartir las interconexiones de tránsito fuera de sus redes.

Los PSI se encargan de transportar el tráfico de Internet en nombre de otros PSI, empresas u organizaciones e individuos que no son PSI. Se clasifican en un modelo de tres niveles que los cataloga en función del tipo de servicios de Internet que prestan:

- Los proveedores de Internet del nivel 1 son las redes que constituyen la red troncal de Internet. Esos PSI de nivel 1, también conocidos como proveedores de servicios de red, construyen infraestructuras como los cables marítimos de Internet del océano Atlántico. Facilitan el tráfico de todos los demás PSI, no de los usuarios finales. Los PSI de nivel 1 poseen y gestionan su infraestructura operacional, incluidos los enrutadores y otros dispositivos intermedios (como los conmutadores) que conforman la red troncal de Internet. Solo intercambian tráfico de Internet con otros proveedores de nivel 1 en condiciones no comerciales a través de interconexiones privadas igualitarias gratuitas. Las redes de nivel 1 soportan volúmenes de tráfico muy elevados y grandes bases de clientes con numerosos enrutadores, y suelen estar compuestas por muchos sistemas autónomos.
- Un PSI de nivel 2 es un proveedor de servicios que utiliza una combinación de tránsito de pago a través de PSI de nivel 1 e interconexiones con otros PSI de nivel 2 para facilitar el tráfico de Internet a los clientes finales a través de PSI de nivel 3. Los PSI de nivel 2 suelen ser proveedores regionales o nacionales. Solo unos pocos PSI de nivel 2 pueden dar servicio a clientes de más de

dos continentes. A menudo, tienen velocidades de acceso más lentas que los PSI de nivel 1 y están al menos a un "salto de enrutador" de la red troncal de Internet.

- Un PSI de nivel 3 es un proveedor que compra estrictamente el tránsito de Internet. Un proveedor de nivel 3, por definición, se dedica principalmente a proporcionar acceso a Internet a los clientes finales. Los PSI de nivel 3 se centran en las condiciones del mercado local de empresas y consumidores. Proporcionan la "rampa de entrada" o el acceso local a Internet para los clientes finales, a través de redes de cable, línea digital de abonado, fibra o acceso inalámbrico. Su cobertura se limita a países o subregiones específicas, como un área metropolitana. Los PSI de nivel 3 utilizan y pagan a los de nivel superior para acceder al resto de Internet.

c) Pasos en la circulación de los datos

Combinando el modelo cliente-servidor y el modelo de 3 niveles de PSI, la circulación de los datos en Internet podría resumirse así:

1. Un mensaje de la aplicación cliente (por ejemplo, un navegador web) se divide en diferentes paquetes de datos que incluyen instrucciones para el reensamblaje (TCP) y el destino (IP).
2. Los paquetes de datos se transmiten desde el dispositivo (por ejemplo, una computadora, una tableta o un teléfono inteligente) a través del enrutador y el módem hasta el PSI del cliente (PSI local/de nivel 3), que proporciona acceso a otras redes de Internet.
3. El PSI local (nivel 3) recibe los paquetes de datos.
4. Los paquetes de datos están conectados a través de los IXP y son enrutados por el PSI de nivel 3 a los PSI de nivel 2, que a su vez pueden enrutarlos a los PSI de nivel 1 (la red troncal de Internet).
5. Utilizando el BGP, se puede dirigir cada paquete de datos a través de diferentes rutas hacia su destino, pasando por diferentes IXP, ubicados en diferentes países y operados por diferentes PSI (véase la siguiente sección).
6. En último término, el PSI de destino (PSI local/de nivel 3) recibe todos los paquetes de datos y los reenvía al servidor de destino (identificado por la dirección IP de destino).
7. En el destino, se reensamblan los paquetes de datos y se ejecuta la solicitud en su aplicación.
8. La respuesta del servidor sigue un proceso similar de vuelta al cliente.

2. Cómo cruzan los datos las fronteras nacionales

a) Identificación de los flujos de datos transfronterizos

Como se explica en el modelo de 3 niveles, los paquetes de datos se enrutan a través de diferentes redes locales, regionales o internacionales. Las transferencias de datos transfronterizas circulan sobre todo entre redes de nivel 1 o dentro de ellas, y normalmente a través de cables de fibra óptica de muy alta velocidad. Habida cuenta de que los datos viajan a la velocidad de la luz y de que la ruta exacta de casi todos los datos solo se determina cuando están en tránsito, es prácticamente imposible concretar dónde y cuándo un paquete de datos específico cruza una frontera nacional. Sin embargo, cuando un paquete de datos atraviesa un país, se redirige a través de un centro de datos, donde se reenvía en la propia infraestructura de red del PSI o se intercambia con la red de otro proveedor en un IXP. Esos son los puntos físicos de entrada y salida en los que se pueden determinar los flujos de datos transfronterizos.

También se pueden analizar los flujos de datos transfronterizos prestando atención a la información (los datos) en lugar de a cada paquete de datos por separado. Esos paquetes tienen un valor limitado, ya que solo transportan una parte de la información que se transmite. Los datos solo se pueden procesar cuando todos los paquetes se reensamblan. En este caso, hay dos ubicaciones físicas por las que fluyen todos los paquetes de datos después de ser enviados por el emisor y antes de ser recibidos por el destinatario, que son el PSI del cliente y el PSI del servidor. En estos PSI es donde se puede determinar el carácter transfronterizo de una transmisión de datos.

b) *Enrutamiento del tráfico internacional de Internet*

El tráfico de Internet se enruta a través de diferentes redes controladas por los PSI y conectadas a los IXP. La ruta que recorrerá un paquete de datos entre las redes viene determinada por el BGP. El BGP es un protocolo de enrutamiento vectorial que toma decisiones de enrutamiento a partir de la ruta, las políticas de red o los conjuntos de reglas que configura el administrador de red. Cada enrutador del BGP contiene una tabla de enrutamiento estándar que se utiliza para dirigir los paquetes en tránsito y tomar las decisiones sobre las mejores rutas según la disponibilidad en el momento, el número de saltos y otras características de la ruta. Si hay varias rutas disponibles (por ejemplo, dentro de una gran instalación de hospedaje), en las políticas del BGP se comunican las preferencias de una organización sobre la ruta que debe seguir el tráfico de entrada y salida. Como se ha comentado, el enrutamiento también puede desarrollarse dentro de un sistema autónomo (red del PSI), en cuyo caso se utilizan los protocolos de puerta de enlace interior para determinar la ruta de un paquete de datos. Aunque los flujos de datos están muy "globalizados", se calcula que más del 66 % del tráfico web internacional pasa por los Estados Unidos (Mueller y Grindal, 2019:77). Esto se debe a la elevada proporción de centros de datos mundiales que se encuentran en ese país.

c) *Registro de los flujos de datos transfronterizos*

Los flujos de datos transfronterizos no se registran a nivel nacional o internacional. Esto no significa que no se puedan rastrear los datos a través de Internet. Por ejemplo, el protocolo de mensajes de control de Internet (ICMP) es utilizado por los dispositivos de red, como los enrutadores, para enviar mensajes de error e información operativa que indica el éxito o el fracaso en la comunicación con otra dirección IP. Traceroute y tracert son comandos de diagnóstico de redes informáticas que utilizan el ICMP para mostrar posibles rutas y calcular los retrasos en el tránsito de los paquetes a través de una red IP.

Las direcciones IP por las que fluyen los paquetes de datos de los dispositivos de red pueden utilizarse para determinar el país, la ciudad o el código postal, y establecer así la ubicación geográfica de un objeto. Existen varias bases de datos de geolocalización en Internet que se pueden consultar. La principal fuente de datos de direcciones IP son los registros regionales de Internet, que asignan y distribuyen las direcciones IP entre las organizaciones situadas en sus respectivas regiones de servicios. Esa información puede complementarse con fuentes secundarias, como la minería de datos o los datos de localización geográfica enviados por los usuarios, y perfeccionarse. Las geolocalizaciones de Internet se utilizan con fines de investigación penal, detección de fraudes, comercialización y concesión de licencias.

La naturaleza particular de los datos, y los desequilibrios que se constatan a nivel mundial en el aprovechamiento de los flujos de datos transfronterizos para diversos objetivos de desarrollo, hacen que las políticas destinadas a lograr esos objetivos estén llamadas a desempeñar un papel clave. No obstante, como se señala en este capítulo y en el capítulo V, los enfoques adoptados en materia de gobernanza de los datos y los flujos de datos transfronterizos varían considerablemente de unos países a otros. Este capítulo se centra en los principales enfoques de las políticas en materia de economía digital y gobernanza de los datos en algunas de las principales economías, que pueden tener una influencia mundial en la economía digital, en aspectos como la regulación de los flujos de datos transfronterizos. La existencia de enfoques divergentes en este ámbito queda reflejada en el surgimiento de tensiones en la economía mundial –especialmente entre los Estados Unidos y China– y la generación de riesgos de fragmentación del espacio digital e Internet, que podrían conllevar repercusiones significativas para los países en desarrollo.

En este capítulo se subraya la importancia de evitar los enfoques que propicien la creación de compartimentos estancos en el ámbito de la economía digital impulsada por los datos y, en su lugar, fomentar el logro de resultados más inclusivos y equitativos. No es probable que en un mundo caracterizado por "nacionalismos de datos" divergentes, los intereses de los países en desarrollo y la economía mundial resulten favorecidos, pues tal contexto daría lugar a normativas nacionales subóptimas, a una reducción de las oportunidades de mercado para las pequeñas empresas y a menos ocasiones para la innovación digital, con lo cual surgiría un pequeño número de ganadores a expensas de muchos perdedores.

PRINCIPALES ENFOQUES EN MATERIA DE GOBERNANZA DE LA ECONOMÍA DIGITAL IMPULSADA POR LOS DATOS EN TODO EL MUNDO: ¿RIESGO DE FRAGMENTACIÓN EN EL ESPACIO DIGITAL?

IV

CAPÍTULO IV LOS ENFOQUES DIVERGENTES EN MATERIA DE GOBERNANZA DIGITAL Y GOBERNANZA DE LOS DATOS CORREN EL RIESGO DE FRAGMENTAR ESPACIO DIGITAL

Los enfoques de regulación de los datos y los flujos de datos

varían considerablemente entre los principales actores de la economía digital, y hay poco consenso a nivel internacional y regional

Enfoques de gobernanza de los datos

Estados Unidos	Unión Europea	China
Control de los datos por el sector privado	Control de los datos por los particulares sobre la base de valores	Control de los datos por el Estado
Estrategia de expansión para aumentar el control de los datos		
Mediante las corporaciones digitales privadas	**Liderazgo normativo y alianzas**	**Ruta de la Seda Digital**

Contexto actual a nivel mundial

- Riesgo de fragmentación del espacio digital y de Internet
- Las plataformas digitales globales siguen ampliando sus propios ecosistemas de datos
- Tensiones entre los principales actores
- Carrera por el liderazgo en las innovaciones tecnológicas para obtener ventajas económicas y estratégicas

Una economía digital impulsada por los datos que propicie la creación de compartimentos estancos iría en contra del espíritu de Internet y, probablemente, de los intereses de los países en desarrollo

En términos económicos, la **interoperabilidad** debería generar mejores resultados

La **fragmentación** obstaculizaría el progreso tecnológico, reduciría la competencia, posibilitaría la aparición de estructuras de mercado oligopólicas en diferentes áreas y permitiría una mayor influencia del Estado

La fragmentación también obstaculizaría la **colaboración entre jurisdicciones**

A falta de un sistema **internacional de regulación de los flujos de datos**, ciertos países podrían percibir la restricción de estos como única opción para cumplir determinadas metas políticas

A. INTRODUCCIÓN

Para que los flujos de datos transfronterizos propicien el desarrollo, es necesario elaborar políticas, como se muestra en el capítulo III. La mayoría de los países están aplicando algún tipo de medida para regular sus datos y flujos de datos transfronterizos. Estas pueden adoptar diversas formas en función de las diferencias en las condiciones y los valores políticos, económicos, sociales y culturales, y también reflejan la disparidad de prioridades en el ámbito de la formulación de políticas. En el presente capítulo, junto con el capítulo V, se presenta la situación de la gobernanza de los flujos de datos transfronterizos a nivel nacional en todo el mundo. Inicialmente, se examinan los principales enfoques y tendencias en materia de gobernanza de la economía digital impulsada por los datos en las economías que pueden tener una influencia global en los flujos de datos transfronterizos. A continuación, el capítulo V se centra en proporcionar más detalles sobre las medidas específicas adoptadas en relación con la regulación de los flujos de datos transfronterizos, con el fin de ofrecer una perspectiva global de la situación de esas normativas en cada país.

En su momento, Internet se caracterizaba principalmente por la ausencia de centralización (Medhora y Owen, 2020), en un espacio libre y abierto. También se ha hablado mucho de la necesidad de una Internet global e interoperable (ECLAC e I&JPN, 2020; Internet Society, 2020a), cuyos beneficios permitirían potencialmente llegar a audiencias en todo el mundo, integrar las cadenas globales de valor digitales y acceder a mercados más amplios que los nacionales[1]. En contraste, ahora la economía de plataformas, la inteligencia artificial (IA), el "Estado de vigilancia" y la computación cuántica demandan conjuntos de datos a gran escala, lo que potencia la existencia de nodos centralizados de influencia. A este respecto, las corporaciones digitales globales que recopilan y controlan los datos están creando sus propios ecosistemas de datos. Al mismo tiempo, ante las voces que piden más soberanía sobre los datos generados en cada país, las cuestiones relativas a la economía digital impulsada por los datos se consideran cada vez más como un asunto nacional. Si bien ambas tendencias apuntan a la deriva de Internet hacia una arquitectura de compartimentos estancos —que no encaja bien con su naturaleza abierta—, en los diversos nodos centralizados es posible encontrar nociones muy diferentes de gobernanza digital y gobernanza de los datos.

En la sección B de este capítulo se analizan los principales enfoques respecto de la economía digital y la gobernanza de los datos en las cinco grandes economías que podrían tener una influencia global en la regulación de los flujos de datos transfronterizos, a saber, los Estados Unidos, China, la Unión Europea, la Federación de Rusia y la India. Las estrategias de expansión de los enfoques de los Estados Unidos, China y la Unión Europea se analizan en la sección C. A continuación, en la sección D se examina la posibilidad de fragmentación del espacio digital, y se exploran las repercusiones del choque entre los diferentes modelos de regulación de datos, especialmente entre los Estados Unidos y China, y los posibles riesgos derivados de una potencial fragmentación de Internet y de la economía digital impulsada por los datos. También se reseñan las posibles consecuencias de dicha fragmentación para los países en desarrollo. Así pues, en este capítulo se ofrece un panorama general de la gobernanza en materia de datos en todo el mundo, centrado en las principales áreas de influencia. En el capítulo siguiente se examinan las políticas específicas sobre los flujos de datos transfronterizos que los diferentes países aplican internamente.

B. PRINCIPALES ENFOQUES EN MATERIA DE ECONOMÍA DIGITAL Y DE FLUJOS DE DATOS TRANSFRONTERIZOS

En esta sección se analizan los principales enfoques predominantes en materia de gobernanza de la economía digital, así como los correspondientes modelos de regulación de los flujos de datos transfronterizos. Los cinco casos pueden describirse, de forma algo simplificada, como un enfoque de

[1] Internet Society ha identificado las propiedades esenciales que definen el Modo Internet de Interconectarse y que posibilitan que, como "red de redes", aporte beneficios tecnológicos y económicos. Son las siguientes: una infraestructura accesible con un protocolo común; una arquitectura abierta de componentes básicos interoperables y reutilizables; una gestión descentralizada; un único sistema de enrutamiento distribuido; identificadores globales comunes; y una red de uso general y neutralidad tecnológica. Véase Internet Society, El Modo Internet de Interconectarse, disponible en www.internetsociety.org/es/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/.

mercado (Estados Unidos); una compleja mezcla de enfoques orientados a la seguridad y al desarrollo digital (China); un enfoque basado en los derechos (Unión Europea); un enfoque orientado a la seguridad (Federación de Rusia); y un enfoque que persigue el desarrollo nacional (India). Otros países han optado por emular estos modelos de regulación de diferentes maneras, como se verá en el siguiente capítulo. Sin embargo, estos enfoques principales no se presentan en modo alguno como modelos, ya que cada uno refleja la situación y las prioridades específicas de la economía correspondiente. De hecho, las reflexiones que se plasman en este capítulo y en el siguiente muestran que, en lo que respecta a la gobernanza de los flujos de datos transfronterizos, no existe un enfoque único.

El objetivo de esta sección es describir el marco general de los principales enfoques para poner de relieve las diferencias que podrían dar lugar a problemas de compatibilidad o interoperabilidad entre ellos o fragmentar el espacio digital a nivel mundial, con posibles repercusiones para los países en desarrollo (como se analiza en la sección siguiente). Además, dada la rápida velocidad de los cambios en las tecnologías digitales y la creciente conciencia sobre la necesidad de regular sus implicaciones en la economía digital impulsada por los datos, estos planteamientos no deben entenderse como estáticos; los enfoques reguladores en materia de datos y de flujos de datos transfronterizos están en constante evolución. Lo que aquí se presenta es un panorama general de la situación a principios de 2021.

1. Planteamiento de mercado y fomento de la innovación: el enfoque de los Estados Unidos

En términos generales, los Estados Unidos han adoptado un enfoque de libre mercado en lo que respecta a la economía digital[2], que incluye un marco regulador igualmente liberal para los flujos de datos transfronterizos. Así pues, el país ha favorecido un planteamiento basado en la iniciativa del sector privado, que estimula la innovación, alienta las ventajas de los precursores y refuerza la subsiguiente posición dominante de sus empresas digitales, a través de adquisiciones y de los efectos de red. En ese contexto, el país ha utilizado los acuerdos comerciales para garantizar a sus empresas un acceso sin trabas a los mercados extranjeros, por ejemplo favoreciendo la libre circulación de los datos y prohibiendo prácticas como los requisitos de localización de los datos y los servidores (véase el capítulo VI). Como se señala en informes del Servicio de Investigación del Congreso, "en general, los Estados Unidos adoptan un enfoque de mercado que apoya una Internet abierta, interoperable, segura y fiable que facilita la libre circulación de la información en línea" (CRS, 2020a, 2020b). Este planteamiento permite que los datos se transmitan a los Estados Unidos cuando los usuarios de todo el mundo entran en relación con empresas que tienen su sede en ese país.

Una de las principales motivaciones del enfoque normativo de los Estados Unidos sobre los flujos de datos transfronterizos es mantener su liderazgo en el mercado digital global y seguir expandiéndose a nuevos mercados (véase más adelante). Hasta la fecha, su sector tecnológico ha tenido un gran éxito en el desarrollo de productos y servicios basados en datos que han penetrado en la mayoría de los mercados del mundo. Esto ha generado una "dinámica de retroalimentación positiva", en la que cuantos más datos recopilan las empresas estadounidenses, mejores son sus productos de datos y, por tanto, mayor es su capacidad para triunfar en los mercados mundiales (Weber, 2017). En consecuencia, los Estados Unidos han abogado contra el proteccionismo digital y el proteccionismo de los datos, por ejemplo respaldando el Marco de Privacidad del Foro de Cooperación Económica de Asia y el Pacífico (APEC) y el Sistema de Normas de Privacidad Transfronteriza, que permite a las entidades de verificación aprobadas por el Estado certificar a las empresas que realizan transferencias internacionales de datos (véase el capítulo VI).

Una Internet no fragmentada y la libre circulación de la información a través de las fronteras son parte integral de la filosofía política y económica de los Estados Unidos (Clinton, 2010). A diferencia de la mayoría de las economías desarrolladas, este país no cuenta con un marco general de privacidad de datos ni impone requisitos específicos para las transferencias transfronterizas de datos personales. Sin embargo, los Estados Unidos sí se han dotado de políticas estrictas de localización para los datos relacionados con la defensa, que exigen que cualquier empresa que suministre servicios en la nube a su

[2] Sin embargo, el Estado ha desempeñado un papel fundamental en el desarrollo de Internet y en la aparición de las plataformas digitales globales.

Departamento de Defensa almacene sus datos únicamente en el territorio nacional[3]. Más recientemente, y aunque no se trata de una restricción general de los flujos de datos, los Estados Unidos han aprobado el programa Red Limpia, cuyo objetivo es proteger las infraestructuras críticas de injerencias extranjeras y velar por la privacidad de las personas mediante la imposición de restricciones a los operadores de telecomunicaciones, las aplicaciones y los servicios en la nube considerados poco fiables, especialmente cuando estos proceden de China[4]. Así pues, a pesar del carácter liberal del marco general sobre los flujos de datos transfronterizos, los Estados Unidos adoptan un enfoque restrictivo en lo que respeta a cuestiones que afectan específicamente a la defensa y la seguridad nacionales.

Debido a la estructura global del modelo de computación en la nube impulsado por el mercado, en ocasiones las autoridades federales de los Estados Unidos han experimentado dificultades para obtener datos almacenados en servidores del extranjero. A raíz de una compleja causa sobre la obtención en 2013 de datos de usuarios almacenados en servidores de Irlanda que enfrentó al Buró Federal de Investigaciones y a Microsoft[5], los Estados Unidos aprobaron la Ley de Aclaración del Uso de Datos en el Extranjero (CLOUD)[6], con el objetivo de: a) permitir a las autoridades policiales federales exigir a las empresas con sede en los Estados Unidos que proporcionen los datos de los usuarios almacenados en el extranjero sobre la base de una orden o un requerimiento judicial, siempre que no se vulneren los derechos de privacidad de una persona en el país extranjero donde se almacenan los datos; b) establecer un procedimiento por el cual los Estados Unidos puedan celebrar acuerdos ejecutivos con países extranjeros[7] respecto de la provisión de datos con fines policiales, siempre que dichos países extranjeros respeten el estado de derecho y la protección de la privacidad. Dichos acuerdos ejecutivos pretenden agilizar el acceso a los datos con fines policiales, que tradicionalmente ha sido lento en el marco de los tratados de asistencia judicial recíproca (United States Department of Justice, 2019).

Los Estados Unidos han optado por un enfoque sectorial flexible y ad hoc de la regulación de la privacidad de los datos, y han prescrito normas específicas solo en algunos ámbitos, como la privacidad infantil[8], la información sanitaria[9] y la privacidad de los datos financieros[10]. Sin embargo, aunque esas normativas sectoriales imponen requisitos relativamente estrictos a todos los proveedores de servicios, ninguna de ellas restringe los flujos de datos transfronterizos. En los últimos años ha aumentado la presión para aprobar una ley de privacidad a nivel federal, lo que llevó a la presentación del primer proyecto de ley en

3 Departamento de Defensa de los Estados Unidos, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)*, disponible en www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reportingand-contracting-for.

4 Departamento de Estado de los Estados Unidos, *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, 5 de agosto de 2020, disponible en https://2017-2021.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/index.html. Véase también “The Clean Network”, disponible en https://2017-2021.state.gov/the-clean-network/index.html.

5 *United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

6 *Clarifying Lawful Overseas Use of Data Act o CLOUD Ac*t (S.2383, H.R. 4943).

7 Hasta la fecha, los Estados Unidos y el Reino Unido han suscrito un acuerdo ejecutivo de este tipo. Departamento de Justicia, “U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online”, 3 de octubre de 2019, disponible en www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-accessagreement-combat-criminals-and-terrorists.

8 La Ley de Protección de la Privacidad Infantil en Línea prescribe los requisitos para la recopilación de información personal de los niños y niñas menores de 13 años, incluida la obtención del consentimiento verificable de sus progenitores.

9 La Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996 crea normas nacionales para la protección de la información sanitaria sensible de los pacientes, y prevé el consentimiento expreso de estos para la divulgación de los datos.

10 La Ley Gramm-Leach-Bliley establece normas para que las instituciones financieras protejan y almacenen la información de sus clientes.

marzo de 2021[11]. Además, algunos estados, como California y Virginia[12], han aprobado completas leyes de privacidad que garantizan robustos derechos individuales en la materia (Christakis, 2020).

Es posible que estos avances hacia la regulación de la privacidad en algunos estados de los Estados Unidos, junto con la propuesta de regulación federal en la materia, apunten a un cambio de rumbo hacia un planteamiento menos alineado con el enfoque de libre mercado promovido por las empresas digitales de gran tamaño. Ocurre lo mismo en el ámbito de la legislación antimonopolio, en el que el Congreso ha llevado a cabo una pormenorizada investigación sobre la competencia en los mercados digitales, y se han emprendido diferentes acciones antimonopolio en las que participan varios estados, el Departamento de Justicia y la Comisión Federal de Comercio[13]. También es una señal de que las autoridades se están dando cuenta de que los excesos de estas empresas pueden tener efectos indeseables en la sociedad que tal vez sea necesario corregir con la actuación del Estado. Además, las recientes prohibiciones de las actividades de algunas empresas digitales extranjeras (por ejemplo, Huawei, TikTok y Grindr) en el mercado estadounidense también apuntan a una mayor intervención del Estado en los mercados y a un aumento de las restricciones relacionadas con los datos y los flujos de datos transfronterizos, por motivos de seguridad nacional. Cabe afirmar en ese sentido que los Estados Unidos abogan por una política de libre circulación de los datos para sus empresas en todo el mundo —y, por tanto, por la libre entrada de datos extranjeros en el país—, pero al mismo tiempo imponen una política que impide a las empresas extranjeras de datos penetrar en el mercado estadounidense y prohíbe la salida de flujos de datos nacionales conexos.

2. Defensa de la seguridad nacional y pública y fomento del desarrollo digital: el enfoque de China

A diferencia del enfoque de libre mercado de los Estados Unidos, el sistema económico y político chino se caracteriza por una marcada intervención del Estado en la economía y la sociedad, lo que naturalmente se traduce en un enfoque intervencionista del Estado en la economía digital y, por tanto, en una estricta regulación de los flujos de datos transfronterizos. En China, las instancias normativas controlan los datos y la información, no solo cuando estos atraviesan las fronteras, sino también dentro del país, para mantener la estabilidad social y nutrir los sectores basados en el conocimiento.

China ha creado un excepcional sector digital nacional, lo cual puede atribuirse a una serie de factores, como la limitada competencia extranjera (gracias en parte al "Gran Cortafuegos"), el enorme mercado interno, la laxa aplicación de las leyes de propiedad intelectual en el país, el contar con competencias y recursos tecnológicos adecuados, la fuerte capacidad reguladora y las inversiones estratégicas públicas y privadas en el sector digital (Foster y Azmeh, 2020). El desarrollo digital es un componente clave de la iniciativa Hecho en China 2025, que incluye la concesión de subvenciones a plataformas chinas emergentes; cuantiosas inversiones del Estado en tecnologías digitales emergentes y de próxima generación, como la IA y la Internet de las cosas; y el fomento del crecimiento de las empresas chinas en los mercados regionales. La ampliación de las capacidades tecnológicas nacionales y la autosuficiencia en las tecnologías esenciales también ocupan un lugar destacado en las prioridades del Gobierno de China. No obstante, el país ha tomado medidas recientemente en materia de política de competencia

[11] Véase, por ejemplo, Remarks at the Future of Privacy Forum by Christine S Wilson, Commissioner, United States Federal Trade Commission "A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation", 6 de febrero de 2020, disponible en www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_ speech_02-06-2020.pdf; e IAPP, "The first but not last comprehensive US privacy bill of 2021", 17 de marzo de 2021.

[12] Ley de Privacidad del Consumidor de California de 2018 [1798.100 - 1798.199] y Ley de Protección de Datos del Consumidor de Virginia de 2021.

[13] Véase Subcomité de Derecho Antimonopolio, Comercial y Administrativo del Comité Judicial, Investigation of Competition in Digital Markets, disponible en https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519; y *The Guardian*, 19 de diciembre de 2020, "'This is big': US lawmakers take aim at once-untouchable big tech".

para poner freno al gran poder de mercado de algunas empresas (por ejemplo, imponiendo una histórica multa de 2.800 millones de dólares a Alibaba en relación con una investigación antimonopolio)[14].

El modelo regulador de China en materia de flujos de datos transfronterizos se basa en el papel central de la ciberseguridad en la seguridad nacional (Lee, 2018; Liu, 2020) y es, por tanto, muy restrictivo. Al mismo tiempo, China destaca como un ejemplo excepcional de éxito entre los países en desarrollo, ya que su modelo restrictivo, junto con varias intervenciones estratégicas del Estado, ha estimulado el crecimiento del mercado digital nacional y ha conducido además al éxito en todo el mundo de varias empresas tecnológicas chinas, como Baidu, Alibaba, Meituan Dianping y Tencent. Así pues, aunque la razón predominante para la regulación de los datos transfronterizos en China es la seguridad nacional y la estabilidad social, con el paso del tiempo la agenda económica ha adquirido una mayor centralidad y relevancia en sus políticas de regulación de los datos. Esto se tradujo inicialmente en un enfoque orientado a la regulación de los flujos entrantes de datos por razones de seguridad nacional y vigilancia (Nussipov, 2020a), y también en un mayor interés por restringir los flujos salientes. Sin embargo, la protección de la privacidad no ha sido una prioridad, y China es uno de los principales actores en términos de vigilancia digital en masa (véase el capítulo I).

China ha introducido varias restricciones relativas a los flujos de datos transfronterizos en su legislación nacional. Por ejemplo, su ley nacional de ciberseguridad exige a los proveedores de "infraestructuras críticas" que almacenen los "datos importantes" y la "información personal" dentro de China[15]. El término "infraestructuras críticas" se define de forma amplia y ambigua, e incluye los servicios públicos de comunicaciones, la energía, el transporte, la conservación del agua, las finanzas, los servicios públicos, los asuntos de gobierno electrónico o cualquier otro ámbito en el que la pérdida, destrucción o filtración de datos pueda "resultar en un daño grave para la seguridad del Estado, la economía nacional o los medios de vida de las personas y los intereses públicos"[16]. Además, el envío transfronterizo de datos personales por los proveedores de infraestructuras críticas está sujeto a un pormenorizado examen de seguridad por las autoridades reguladoras[17] y, con el fin de garantizar la seguridad pública y facilitar el acceso de dichas autoridades a los datos, China impone varias condiciones de localización de los datos que son específicas para cada sector, entre ellas las relativas a la información sanitaria[18], la información recopilada por organizaciones de investigación[19], la información personal recopilada por bancos comerciales[20], los servicios de cartografía en línea[21], la información personal y los datos comerciales recopilados por las plataformas de taxis en línea[22] y los operadores de alquiler de bicicletas por Internet[23], así como una restricción general a la transferencia transfronteriza de secretos de Estado[24].

El enfoque chino de preservación de la cibersoberanía ha evolucionado a lo largo de los años, de manera que actualmente incluye también la regulación del *hardware* (controlando cómo circulan los datos a través de las redes; por ejemplo, el intercambio de datos en los puntos de intercambio de tráfico de Internet (IXP)), del *software* (como el acceso a las redes privadas virtuales) y de los datos y contenidos (Gao, 2019). Además, China ejerce un control estricto sobre los protocolos de Internet y de datos utilizados en las

14 *The Verge*, 10 de abril de 2021, "China fines Alibaba $2.8 billion after antitrust investigation".

15 Artículo 37 de la Ley de Ciberseguridad (China).

16 Artículo 31 de la Ley de Ciberseguridad (China).

17 Proyecto de medidas sobre la evaluación de la seguridad de la transferencia transfronteriza de información personal (China).

18 Artículo 10 de las Medidas de Gestión de la Población y la Asistencia Sanitaria (China).

19 Artículo 24 del Reglamento sobre la Administración de la Industria de Investigación Crediticia (China).

20 Artículo 6 de la Nota de Llamamiento a Proteger la Información Financiera Personal destinada a las Instituciones Financieras Bancarias (China).

21 Artículo 34 del Reglamento para la Administración de los Servicios de Cartografía (China).

22 Artículo 27 de las Medidas Provisionales para la Administración de las Operaciones y Servicios Comerciales de Reserva de Taxis en Línea (China).

23 Artículo 4, párr. 13, de las Directrices para Fomentar y Regular el Desarrollo del Alquiler de Bicicletas por Internet (China).

24 Artículo 48 de la Ley de la República Popular China sobre la Protección de los Secretos de Estado (versión revisada de 2010) (China).

tecnologías nacionales, lo que aumenta indirectamente el control soberano sobre los flujos de datos (Hoffman y otros, 2020). De hecho, China está promoviendo la estandarización en el sector tecnológico, con vistas a influir en las normas mundiales, mediante la iniciativa "Estándares Chinos 2035". Por ejemplo, en la Unión Internacional de Telecomunicaciones este país ha propuesto un nuevo sistema de protocolo IP que podría cambiar la forma en que se transmiten los datos[25]. El Gobierno también ha propuesto una normativa que obligaría a enrutar el tráfico localmente si un usuario de China accede a un sitio web local (Bennett y Raab, 2020).

Actualmente, China está ultimando su marco de protección de datos, en el que se propone que para transferir de manera transfronteriza datos personales deba cumplirse una de las condiciones siguientes: a) la transferencia de datos debe superar una evaluación de las autoridades en cuanto a la seguridad; b) el Estado debe haber proporcionado una certificación de protección de la información personal para la transferencia de datos; c) la transferencia de datos debe realizarse de conformidad con un acuerdo internacional; y d) la transferencia de datos debe cumplir el resto de las condiciones especificadas en la normativa[26]. Además, esta ley incluye un claro mandato de localización de los datos: todos los operadores de infraestructuras de información críticas y los encargados del tratamiento de la información personal notificados deben almacenar la información personal que recopilen en el territorio nacional[27]. Además, el Gobierno tiene la intención de suscribir acuerdos internacionales para la transferencia de datos personales y el reconocimiento mutuo de las normas de protección de la información personal[28].

El interés económico de China en el mercado digital puede explicar el sutil cambio en su postura sobre los flujos de datos transfronterizos —que antes no era negociable— en los últimos meses. Por ejemplo, en 2020, el país manifestó su disposición a permitir los flujos de datos transfronterizos en la zona franca de Hainán[29]. Del mismo modo, en otra declaración, el Gobierno señaló la importancia de la coordinación internacional en materia de seguridad de datos y rechazó la adopción de disposiciones "uniformes" para el almacenamiento de datos en el territorio chino, con el fin de garantizar la seguridad nacional en un entorno económico global impulsado por la tecnología digital (Liu, 2020:94)[30]. Uno de los motores del cambio en la política de China sobre los flujos de datos comerciales podría ser el deseo de facilitar el componente digital de la Iniciativa de la Franja y la Ruta, conocida como la Ruta de la Seda Digital, que se puso en marcha en 2015 (Liu, 2020). Se trata de una estrategia importante con la que China pretende ampliar su influencia a nivel mundial en la economía digital impulsada por los datos, como se analiza más adelante.

3. Protección de los derechos individuales y los valores fundamentales: el enfoque de la Unión Europea

A diferencia del enfoque de los Estados Unidos, que promueve el control de los datos por el sector privado, y del de China, basado en el control de los datos principalmente por el Estado, la Unión Europea hace hincapié en el control de los datos por los particulares. En consecuencia, su enfoque de la economía digital impulsada por los datos, con un potente componente regulador, se basa en la protección de los derechos y los valores fundamentales de la Unión Europea y, por ello, se considera un enfoque antropocéntrico[31]. Así pues, la normativa sobre los flujos de datos transfronterizos es relativamente

[25] Para más información sobre la nueva propuesta en materia de IP, véase Internet Society (2020b). Para información relativa al contenido de la iniciativa "Estándares Chinos 2035", véase Datenna, "China Standards 2035: A Global Standard for Emerging Technologies", 15 de junio de 2020, disponible en https://www.datenna.com/2020/06/15/china-standards-2035-a-global-standard-for-emerging-technologies/ y Rühlig (2020).

[26] Artículo 38 de la Ley de Protección de los Datos Personales (China).

[27] Artículo 40 de la Ley de Protección de los Datos Personales (China).

[28] Artículo 12 de la Ley de Protección de los Datos Personales (China).

[29] *The Diplomat*, 4 de junio de 2020, "Is China Changing Its Thinking on Data Localization?".

[30] De hecho, como indica Liu, el Comité Permanente de la Asamblea Popular Nacional también propuso incluir una disposición en la Ley de Ciberseguridad de China destinada a permitir la circulación de los datos en el marco de un tratado internacional.

[31] Véase Unión Europea, "Principles for a human-centric, thriving and balanced data economy", disponible en https://dataprinciples2019.fi/wp-content/uploads/2019/09/Dataprinciples_web_1.0.pdf.

estricta y se centra en gran medida en la protección de la privacidad de las personas. La Unión Europea pretende construir un mercado digital único dentro de sus fronteras, en el que los productos digitales, así como los datos, circulen libremente cumpliendo un conjunto de normas diseñadas para proteger a los particulares, las empresas y los Gobiernos de los abusos derivados de la recopilación, el procesamiento y la comercialización de los datos.

La regulación de la economía digital y de los datos en la Unión Europea se ha llevado a cabo en su mayor parte de forma defensiva o reactiva, ya que pretende abordar las preocupaciones derivadas de las actividades de las plataformas digitales globales, por ejemplo, respecto de los abusos de posición dominante en el mercado, la competencia o la fiscalidad, además de la protección de los datos. Como se destaca en una publicación anterior de la UNCTAD (2019a) y en el capítulo I de este Informe, la mayoría de las plataformas digitales globales tienen su sede en los Estados Unidos o en China, mientras que las plataformas digitales domiciliadas en la Unión Europea son relativamente marginales. En los últimos años, la Unión Europea ha adoptado una postura más proactiva para desarrollar la economía digital impulsada por los datos, con múltiples iniciativas políticas a ese respecto. La Unión Europea también se caracteriza por contemplar las diferentes políticas en materia de economía digital con un enfoque más integrado que en el resto del mundo[32].

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que entró en vigor en 2018, es uno de los marcos de protección de datos más completos del mundo, y contiene amplios requisitos para la transferencia de datos personales fuera de la región. Sin embargo, no existe ninguna restricción explícita para las transferencias transfronterizas de datos no personales en la Unión Europea. El RGPD es aplicable al procesamiento o tratamiento[33] de cualquier "dato personal", que se define como "toda información sobre una persona física identificada o identificable"[34]. El planteamiento fundamental del RGPD es que los datos personales solo pueden transferirse y tratarse fuera de la Unión Europea si se respetan plenamente los derechos de privacidad de su ciudadanía[35]. A tal efecto, la transferencia automática de datos personales solo se permite a un grupo específico de países y territorios que la Comisión Europea ha aprobado por tener marcos de protección de datos que son esencialmente equivalentes al RGPD ("decisión de adecuación")[36]. Hasta la fecha, la Comisión Europea ha entendido que Andorra, la Argentina, el Canadá (organizaciones comerciales), Guernsey, las Islas Feroe, la Isla de Man, Israel, el Japón, Jersey, Nueva Zelandia, Suiza y el Uruguay ofrecen una protección adecuada[37]. Estas decisiones de adecuación son el resultado de extensas negociaciones bilaterales, y la Comisión Europea ha tenido en cuenta varios factores de esas economías extranjeras, como sus marcos de privacidad y protección de datos, el respeto del estado de derecho, los compromisos internacionales en materia de protección de datos y la solidez de su relación económica y política con la Unión Europea[38].

La transferencia de datos personales a países no pertenecientes a la Unión Europea que no hayan sido objeto de una decisión de adecuación solo es posible en dos supuestos: a) si el encargado del tratamiento de los datos puede ofrecer "garantías adecuadas", que pueden ser normas corporativas vinculantes que permitan las transferencias dentro de la empresa, cláusulas contractuales tipo adoptadas por la Comisión Europea para las transferencias entre empresas y mecanismos de certificación aprobados por

[32] Véase "La Década Digital de Europa: metas digitales para 2030", disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es.

[33] El tratamiento se define ampliamente en el RGPD (artículo 4, párr. 2) como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

[34] Artículo 4, párr. 1, del RGPD.

[35] Considerando 101 del RGPD.

[36] Artículo 45, párr. 1, del RGPD.

[37] La evolución de la situación con respecto a las decisiones de adecuación puede consultarse en "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/lawtopic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[38] Artículo 45, párr. 2, del RGPD.

la Unión[39]; o b) si es aplicable una de las siguientes excepciones: el encargado del tratamiento obtiene el consentimiento explícito del interesado para la transferencia tras informarle de los riesgos, la transferencia de datos es necesaria para la ejecución de un contrato, por razones importantes de interés público o para proteger los intereses vitales del interesado, o si la transferencia se realiza desde un registro público[40]. Sin embargo, estas excepciones solo pueden utilizarse en situaciones específicas, y no para las transferencias transfronterizas de datos habituales.

Aunque el RGPD es una normativa aplicable a los datos personales dentro de la Unión Europea, tiene un efecto extraterritorial, ya que se aplica a todas las actividades de los responsables o encargados del tratamiento de datos en la Unión, "independientemente de que el tratamiento tenga lugar en la Unión"[41]. Por "responsable del tratamiento" se entiende todo organismo que determine "los fines y medios del tratamiento" de los datos personales[42], mientras que el término "encargado del tratamiento" alude a los organismos "que tratan datos personales por cuenta del responsable del tratamiento"[43]. Debido a esta disposición, aunque una empresa no tenga presencia física en la Unión Europea, está obligada a cumplir el RGPD si sus actividades comerciales incluyen la oferta de productos o servicios digitales en la Unión o el seguimiento del comportamiento de sus residentes[44]. No obstante, esta extraterritorialidad puede plantear algunos problemas de aplicación (Greze, 2019).

En los últimos años, la Unión Europea ha hecho cierto hincapié en el objetivo de la "soberanía digital". Esto se debe a varios factores, como el predominio de las empresas estadounidenses y chinas en el sector de la tecnología digital y la necesidad de reducir la dependencia de las tecnologías externas ante la falta de empresas tecnológicas europeas de éxito. También refleja la preocupación por la capacidad de la Unión Europea para garantizar la privacidad de su ciudadanía y los riesgos de seguridad asociados a las tecnologías extranjeras (Hesselman y otros, 2020). Por ejemplo, la incapacidad de los Gobiernos de la Unión Europea para desarrollar aplicaciones nacionales de rastreo de contactos durante la pandemia de COVID-19 y su dependencia de las tecnologías diseñadas por Google y Apple se interpretaron como importantes limitaciones a su soberanía digital. Aunque no existe una definición clara de "soberanía digital" en las políticas de la Unión Europea, puede considerarse que esta expresión se refiere en términos generales al aseguramiento y protección de la infraestructura digital de Europa y a la preservación de los derechos de privacidad de la ciudadanía europea, que incluyen su derecho a decidir quién utiliza sus datos personales y dónde y cómo lo hace (Christakis, 2020)[45]. El objetivo de la soberanía digital queda reflejado en una reciente iniciativa europea denominada GAIA-X[46] (recuadro IV.1), propuesta por primera vez por los Gobiernos de Francia y Alemania.

La integración digital ha sido uno de los ámbitos priorizados por las instancias normativas europeas en los últimos años, con iniciativas como el Mercado Único Digital. La Estrategia Europea de Datos es un pilar fundamental de esos esfuerzos y, en ese contexto, se ha propuesto la Ley de Gobernanza de Datos para mejorar la disponibilidad de datos y reforzar los mecanismos de intercambio de datos en toda la Unión Europea. La ley contiene disposiciones específicas para la transferencia de datos no personales a países no pertenecientes a la Unión Europea, en línea con las decisiones de adecuación en el marco del RGPD. Aunque los requisitos no son equivalentes a los aplicables a la localización de

39 Artículo 46, párr. 2, del RGPD.

40 Artículo 49 del RGPD.

41 Artículo 3, párr. 1, del RGPD.

42 Artículo 4, párr. 7, del RGPD.

43 Artículo 4, párr. 8, del RGPD.

44 Artículo 3, párr. 2, del RGPD

45 Véase también Statement by European Commission President von der Leyen at the round table event "Internet, a new human right", after the intervention by Sir Berners-Lee, 28 de octubre de 2020, disponible en https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1999.

46 Véase "GAIA-X. A federated data infrastructure for Europe", disponible en www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

Recuadro IV.1. GAIA-X

GAIA-X es una organización internacional sin fines de lucro con sede en Bélgica que nació a raíz de una propuesta de los Gobiernos de Alemania y Francia en 2019 con el fin de dotar el mercado europeo de una infraestructura en la nube de carácter federado que facilitase el intercambio interoperable de datos en la Unión Europea al amparo de sus leyes, y se ha convertido en una iniciativa europea. Su objetivo es crear una "infraestructura de datos de alto rendimiento, competitiva, segura y fiable para Europa" que permita materializar "las más altas aspiraciones en términos de soberanía digital y que a la vez fomente la innovación". Así pues, pretende dotar a Europa de una infraestructura de datos federada que se base en estándares abiertos e interoperables y facilite un mercado único de datos en la Unión Europea, lo que a su vez podría impulsar la capacidad de los proveedores europeos de servicios en la nube para monetizar los datos y, a largo plazo, afianzar la posición de las empresas digitales europeas en el mercado.

La iniciativa promueve la noción europea de soberanía digital basada en la transparencia, la apertura, la protección de datos y la seguridad. Su objetivo es crear una infraestructura y un ecosistema seguros y robustos en la Unión Europea para facilitar el intercambio de datos entre los diversos sectores económicos europeos y, de ese modo, apoyar el crecimiento de aquellos que se nutren de datos impulsando la IA, la Internet de las cosas y el análisis de macrodatos.

La iniciativa GAIA-X da cabida también a las empresas extranjeras, siempre y cuando respeten los principios y las políticas que siguen sus homólogas de la Unión Europea en el marco de la iniciativa. Entre los resultados esperados de esta iniciativa cabe citar el favorecimiento de la infraestructura de datos en Europa, la promoción de las empresas nacionales, una mayor adhesión a los valores europeos y una reducción de la excesiva dependencia de las empresas tecnológicas estadounidenses y chinas. Se espera que el proyecto se convierta en un revulsivo del sector digital en la Unión Europea y que mejore la capacidad de sus Gobiernos para garantizar la adopción de las normas de la Unión Europea en materia de privacidad. La iniciativa se concretizará en 2021.

Fuente: UNCTAD, a partir de Project GAIA-X, disponible en www.bmwi.de/Redaktion/EN/Publikationen/DigitaleWelt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6; BMWI, GAIA-X A Federated Data Infrastructure for Europe, disponible en www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html; *The Financial Times*, 21 de diciembre de 2020, "Regulation alone will not strengthen Europe's digital sector"; y Reunión extraordinaria del Consejo Europeo (1 y 2 de octubre de 2020) – Conclusiones (punto 9), disponible en https://www.consilium.europa.eu/media/45932/021020-euco-final-conclusions-es.pdf.

los datos, imponen un marco estricto para la transferencia transfronteriza de datos públicos fuera de la Unión Europea[47].

Dada la importancia de los flujos de datos entre la Unión Europea y los Estados Unidos, en 2016 se suscribió un acuerdo transatlántico para permitir la transferencia transfronteriza de datos personales: el Escudo de la Privacidad Unión Europea-Estados Unidos. Este acuerdo sustituyó al régimen de puerto seguro entre la Unión Europea y los Estados Unidos, que había sido invalidado por el Tribunal de Justicia de la Unión Europea en el asunto *Schrems I* en 2015. En virtud del Escudo de la Privacidad, las empresas podían certificar por sí mismas que cumplían el RGPD y, a partir de entonces, transferir datos de la Unión Europea a los Estados Unidos. Sin embargo, la sentencia del Tribunal de Justicia de la Unión Europea en el caso *Schrems II* invalidó dicho acuerdo en julio de 2020[48]. En este litigio, el tribunal consideró que las leyes relativas a la vigilancia de datos en los Estados Unidos eran incompatibles con el RGPD (recuadro IV.2).

[47] Véase la Estrategia Europea de Datos, disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es; y la Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0767&from=ES. Existen otras dos propuestas conexas, la Ley de Servicios Digitales y la Ley de Mercados Digitales (véase The Digital Services Act package, disponible en https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package).

[48] *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (asunto C-311/18, *"Schrems II"*).

Recuadro IV.2. El Escudo de la Privacidad y la sentencia en *Schrems II*

En julio de 2020, el Tribunal de Justicia de la Unión Europea, en el asunto *Schrems II*, invalidó el Escudo de la Privacidad por ser incompatible con la legislación de la Unión Europea en materia de protección de datos. En concreto, el Tribunal determinó que la normativa en materia de vigilancia de datos de los Estados Unidos, como el artículo 702 de la Ley de Vigilancia y Adquisición de Inteligencia Extranjera y la Orden Ejecutiva 12333, no proporcionaban una protección equivalente a la de la Unión Europea ni garantizaban los derechos vigentes en esta. Además, el Tribunal entendió que, aunque las cláusulas contractuales tipo eran un mecanismo válido para las transferencias de datos personales a países que no hubieran recibido una decisión de adecuación, podían necesitarse medidas complementarias para garantizar la protección de los datos personales de la ciudadanía europea. Posteriormente, en noviembre de 2020, el Comité Europeo de Protección de Datos formuló algunas aclaraciones sobre las medidas complementarias.

A partir de la sentencia del Tribunal, las transferencias de datos ya no están permitidas en el marco del Acuerdo del Escudo de la Privacidad. Varias asociaciones y especialistas del sector han criticado la sentencia en *Schrems II*, ya que crea nuevas incertidumbres para todas las empresas que utilizan las cláusulas contractuales tipo. Además, el enfoque invasivo del Tribunal de Justicia de la Unión Europea al examinar las leyes de vigilancia de los Estados Unidos no se refleja en prácticas similares para con los países miembros de la Unión Europea. En la respuesta de los Estados Unidos, este país afirmó que el Tribunal no había tenido en cuenta varios mecanismos de supervisión previstos en las leyes de vigilancia de los Estados Unidos y la existencia de instrumentos de reparación para las personas afectadas que incorporaba la Ley de Vigilancia y Adquisición de Inteligencia Extranjera.

Según voces expertas, la sentencia en el asunto *Schrems II* significa que a las empresas extranjeras les resultará más difícil operar en la Unión Europea si no tratan los datos en el territorio de la Unión, por lo que el fallo fomenta una suerte de "localización light de los datos" (Chander, 2020). Estudios recientes del sector también revelan repercusiones negativas de la sentencia en el plano económico, especialmente para las empresas de pequeño tamaño, tanto de la Unión Europea como de otros lugares (DigitalEurope y otros, 2020). Además, las empresas han expresado su preocupación por el requisito de aplicar "medidas complementarias" a las cláusulas contractuales tipo y, aunque el Comité Europeo de Protección de Datos publicó posteriormente unas directrices sobre este tipo de cláusulas (European Data Protection Board, 2020), estas no aportan suficiente claridad e introducen limitaciones adicionales a la transferencia transfronteriza de datos personales a países que no han recibido una decisión de adecuación, como requisitos en materia de encriptación mejorada (Christakis, 2020).

Fuente: UNCTAD.

En su legislación, la Unión Europea no favorece la localización de los datos *per se*[49]. Por ejemplo, en el RGPD se reconoce la importancia de los flujos transfronterizos de datos personales para la expansión del comercio y la cooperación internacionales[50], pero dados los estrictos requisitos de ese reglamento, no existen opciones sencillas para los flujos de datos transfronterizos, ya que pocos países han recibido una decisión de adecuación. Por otra parte, algunas iniciativas recientes —como la Ley de Gobernanza de Datos, la sentencia del Tribunal de Justicia de la Unión Europea en el asunto *Schrems II* o la iniciativa GAIA-X— podrían indicar que la postura de la Unión Europea en materia de localización de los datos está evolucionando. Tanto es así que es posible que esas iniciativas repercutan en la política comercial de la Unión Europea, como afirma la Comisión Europea (European Comission, 2021:15): "La cuestión de los datos será esencial para el futuro de la UE. Por lo que respecta a las transferencias transfronterizas de datos y la prohibición de los requisitos de localización de los datos, la Comisión mantendrá un enfoque

[49] Por ejemplo, en el Reglamento para la libre circulación de datos personales, los miembros acuerdan que "los Estados miembros solo deberían poder invocar la seguridad pública como justificación de los requisitos de localización de datos". Véase el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, párr. 18. Del mismo modo, en varias negociaciones comerciales recientes, como las entabladas con Nueva Zelandia y Australia, la Unión Europea ha propuesto disposiciones que prohíben las medidas de localización de los datos.

[50] Considerando 101 del RGPD.

abierto, pero firme, basado en los valores e intereses europeos. La Comisión trabajará por garantizar que sus empresas puedan beneficiarse de la libre circulación de datos a nivel internacional respetando plenamente las normas de protección de datos de la UE y otros objetivos de servicio público, como la seguridad y el orden públicos. En particular, la UE seguirá abordando los obstáculos injustificados a los flujos de datos, preservando al mismo tiempo su autonomía normativa en el ámbito de la protección de datos y la privacidad". Además, en el contexto de las negociaciones de la OMC, la Unión Europea declaró que "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 de datos transfronterizos 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; 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"[51].

En el cuadro IV.1 se presenta un resumen de las principales características de las políticas de los Estados Unidos, China y la Unión Europea en materia de datos.

Cuadro IV.1. Principales características de las políticas de los Estados Unidos, China y la Unión Europea en materia de datos

	Estados Unidos	China	Unión Europea
Crecimiento económico y desarrollo en la economía digital impulsada por los datos	Principalmente basado en el mercado	Fuerte intervención del Estado	Regulación; parte del plan de recuperación tras la COVID-19 para apoyar el desarrollo de la economía digital
Protección de datos y privacidad	Históricamente no se ha priorizado; no hay una ley federal completa (pero sí debates y propuestas); California y Virginia cuentan con leyes estatales	Normas centradas en las empresas	RGPD, basado en los derechos fundamentales
Seguridad nacional	Los datos ligados a la seguridad nacional son una clara prioridad	Amplio acceso y control del Estado	Competencia de cada miembro; en determinadas circunstancias el criterio de la Unión Europea prevalece
Política de competencia	El área de la competencia no suele englobar los datos, pero la tendencia está cambiando, con importantes investigaciones y causas judiciales sobre prácticas monopolísticas	No está claro si el área de la competencia engloba los datos; puede apoyar a las empresas nacionales y estatales; reciente multa antimonopolio a Alibaba	El área de la competencia puede englobar los datos
Flujos de datos transfronterizos	Se promueve la libre circulación de los datos	Amplias restricciones a los flujos de datos	Libre circulación de los datos dentro de la Unión Europea y los Estados que han recibido una decisión de adecuación; la política comercial promueve la libre circulación de los datos, pero algunas iniciativas recientes apuntan a restricciones

Fuente: UNCTAD, a partir, parcialmente, de Government Office for Science, Reino Unido (2020).

[51] Véase Comunicación de la Unión Europea, "Declaración conjunta sobre el comercio electrónico: Propuesta de disciplinas y compromisos en el marco de la OMC sobre el comercio electrónico presentada por la UE" (INF/ECOM/22), 26 de abril de 2019, disponible en https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/253698/s/INF/ECOM/22.pdf (pág. 4).

Como se analizará en la sección C, estos son los tres principales enfoques que tienen una especial influencia a nivel mundial. Aunque los planteamientos de la Federación de Rusia y de la India también se presentan en esta sección, su influencia en el plano mundial es relativamente limitada. La Federación de Rusia ejerce una influencia que se circunscribe principalmente al ámbito regional, como economía líder e impulsora del desarrollo digital en la Unión Económica Euroasiática (Abramova y Thorne, 2021). Por su parte, el enfoque de la India se centra mayormente en el mercado nacional, sin que por el momento se atisben ambiciones de expansión, aunque el país es un actor de peso entre los países en desarrollo en las deliberaciones internacionales sobre cuestiones relacionadas con la economía digital[52].

4. Protección de la seguridad nacional y pública: el enfoque de la Federación de Rusia

Al igual que el modelo chino, el planteamiento regulador ruso en materia de flujos de datos transfronterizos se centra en la seguridad de las redes y los datos, que se considera una cuestión política y de seguridad nacional. La Federación de Rusia entiende que la ciberseguridad es una prerrogativa puramente soberana (Nocetti, 2015). Sin embargo, a diferencia de China, la Federación de Rusia no ha hecho tanto hincapié en los aspectos económicos del desarrollo digital y ha tenido un éxito relativamente más velado en cuanto a la promoción del sector digital nacional, excepción hecha de casos notables como Yandex (plataforma de motores de búsqueda) y Kaspersky (proveedor de servicios de ciberseguridad y *software* antivirus).

La Federación de Rusia ha impuesto una serie de restricciones a los flujos de datos transfronterizos. La más importante es la exigencia general de localización de los datos personales, que obliga a todas las empresas que operan en el país a "registrar, sistematizar, acumular, almacenar, modificar, actualizar y recuperar los datos personales de toda la ciudadanía rusa utilizando servidores rusos"[53]. El Servicio Federal de Supervisión de las Comunicaciones, las Tecnologías de la Información y los Medios de Comunicación ha aclarado que, para cumplir dicha disposición, toda empresa cuyas actividades comerciales se centren en el país (por ejemplo, si tiene un sitio web en ruso o muestra precios en rublos) debe inicialmente registrar y almacenar las copias maestras de esos datos personales en servidores ubicados en el territorio nacional de la Federación de Rusia, si bien posteriormente puede albergar copias de esos datos en servidores extranjeros (Savelyev, 2016)[54]. Además, varias leyes nacionales incluyen vigorosas medidas de control de la información, por ejemplo obligando a las empresas a permitir el acceso a los datos encriptados como y cuando lo requieran las autoridades (Maréchal, 2017). La Federación de Rusia aprobó recientemente un conjunto de enmiendas a sus leyes federales sobre las "comunicaciones" y sobre la "información, las tecnologías de la información y la protección de la información" (a menudo, los medios de comunicación de otros países utilizan la expresión "Ley de Internet Soberana" para referirse a esta última) que exigen a todos los proveedores de Internet rusos la instalación de *hardware* para enrutar todo el tráfico nacional de Internet a través de servidores ubicados en el país[55]. Además, estas enmiendas posibilitan la implantación de un sistema ruso de nombres de dominio que permitiría el funcionamiento de Internet en el país en caso de desconexión de la red mundial (Epifanova, 2020).

---

52 Algunos países, como Kenya, Nigeria, Sudáfrica y Rwanda, parecen estar influidos por ideas similares a las de la localización de los datos en la India (Elmi, 2020).

53 Artículo 18, párr. 5, de la Ley Federal núm. 152-FZ, de Datos Personales, con las enmiendas introducidas en julio de 2014 por la Ley Federal núm. 242-FZ, por la que se modifican algunos instrumentos legislativos de la Federación de Rusia para aportar claridad en el ámbito del tratamiento de datos personales en las redes de información y telecomunicaciones (Federación de Rusia).

54 Según la Ley Federal núm. 152-FZ, de Datos Personales (Federación de Rusia), las transferencias transfronterizas solo están permitidas hacia países que hayan firmado el Convenio del Consejo de Europa de 1981, o hacia países que hayan recibido la aprobación expresa del regulador (Angola, Argentina, Australia, Benin, Canadá, Chile, Costa Rica, Gabón, Israel, Japón, Kazajstán, Malasia, Malí, Mongolia, Marruecos, Nueva Zelandia, Perú, Qatar, República de Corea, Singapur, Sudáfrica y Túnez).

55 *BBC News*, 1 de noviembre de 2019, "Russia Internet: Law introducing new controls comes into force", disponible en www.bbc.com/news/world-europe-50259597.

A diferencia de China, la Federación de Rusia no contaba hasta hace muy poco con una estrategia económica para desarrollar el sector digital nacional, pues su Programa de Economía Digital fue establecido en 2017 (Lowry, 2020). Según especialistas, el Gobierno considera necesaria la autosuficiencia tecnológica en la medida en que se requiere para establecer una industria nacional soberana libre de influencias extranjeras; sin embargo, no existe una ambición sostenida de que las empresas digitales rusas compitan en el mercado global (Budnitsky y Jia, 2018). La plataforma digital de mayor éxito en la Federación de Rusia es Yandex, que representa aproximadamente el 55 % del mercado nacional de motores de búsqueda. Yandex se considera superior al motor de búsqueda de Google debido a sus excepcionales capacidades en ruso[56]. Otras empresas, como Mail.ru y Avito, han cosechado un éxito moderado en el mercado nacional (Eferin y otros, 2019). Las plataformas rusas no tienen un gran mercado fuera del país, y solo son populares en algunos países con poblaciones rusohablantes.

5. Fomento del desarrollo digital nacional: el enfoque de la India

En contraste con los anteriores planteamientos sobre los flujos de datos transfronterizos, la India está evolucionando cada vez más hacia un enfoque de regulación centrado principalmente en maximizar los beneficios económicos y sociales de los datos y los sectores impulsados por los datos para su ciudadanía y la economía nacional, y en minimizar la salida de ingresos hacia las empresas con sede en economías digitalmente avanzadas. La idea subyacente a este enfoque es proteger a la India del "colonialismo de datos", es decir, evitar que los países ricos obtengan beneficios de los flujos de datos transfronterizos a costa de perjudicar los intereses de la India (Weber, 2017).

El proyecto de ley de protección de los datos personales de 2019[57] y el proyecto de política nacional de comercio electrónico, que lleva el título "Los Datos de la India para el Desarrollo de la India"[58], describen claramente la ambición de este país de construir su sector digital aprovechando los datos de los habitantes de la India a través de medidas de localización de los datos. El proyecto de ley de protección de los datos personales contiene requisitos de localización de los datos, ya que exige que se almacene en la India una copia de los datos personales sensibles[59] y además prohíbe las transferencias transfronterizas de datos personales críticos[60]. Se consideran datos personales sensibles: a) los datos financieros, b) los datos sanitarios, c) los identificadores oficiales, d) la información referida a la vida sexual, e) los detalles relativos a la orientación sexual, f) los datos biométricos, g) los datos genéticos, h) las informaciones ligadas a la condición de persona transgénero, i) las referencias a la condición de persona intersexual, j) las indicaciones de casta o tribu, k) los pormenores que señalan creencias o afiliación religiosa o política, y l) cualquier otro tipo de información categorizada como dato personal sensible por el Gobierno[61]. Dada la amplitud del concepto de datos personales sensibles, la legislación propuesta genera una mayor carga para las empresas en comparación con el régimen actual (según el cual los datos pueden transferirse a cualquier país que ofrezca el mismo nivel de protección que la India, siempre que la transferencia sea necesaria para la ejecución de un contrato existente y que el usuario haya consentido en dicha transferencia)[62]. El Gobierno es libre de estimar qué informaciones se consideran "datos personales críticos", ya que este término no está definido[63]. Además, este proyecto de ley emula el planteamiento del RGPD al permitir la transferencia transfronteriza de datos personales solo en circunstancias limitadas: a

[56] *CNBC*, 21 de enero de 2019, "Google is the most popular search engine in most of the world except Russia – here's why", disponible en https://www.cnbc.com/2019/01/18/yandex-is-beating-google-in-russia.html.

[57] Proyecto de ley de protección de los datos personales (India), disponible en http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[58] Proyecto de política nacional de comercio electrónico: Los Datos de la India para el Desarrollo de la India, 2019, disponible en https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

[59] Artículo 33, párr. 1, del proyecto de ley de protección de los datos personales (India).

[60] Artículo 33, párr. 2, del proyecto de ley de protección de los datos personales (India).

[61] Artículo 3, párr. 36, del proyecto de ley de protección de los datos personales (India).

[62] Artículo 7 del Reglamento sobre Tecnología de la Información (prácticas y procedimientos razonables en materia de seguridad, e información y datos personales de carácter sensible) de 2011 (India).

[63] Artículo 33, párr. 2, explicación, del proyecto de ley de protección de los datos personales (India).

países a los que el Gobierno permite expresamente dicha transferencia (enfoque de adecuación); sujeta a la aprobación de mecanismos de transferencia de datos intragrupo; previo consentimiento del titular de los datos; y en respuesta a una necesidad específica, aprobada por el regulador[64].

El proyecto de política nacional de comercio electrónico[65] prevé amplias medidas relativas a la localización de los datos, aunque no incluye ninguna restricción explícita a los flujos transfronterizos de datos no personales. No obstante, más recientemente, un informe del Comité de Especialistas en Datos No Personales, creado por el Ministerio de Electrónica y Tecnología de la Información, ha recomendado que se adopten requisitos de localización de los datos para algunas categorías de datos no personales (en línea con el proyecto de ley de protección de los datos): los datos no personales de carácter general podrán almacenarse y tratarse en cualquier parte del mundo; los datos no personales sensibles podrán transferirse fuera del país, pero deben almacenarse en la India; y los datos no personales críticos solo podrán almacenarse y procesarse en la India[66]. Los requisitos de localización de los datos también se aplican a los datos recopilados con fondos públicos[67], a la información de los abonados recogida por las empresas de radiodifusión[68], a los libros de contabilidad electrónicos[69] y a la información recopilada por las compañías de seguros sobre las personas aseguradas[70].

Una de las motivaciones clave de las distintas propuestas reguladoras en materia de datos que existen en la India parece ser la protección de los intereses económicos del país, para lo cual se pretende conseguir que los datos digitales generados en la India se utilicen principalmente para el desarrollo de nuevas empresas digitales en el territorio nacional ("fomento de referentes nacionales en materia de datos"), y así hacer frente al "colonialismo de datos" de las grandes compañías tecnológicas[71].

Además de la protección de los intereses económicos, el enfoque normativo de la India sobre los flujos de datos transfronterizos se basa en las diversas ventajas que presenta la localización de los datos para garantizar una supervisión normativa eficaz y la aplicación de la legislación nacional. Por ejemplo, la India exige a todos los proveedores de sistemas de pago que almacenen los datos relativos a estos en la India (aunque dichos datos se procesen en el extranjero) para que el Banco de la Reserva de la India pueda "tener acceso irrestricto a los datos almacenados con esos proveedores de sistemas o con sus proveedores de servicios/intermediarios/proveedores externos y otras entidades del ecosistema de pagos, cuando así lo requieran sus actividades de supervisión"[72]. En el contexto de la protección de los datos personales, en el informe del Comité Srikrishna se afirma que "la aplicación efectiva de la ley de privacidad india requerirá indefectiblemente que los datos se almacenen en el territorio nacional, con lo que dicho requisito, cuando sea aplicable, limitará la permisibilidad de las transferencias transfronterizas" (Srikrishna Committee Report, 2018:87). Por otra parte, exigir la localización de los datos con fines legales también encaja en la lógica de desarrollo económico nacional que subyace al enfoque normativo de la India respecto de la regulación en materia de datos, es decir, si se logra que se almacenen más datos

64 Artículo 34 del proyecto de ley de protección de los datos personales (India).

65 Aún se estaba revisando cuando se elaboró el presente Informe.

66 Ministerio de Electrónica y Tecnología de la Información, Report by the Committee of Experts on Non-Personal Data Governance Framework (agosto de 2020), párr. 7.6 y recomendación 6 ix), disponible en https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

67 Política Nacional de Intercambio de Datos y Accesibilidad (India), 9 de febrero de 2014, disponible en https://dst.gov.in/national-datasharing-and-accessibility-policy-0.

68 Política Consolidada de IED de 2017 (India).

69 Artículo 3, párr 5, del Reglamento relativo a las Empresas (Contabilidad), 2014 (India).

70 Artículo 18 del Reglamento sobre la Subcontratación de Actividades por las Aseguradoras Indias (IRDAI), 2017 (India).

71 Véase, por ejemplo, Sinha y Basu (2019); *The Print*, 29 de septiembre de 2019, "Digital colonialism: Why countries like India want to take control of data from Big Tech"; y *Mint*, 20 de enero de 2019, "India's data must be controlled by Indians: Mukesh Ambani".

72 Nota del Banco de Reserva de la India sobre el almacenamiento de datos de los sistemas de pagos (India), RBI/2017-18/153, DPSS.CO.OD núm. 2785/06.08.005/2017-2018, 6 de abril de 2018, disponible en www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.

en la India, se conseguirá dotar al país de una mejor infraestructura digital para las tecnologías digitales emergentes, como la IA o la Internet de las cosas (Srikrishna Committee Report, 2018).

Algunas entidades de la sociedad civil han expresado su preocupación por el hecho de que el proyecto de ley de protección de los datos personales no incorpore garantías y controles adecuados, especialmente porque cualquier organismo gubernamental puede quedar eximido de cumplir la referida ley[73]. Por lo tanto, aunque el proyecto de ley de protección de los datos personales incluye requisitos estrictos de cumplimiento para las empresas privadas, también en lo que concierne a las transferencias transfronterizas de datos personales, sigue sin estar claro si este instrumento legislativo será igualmente eficaz para proteger a los particulares de la vigilancia del Estado (Burman, 2020).

C. ESTRATEGIAS DE EXPANSIÓN GLOBAL DE LOS ESTADOS UNIDOS, CHINA Y LA UNIÓN EUROPEA

Ante la toma de conciencia del enorme valor económico y estratégico que pueden tener los datos a raíz de los avances en tecnología digital, los Estados Unidos, China y la Unión Europea se han mostrado muy activos en lo referente a la expansión global de los enfoques que adoptan respecto de la economía digital impulsada por los datos, pues buscan capturar la mayor parte posible de las ganancias derivadas de los datos. Sus planteamientos de expansión coinciden con la lógica de sus normativas nacionales. En los Estados Unidos, el principal vector de expansión es la internacionalización de sus corporaciones digitales globales, que es facilitada por la libre circulación de los datos y la prohibición de los requisitos de localización de los datos en los acuerdos comerciales (véase el capítulo VI). En China, la Iniciativa de la Franja y la Ruta, impulsada por el Gobierno, apoya la expansión de sus grandes empresas globales de telecomunicaciones y servicios digitales a otros países. Las poderosas empresas digitales de esos países buscan nuevos mercados con un gran número de clientes potenciales aún no conectados a los mercados de Internet. Como la mayor parte de la población de las economías desarrolladas y de China está bien conectada, y sus datos ya están en gran medida bajo su control, los nuevos usuarios potenciales y el correspondiente acceso a nuevos datos se encuentran principalmente en las economías en desarrollo; a menudo se denomina a este grupo los “próximos 1.000 millones de usuarios” (Pisa y Polcari, 2019; Arora, 2019). En contraste, la estrategia de la Unión Europea se centra en la exportación de marcos normativos.

Estas estrategias de expansión tendrían como objetivo fundamental ampliar la influencia en la economía digital global impulsada por los datos, a fin de incrementar el poder derivado del control de los datos, que a su vez permite controlar los mercados y la sociedad. En el caso de los Estados Unidos y China, dado su dominio tecnológico, uno de los principales objetivos es establecer protocolos tecnológicos globales en el ámbito de los datos. La Unión Europea busca principalmente influir en los marcos normativos a nivel mundial. Si bien se intenta etiquetar estas estrategias de expansión respecto de los países en desarrollo como iniciativas para propiciar la cooperación internacional o actuaciones humanitarias u orientadas al desarrollo, la motivación real parece ser la extracción de datos de esos países para crear valor a partir de su tratamiento. Así pues, subyace una lógica extractiva en esas estrategias de expansión, que se asemeja a lo ocurrido con los países en desarrollo que se han especializado en la producción de recursos naturales. Estas prácticas darían lugar a un intercambio desigual, ya que los países que proporcionan los datos brutos pasan a depender en gran medida de los que los extraen hacia el extranjero y los controlan desde allí. Estos últimos tienen la capacidad tecnológica para captar el valor de los datos convirtiéndolos en inteligencia digital, mientras que los países en desarrollo tendrían que pagar si desean importar esos productos de datos, que podrían apoyar su desarrollo, cuando originalmente fueron generados gracias en parte a los datos brutos extraídos en su territorio[74].

Las corporaciones digitales globales de los Estados Unidos han puesto en marcha diferentes programas para mejorar el acceso a Internet en los países en desarrollo, como Facebook Free Basics o Google

[73] Artículo 35 del proyecto de ley de protección de los datos personales (India).

[74] Para un análisis de la lógica extractiva de la economía digital impulsada por los datos, véase Morozov (2017) y Gurumurthy y Chami (2020).

Project Loon. También están realizando grandes inversiones en infraestructuras digitales en los países en desarrollo. Por ejemplo, Facebook lidera el proyecto "2Africa", en el marco del cual se está construyendo un cable submarino alrededor de África que conectará 23 países de África, Asia Occidental y Europa de aquí a 2023[75]. Aunque estas iniciativas e inversiones en infraestructuras pueden aportar algunos beneficios a los países en desarrollo en términos de conectividad, no es evidente que compensen los costos (véase también el capítulo III). Es probable que resulten en una salida de datos generados en esos países hacia empresas de los Estados Unidos, lo que afectará a sus capacidades para innovar y generar valor con su tratamiento. Así pues, existe una creciente preocupación por esta nueva forma de "colonialismo" a través de los datos (Elmi, 2020), que puede plantear desafíos relacionados con la privacidad de los datos, la desinformación y el aumento de la concentración del mercado y las desigualdades (Pisa y Polcari, 2019). Otro de los métodos utilizados por esas corporaciones para expandirse por todo el mundo es la adquisición de nuevas empresas digitales de éxito y de competidores potenciales (UNCTAD, 2019a), lo que merma la capacidad de las empresas nacionales para favorecer el desarrollo a largo plazo.

China pretende contribuir a la cooperación Sur-Sur y ampliar su influencia a través de la Iniciativa de la Franja y la Ruta, que aúna las infraestructuras tradicionales con las tecnologías digitales que reflejan los valores y normas de China. Con la Ruta de la Seda Digital se persigue, entre otros objetivos, ampliar el crecimiento de las empresas tecnológicas chinas —como Alibaba, Tencent y Huawei[76]— a los mercados extranjeros. Para expandirse, estas compañías también recurren a menudo a la adquisición de empresas extranjeras, como en el caso de los Estados Unidos. El país también busca aumentar la inversión china en infraestructuras digitales y de telecomunicaciones —tales como zonas de comercio digital y proyectos de ciudades inteligentes— en países extranjeros (Triolo y otros, 2020)[77].

El éxito de los proyectos llevados a cabo en el marco de la Ruta de la Seda Digital depende de la adopción generalizada de tecnologías y servicios chinos impulsados por los datos en los países participantes en la Iniciativa de la Franja y la Ruta y de la interconectividad entre China y esos países, para lo cual se requiere que los datos circulen entre ellos. Según Erie y Streinz (2021), China modela la gobernanza transnacional en materia de datos suministrando infraestructuras digitales a los mercados emergentes a través de la Ruta de la Seda Digital, en lo que denominan el "efecto Beijing". En términos económicos, estas inversiones también conllevan para los países en desarrollo beneficios —de desarrollo y de otros tipos (Arcesati, 2020; Gong, Gu y Teng, 2019)—, así como costos ligados a la pérdida de control de sus datos en favor de un país extranjero. Además, se añade una dimensión política al enfoque chino, ya que se teme que las tecnologías chinas puedan contribuir a la vigilancia del Estado a la población de los países en desarrollo (Kurlantzick, 2020; CFR, 2020).

A diferencia de las estrategias de expansión mundial de los Estados Unidos y China, que se basan en su liderazgo tecnológico, la Unión Europea se apoya principalmente en su liderazgo normativo. A este respecto, el RGPD podría estar convirtiéndose en un modelo mundial en cuanto a la protección de los datos (recuadro IV.3).

Según especialistas en la materia, a través del RGPD, la Unión Europea pretende exportar sus normas de privacidad al extranjero y erigirse en "referente en materia de regulación" a nivel mundial (Ciuriak y Ptashkina, 2018), en lo que se ha denominado "efecto Bruselas". A este respecto, cabe citar el ejemplo de

[75] Véase Facebook, "Building a transformative subsea cable to better connect Africa", disponible en https://engineering.fb.com/2020/05/13/connectivity/2africa/.

[76] Por ejemplo, se ha informado de que Huawei ha instalado más del 70 % de las redes 4G en África (véase The Africa Report, "Huawei's African business could be hurt by US blacklisting", 22 de mayo de 2019).

[77] Véase *Nikkei Asia*, 24 de noviembre de 2020, "China Rises as World's Data Superpower as Internet Fractures", disponible en https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-Internet-fractures?utm_ source=CSIS+All&utm_campaign%E2%80%A6; George Magnus, "Will digital diplomacy cement the Belt and Road Initiative's 'common destiny'?", 17 de septiembre de 2020, disponible en https://blogs.lse.ac.uk/cff/2020/09/17/will-digitaldiplomacy-cement-the-belt-and-road-initiatives-common-destiny/; Robert Greene y Paul Triolo, "Will China Control the Global Internet Via its Digital Silk Road?", 8 de mayo de 2020, disponible en https://carnegieendowment.org/2020/05/08/willchina-control-global-Internet-via-its-digital-silk-road-pub-81857. Para más información reciente y detallada sobre la Ruta de la Seda Digital, véase Ly (2020); CFR (2020); Dekker, Okano-Heijmans y Zhang (2020); y Eder, Arcesati y Mardell (2020).

Recuadro IV.3. ¿El RGPD como estándar mundial de protección de datos?

El RGPD está extendiendo su alcance global por varias vías. En primer lugar, para cumplir con el RGPD, varias empresas han realizado cambios significativos en sus modelos globales de negocio y de tratamiento de datos y, en consecuencia, ofrecen dichas protecciones de privacidad en todo el mundo (Chakravorti, 2018). En segundo lugar, el carácter integral del RGPD se ha convertido en un modelo para varios países en desarrollo que han aprobado recientemente leyes de protección de datos o están elaborándolas. En 2018, de 120 países no pertenecientes a la Unión Europea, 67 habían aprobado leyes similares al RGPD (Srikrishna Committee Report, 2018). En tercer lugar, además de lograr los niveles deseados de protección de datos, varios países en los que se han aprobado leyes similares al RGPD esperan recibir de la Comisión Europea una decisión de adecuación en el futuro, lo que podría facilitar el acceso de sus empresas nacionales a los mercados europeos (Christakis, 2020). Sin embargo, la aplicación de normas similares a las del RGPD requiere importantes recursos reguladores, lo que podría ser complicado en muchos países en desarrollo (Chakravorti, 2018). Además, las normativas similares al RGPD sobre la transferencia de datos imponen a las empresas altos costos de cumplimiento que podrían estar fuera del alcance, sobre todo, de las microempresas y pequeñas y medianas empresas (mipymes) de los países en desarrollo. De hecho, se ha afirmado que el RGPD no resulta adecuado para los países de ingreso bajo, debido a su complejidad (Pisa y otros, 2020).

En el caso de América Latina, por ejemplo, la directiva europea de 1995 relativa a la protección de datos ya había llevado a algunos países a obtener una decisión de adecuación para intercambiar flujos de datos. Pero la dinámica que condujo a la implementación del RGPD sirvió para catalizar los debates y reevaluar el nivel actual de adecuación en materia de protección, a la luz de la omnipresencia de las tecnologías de comunicación digital que conectaban a más sectores productivos, así como de la tendencia a revisar la forma en que se recopilan y procesan los datos que surgió en 2013 tras las declaraciones de Edward Snowden (ECLAC e I&JPN, 2020). La implementación del RGPD ha propiciado más adaptaciones que aún están estudiando muchas jurisdicciones de la región. Actualmente, tres Estados de la región (Argentina, México y Uruguay) han recibido una decisión de adecuación al RGPD, mientras que en el caso de los territorios del Caribe, Guadalupe y Martinica también entran dentro del ámbito del RGPD (Bleeker, 2020). En el RGPD se han inspirado las leyes del Brasil, Panamá y Barbados que han sido aprobadas recientemente y con las que se pretende conseguir una pronta adecuación a dicha normativa (Rodríguez y Alimonti, 2020).

Fuente: UNCTAD.

la reciente propuesta europea relativa a un marco jurídico sobre la IA (que está estrechamente vinculada a los datos), cuyo objetivo es "proporcionar a Europa un papel protagonista en el establecimiento de los estándares de referencia a nivel mundial"[78].

La Unión Europea también está forjando alianzas con países en desarrollo. Un ejemplo es la Alianza de Economía Digital África-Europa. De hecho, en el contexto de las asociaciones internacionales para la década digital, en los objetivos digitales para 2030 se incluye que "la UE promoverá su agenda digital centrada en el ser humano en la escena mundial y promoverá la armonización o la convergencia con las normas y los estándares de la UE"[79]. Esto implica que, una vez que las normativas converjan con las de la Unión Europea, será posible la libre transmisión de datos entre la Unión Europea y los países correspondientes.

[78] Véase Bradford (2020) y The Brussels Effect, 2How the European Union rules the world2, disponible en www.brusselseffect.com/; Comisión Europea, "A European approach to Artificial intelligence", disponible en https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence; y *The Economist*, 24 de abril de 2021, "The EU wants to become world's super-regulator in AI".

[79] Véase Comisión Europea, "Africa–Europe Alliance: European Commission and African Union Commission welcome the Digital Economy Task Force report", disponible en https://digital-strategy.ec.europa.eu/en/news/africa-europe-allianceeuropean-commission-and-african-union-commission-welcome-digital-economy; y Comisión Europea, "La Década Digital de Europa: metas digitales para 2030", disponible en https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es.

Cualquiera que sea la estrategia de expansión global, corresponde a los países en desarrollo evaluar los beneficios netos que una u otra puede en último término aportar en el ámbito del desarrollo. A tal efecto, deberían sopesar los efectos positivos (las mejoras en infraestructura y conectividad y en sus normativas sobre datos) con los costos de ceder sus datos a entidades situadas en países extranjeros, con la consiguiente pérdida de capacidad para extraer valor de esos datos.

D. RIESGOS Y REPERCUSIONES DE UNA POSIBLE FRAGMENTACIÓN DEL ESPACIO DIGITAL

1. ¿Fragmentación o convergencia?

Los análisis presentados en las secciones precedentes muestran que los enfoques mundiales predominantes y más influyentes en lo que respecta a la economía digital y a la gobernanza de los datos difieren bastante entre sí, como también lo hace su influencia a nivel global. Las políticas sobre los flujos de datos transfronterizos varían según las concepciones y los valores económicos, sociales, políticos, institucionales y culturales. Lo más destacable es que el "modelo de cibersoberanía" defendido por China y la Federación de Rusia contrasta notablemente con el planteamiento de "libre circulación de la información" por el que abogan los Estados Unidos. Además, el modelo de soberanía digital de la Unión Europea no está alineado con el planteamiento de los Estados Unidos en materia de gobernanza de los datos. Por último, economías emergentes en desarrollo como la India favorecen modelos de desarrollo económico digital y de regulación de los flujos de datos basados en la localización de los datos dentro de las fronteras nacionales, en discrepancia con la libre circulación de la información y distintos del modelo de regulación chino o europeo.

Estas diferencias han despertado inquietudes ante la posibilidad de fragmentación de Internet y de la economía digital impulsada por los datos. Por ejemplo, uno de los principales riesgos mundiales que se destacaron en 2020 (WEF, 2020c) era la fragmentación de la economía digital. Respecto de la fragmentación de Internet existen muchos planteamientos interrelacionados. Drake, Cerf y Kleinwächter (2016) desarrollaron un enfoque heurístico en el que describieron las fuerzas que conducen a una fragmentación de Internet desde una perspectiva política, comercial y técnica. Según estos autores, la fragmentación política incluye cuestiones como la cibersoberanía, la soberanía nacional y el ciberespacio, la venta en línea y el comercio, el contenido y la censura, la seguridad nacional, la localización de los datos y la privacidad, y la protección de los datos. La fragmentación comercial se debe a los procedimientos de *peering* (intercambio de tráfico) y estandarización, la no protección de la neutralidad de la red, los enfoques de compartimentos estancos, los mecanismos de geolocalización y geobloqueo, y la aplicación de los derechos de propiedad intelectual. La fragmentación técnica ocurre al manipular los servidores de nombre de dominio (DNS) y las direcciones IP, elementos que se consideran recursos críticos de Internet. De Nardis (2016), por su parte, ha clasificado los enfoques de la fragmentación de Internet considerando los estratos de infraestructura, lógica y contenido. Si bien estos diferentes enfoques y estratos podían estar bastante separados en los primeros tiempos de Internet, con la creciente digitalización de cada vez más actividades y áreas de la vida, la economía y la sociedad, y el aumento de la interconexión, la separación entre ellos se ha vuelto cada vez más tenue. Esto también obedece a que las principales plataformas digitales globales pueden desempeñar un papel prominente en todo el espacio digital y de Internet, incluidas las infraestructuras de red (capítulo I). Por lo tanto, la fragmentación de Internet y la de la economía digital se estarían fusionando en un proceso único.

El impacto de las diferencias en los modelos de Internet, las tecnologías digitales y la gobernanza de los datos queda patente en las tensiones geopolíticas a nivel internacional. Las más notables son las actuales tiranteces tecnológicas y comerciales entre los Estados Unidos y China. Mientras que China ha adoptado históricamente un enfoque restrictivo y ha prohibido varios servicios basados en los Estados Unidos, y en su lugar ha promovido plataformas y servicios digitales nacionales, los Estados Unidos han comenzado a adoptar una postura más agresiva hacia las empresas tecnológicas chinas en los últimos años. El programa Red Limpia, al que ya se ha hecho referencia, es un ejemplo de ello. Ciertas voces han señalado que este programa, destinado a eliminar las aplicaciones y servicios chinos no fiables de la

red en los Estados Unidos y a reducir la presencia china en las redes de telecomunicaciones y los cables submarinos estadounidenses, contribuirá en última instancia a la fragmentación de Internet[80].

El reciente conjunto de medidas aprobadas por la Federación de Rusia para desconectarse de la red mundial también pone de manifiesto la creciente fragmentación de Internet[81]. Otro ejemplo es la prohibición de las aplicaciones chinas en la India. Por último, aunque la Unión Europea ha seguido siendo partidaria de una Internet libre y abierta, la aplicación altamente prescriptiva de las normas del RGPD a la transferencia transfronteriza de datos personales (por ejemplo, en el asunto *Schrems II*) y la afirmación de la soberanía digital para salvaguardar el margen de actuación de los Gobiernos europeos para proteger los valores de la UE (por ejemplo, la Ley de Gobernanza de Datos y la iniciativa GAIA-X) también pueden considerarse una amenaza potencial para un ecosistema de comercio digital integrado.

Estas tensiones, especialmente entre los Estados Unidos y China, tienen como origen la búsqueda del liderazgo o la supremacía en el ámbito digital y tecnológico a nivel mundial, y su objetivo es establecer normas globales. Dado que el control de los datos y de las tecnologías de IA permite cada vez más el dominio de la economía y la sociedad, se trata básicamente de una cuestión de poder económico y político a escala mundial. Sin embargo, aunque en términos de ganadores y perdedores podría haber un vencedor en dicha "carrera", es muy poco probable que esto beneficie a la población del planeta en general. Es probable que, desde una perspectiva global, una solución cooperativa produzca mejores resultados.

Aunque la diversidad de enfoques a nivel nacional indica que la fragmentación no deja de ser plausible, como se ha indicado, puede observarse cierta convergencia si se adopta una perspectiva dinámica de los diferentes enfoques. Como se analizará más pormenorizadamente en el capítulo V, si se examinan las normativas específicas sobre los flujos de datos transfronterizos, todos los países tienden a fijarse como objetivos principales el crecimiento económico y el desarrollo, la privacidad y la protección de datos y la seguridad nacional. Lo que cambia es la prioridad que se concede a cada uno de esos tres objetivos y la manera en que se aplica la normativa. En el caso de los Estados Unidos, a pesar de su enfoque de libre mercado, el país está evolucionando hacia planteamientos más defensivos, como se ha explicado anteriormente; China está insinuando cierta apertura de sus flujos de datos; y los intereses inicialmente protectores de la Unión Europea están mudando hacia políticas industriales parecidas a las de China. Así pues, los respectivos enfoques parecen apuntar a una moderación de las posiciones y a un ligero ajuste de rumbo hacia planteamientos más equilibrados, lo que podría posibilitar el encontrar áreas básicas de entendimiento entre los principales actores.

En última instancia, no se puede decir a ciencia cierta si se llegará a fragmentar Internet y la economía digital, lo cual dependerá en gran medida de la voluntad que muestren los responsables políticos de todo el mundo de encontrar una solución global que beneficie a todos. Un enfoque dividido de la gobernanza de los datos podría abocar al mundo a un "nacionalismo de datos divergente", en el que los países aprobarían políticas nacionales de datos sin consensuarlas en el plano internacional, lo que daría lugar a una reducción de las oportunidades de innovación y desarrollo digitales en todo el mundo (Government Office for Science (Reino Unido), 2020). Es probable que esta fragmentación dé lugar a un resultado subóptimo, en el que no será posible que se materialicen los beneficios potenciales de la economía impulsada por los datos, que se basan sobre todo en su circulación.

2. Impacto de la fragmentación en los países en desarrollo

La posible fragmentación de la economía digital impulsada por los datos podría crear dificultades para el progreso tecnológico, a raíz de una menor competencia, estructuras de mercado oligopolistas en distintos ámbitos y una mayor influencia del Estado. De producirse dicha fragmentación se reducirían las oportunidades de negocio, ya que el acceso de los usuarios y las empresas a las cadenas de suministro

[80] Véase, por ejemplo, *Forbes*, 17 de septiembre de 2020, "CFIUS and a Tale of Two Internets", disponible en www.forbes.com/sites/riskmap/2020/09/17/cfius-and-a-tale-of-two-Internets/?sh=5c37db2439fb.

[81] Véase Internet Governance Project, 16 de mayo de 2019, "A closer look at the 'sovereign Runet' law", disponible en www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/; y *Wired*, 6 de junio de 2019, "Russia and Iran Plan to Fundamentally Isolate the Internet".

sería más complicado y se restringiría la circulación de los datos entre países diferentes. Además, habría más obstáculos para la colaboración entre jurisdicciones, que sería menos fiable (Feijóo y otros, 2020).

Cada una de las tres potencias en materia de datos —Estados Unidos, China y Unión Europea— han creado reinos diferenciados de datos, lo que crea problemas de compatibilidad o interoperabilidad entre ellos y obstaculiza gravemente la capacidad de concebir normas mundiales que regulen los flujos de datos transfronterizos y, por tanto, creen condiciones de igualdad para todos los países. Para los países que se encuentran fuera de estos "reinos de datos" dominantes (salvo algunas excepciones, como la India y la Federación de Rusia), esto significa que, en cuanto actores que han de acatar las normas impuestas por terceros, probablemente tendrán que elegir cuál de los modelos de gobernanza de datos seguir si la divergencia sigue creciendo (Aaronson y Leblond, 2018).

Para mejorar su acceso a los datos y su dominio del mercado, los Estados Unidos, China y la Unión Europea intentan atraer a otros países a su reino mediante acuerdos comerciales y actividades de fomento de la capacidad, o a cambio de acceso al mercado. En muchos casos, las autoridades de los países más pequeños o menos avanzados se sentirán obligadas a elegir un reino en lugar de los otros porque ya tienen relaciones comerciales importantes con ese mercado o porque están a favor del enfoque de ese reino en lo que respecta a la gobernanza de los datos. Sin embargo, a muchos países les resultará difícil, si no imposible, elegir, ya que mantienen importantes relaciones económicas con más de un reino. En consecuencia, los Gobiernos de esos países intentarán retrasar lo máximo posible su alineación con un reino concreto, lo que hará que los países en desarrollo se vean en la incómoda posición de tener que adoptar decisiones que afectarán a otras relaciones económicas.

Por ejemplo, los países latinoamericanos a menudo tienen que elegir entre el modelo del RGPD y el planteamiento de los Estados Unidos con respecto a la regulación de los flujos de datos transfronterizos y las normas de protección de datos. Dado que hay intereses económicos que los unen a ambos bloques, la mayoría de los países latinoamericanos se enfrentan a una difícil elección (Aguerre, 2019). Varios países de África parecen alinearse ahora con el modelo chino de cibersoberanía[82], pero también tienen vínculos con la Unión Europea y los Estados Unidos. China ejerce una mayor influencia en numerosos países en desarrollo de Asia. Los Estados Unidos han alentado a sus aliados tradicionales a adoptar una postura dura contra las empresas chinas, por ejemplo excluyendo a Huawei de sus redes de telecomunicaciones y prohibiendo aplicaciones de medios sociales como TikTok[83].

En términos de infraestructura, el menor número de puntos de interconexión a la red global que resultaría de la fragmentación de Internet supondría un aumento de los costos y una menor eficiencia en términos generales. Además, esa fragmentación llevaría a una menor capacidad de beneficiarse de los efectos de red que generan las dinámicas de una interconexión relativamente global. En numerosos países en desarrollo, dado el alto grado de interconexión e interdependencia respecto de los proveedores de contenidos y servicios globales, la fragmentación de los servicios de Internet tendría considerables consecuencias para las empresas y los usuarios locales.

El "nacionalismo de datos" divergente será especialmente perjudicial para los intereses de los países en desarrollo, incluidos los PMA. En primer lugar, dará lugar a normativas nacionales subóptimas, especialmente en los países en desarrollo con poca capacidad reguladora, lo que tendrá consecuencias adversas para la privacidad y la seguridad, y perjudicará los intereses de los usuarios nacionales de Internet, como se verá en el siguiente capítulo. En segundo lugar, una Internet fragmentada reduciría las oportunidades de mercado de las mipymes nacionales para llegar a los mercados mundiales, con lo que tendrían que limitarse a ciertos mercados nacionales o regionales. En tercer lugar, el nacionalismo de datos divergente reduce las oportunidades de innovación digital, entre ellas las relativas al desarrollo inclusivo propiciado por la participación en el intercambio de datos a través de una cooperación internacional fluida. Por último, en un mundo caracterizado por el nacionalismo de datos divergente habría un reducido número de vencedores y muchos perdedores. Algunas economías digitales consolidadas saldrían ganando debido al ventajoso tamaño de sus mercados y a sus competencias tecnológicas, pero la

[82] *The Diplomat*, 23 de febrero de 2019, "How China Exports Repression to Africa".

[83] Véase, por ejemplo, Rodrik (2020); y *The Guardian*, 13 de julio de 2020, "Europe divided on Huawei as US pressure to drop company grows".

mayoría de las economías pequeñas y las economías en desarrollo perderían oportunidades de aumentar su competitividad en el ámbito digital.

Sin embargo, mientras no exista un sistema internacional de regulación apropiada de los flujos de datos transfronterizos que permita maximizar los beneficios derivados de los datos y que al mismo tiempo aborde los riesgos conexos —de manera que el aumento de ingresos se distribuya equitativamente—, la única opción para los países en desarrollo es regular sus flujos de datos a nivel nacional. En el siguiente capítulo se exploran con cierto detalle determinadas políticas sobre los flujos de datos transfronterizos, con el fin de presentar un panorama de las diferentes medidas nacionales que los países pueden adoptar para regular los flujos de datos transfronterizos.

En este capítulo se traza un esquema de las políticas de regulación de los flujos de datos transfronterizos vigentes en todo el mundo. Las normativas nacionales en esta esfera varían considerablemente y pueden situarse en diferentes puntos de un espectro regulador que va desde la localización estricta de los datos hasta la circulación prácticamente libre de estos. El enfoque adoptado tiende a ser un reflejo de las diferentes condiciones tecnológicas, económicas, sociales, políticas, institucionales y culturales que existen en los países.

La regulación de los flujos de datos transfronterizos responde a diversos motivos de política pública, como los relacionados con la protección de la privacidad y otros derechos humanos, la aplicación de la ley y la seguridad nacional, así como a objetivos de desarrollo económico. Los países se sirven de una amplia gama de instrumentos jurídicos y normativos. Por lo tanto, la elección del modelo adecuado para regular los flujos de datos en cada país sigue siendo una decisión política difícil. Para que las economías en desarrollo puedan aprovechar al máximo los beneficios potenciales de la economía digital y garantizar un mayor grado de bienestar a su ciudadanía, resulta especialmente importante realizar un ejercicio de equilibrio integrador que permita obtener diferentes resultados reguladores a partir de la interacción compleja entre los factores nacionales e internacionales.

ESQUEMA DE LAS POLÍTICAS NACIONALES SOBRE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

V

CAPÍTULO V NO EXISTE UN ENFOQUE UNIVERSAL PARA LA REGULACIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Condiciones que determinan los enfoques nacionales en materia de gobernanza de los datos y los flujos de datos

Tecnológicas
Políticas
Culturales
Sociales
Institucionales
Económicas

Razones de política pública para regular los flujos de datos transfronterizos

- Objetivos de desarrollo económico
- Protección de la privacidad y otros derechos humanos
- Aplicación de la ley
- Seguridad nacional

Los instrumentos jurídicos que regulan los flujos de datos transfronterizos pueden hacer referencia a los siguientes aspectos:

- Protección de datos
- Ciberseguridad
- *Hardware* y *software*
- Contratación pública
- Acuerdos comerciales
- Secretos de Estado
- Tributación
- Contabilidad

Espectro regulador de los flujos de datos transfronterizos

Localización de los datos estricta	Localización de los datos parcial	Transferencia condicionada: estricta	Transferencia condicionada: intermedia/flexible	Libre circulación de los datos
Enfoque restrictivo o cauteloso		Enfoque prescriptivo		Enfoque de baja injerencia

Los países en desarrollo deben encontrar el equilibrio óptimo entre la promoción del desarrollo económico nacional, la protección de los intereses de las políticas públicas y la integración en la economía digital mundial

A. INTRODUCCIÓN

La rápida digitalización de la economía y la "datificación" de la sociedad han llevado a los Gobiernos de todo el mundo a adoptar una gran variedad de instrumentos normativos en relación con los flujos de datos transfronterizos. Tomando como base el panorama de las principales tendencias en materia de gobernanza de los datos a escala mundial que se presenta en el capítulo IV, en particular las que afectan a los flujos de datos transfronterizos, en este capítulo se analizan las medidas específicas adoptadas en diferentes países para regular esta cuestión. La muestra de países examinados no es exhaustiva, ya que, por ejemplo, es posible que en algunos países, especialmente PMA, no se haya aprobado este tipo de normativa. No obstante, la selección es representativa de la variedad de medidas y motivaciones de los diferentes países (con condiciones tecnológicas, económicas, políticas, institucionales y culturales diversas) para regular estos flujos, así como de la posición que ocupan en el espectro normativo.

Mientras que algunos países restringen de manera estricta los flujos de datos transfronterizos, otros han adoptado marcos de cumplimiento más matizados para regular la transferencia de datos a través de sus fronteras. Estas normativas pueden ser específicas para un sector o una categoría de datos, o aplicarse más en general a diversos sectores de la economía y diferentes categorías de datos. En el presente capítulo se examinan los diversos marcos reguladores clasificando las normativas nacionales sobre datos transfronterizos según diferentes criterios, y evaluando a continuación sus ventajas e inconvenientes. También se aporta un esquema de las normativas nacionales en esta esfera.

En función de los valores políticos, económicos, sociales, tecnológicos y culturales de los distintos países, así como de su contexto ideológico, los motivos para regular los flujos de datos transfronterizos pueden ser distintos o solaparse. Entre los principales objetivos políticos están los siguientes: promover el crecimiento económico del país; obtener los máximos beneficios socioeconómicos de las tecnologías impulsadas por los datos; generar confianza en la economía digital nacional; abordar problemas importantes de política pública, como las vulneraciones del derecho a la privacidad y la vigilancia; reducir al mínimo las ciberamenazas (especialmente las que afectan a las infraestructuras críticas); y construir una ciberinfraestructura resiliente y segura. Además, algunos Gobiernos tratan de garantizar el acceso oportuno a los datos de sus órganos de supervisión reglamentaria y sus fuerzas del orden mediante la imposición de medidas de localización de los datos. Por último, varios países consideran que sus normativas nacionales sobre los flujos de datos transfronterizos son herramientas esenciales para establecer y mantener su "soberanía sobre los datos" o "cibersoberanía", es decir, el control soberano sobre el uso de Internet y los flujos de datos a nivel nacional. No obstante, las normativas destinadas a aumentar el control soberano sobre Internet a nivel nacional también pueden utilizarse para reforzar la vigilancia de los usuarios de Internet por el Estado en el territorio nacional. En el recuadro V.1 se definen diferentes conceptos importantes en el marco de estas normativas.

La creación de marcos reguladores sólidos, equilibrados y pertinentes sobre los flujos de datos transfronterizos es uno de los desafíos normativos más importantes de la economía digital. Los Gobiernos deben evaluar los beneficios y riesgos que pueden conllevar para su país los flujos de datos transfronterizos, tanto a nivel social como individual. Por ejemplo, los flujos de datos transfronterizos pueden beneficiar a las sociedades reforzando el ejercicio efectivo de ciertos derechos humanos, proporcionando a las personas una mayor oferta de servicios en línea competitivos y permitiendo a las empresas tomar decisiones económicamente eficientes (Kuner, 2013; WEF, 2020b; Freedom House, 2020). Asimismo, los Gobiernos deben hacer frente a las amenazas críticas que afectan a los datos, en particular los riesgos para la privacidad y la ciberseguridad. Además, el "potencial inherente de fallos del mercado" que caracteriza a los sectores impulsados por los datos —en particular "las externalidades de red, las economías de escala y alcance, y la asimetría de información generalizada" (Chen y otros, 2019:6; Ciuriak, 2019, 2020)— plantea problemas normativos muy complejos en relación con la regulación de los datos. Los Gobiernos también deben garantizar un acceso equitativo a los datos, ya que constituyen un "capital social esencial" para las tecnologías digitales emergentes, como la inteligencia artificial (IA) y la Internet de las cosas (Ciuriak y Ptashkina, 2018). Esto constituye un desafío especialmente importante para los PMA que cuentan con una infraestructura digital deficiente, escasas capacidades digitales y una capacidad reguladora limitada.

Recuadro V.1. Conceptos relacionados con las políticas nacionales sobre los flujos de datos transfronterizos

En los modelos normativos sobre gobernanza de los datos suelen emplearse determinados conceptos y términos comunes. A continuación se aporta una explicación de esos términos formulada en un lenguaje sencillo:

- Por *localización de los datos* se entiende el requisito de utilizar servidores locales para almacenar o procesar los datos. La localización de los datos también suele denominarse "residencia de datos".
- Por *cibersoberanía* se entiende, en general, el control que ejercen los Estados sobre diversos aspectos de Internet y de las actividades relacionadas con Internet —incluidos los contenidos digitales, la infraestructura digital y los servicios digitales— dentro de sus fronteras. A diferencia de los modelos de gobernanza de Internet en los que participan múltiples partes, la cibersoberanía sitúa al Estado en el centro de la gobernanza de Internet.
- Por *soberanía sobre los datos o sobre la información* se entiende el control por los Estados de la totalidad de los flujos de datos que circulan a través de Internet (es decir, tanto dentro de su territorio como hacia y desde él) para garantizar, entre otras cosas, que todos los datos generados y procesados dentro del Estado estén sujetos a las leyes nacionales y puedan ser utilizados de la manera que el Estado considere oportuna.
- Por *proteccionismo de datos* se entiende la regulación de los flujos de datos por los Estados con el objetivo de crear ventajas competitivas para el sector nacional, aun cuando repercuta negativamente a la competencia en condiciones de igualdad con los actores extranjeros.
- El *nacionalismo de datos* hace referencia a las políticas que tienen por objetivo garantizar que los datos nacionales se utilicen principalmente en beneficio de los intereses nacionales.

Fuente: UNCTAD.

En la sección B de este capítulo se clasifican las normativas sobre los flujos de datos transfronterizos conforme a diversos criterios, en particular el tipo de datos que regulan, los sectores a los que afectan y su grado de restricción. A continuación se analizan ejemplos de cada una de las categorías en un gran número de países, y en concreto se señalan las razones políticas que justifican la regulación y los riesgos que se pueden plantear desde el punto de vista de la eficacia normativa, el desarrollo económico y la gobernanza mundial de los datos. En la sección C se describen los marcos reguladores nacionales sobre los flujos de datos transfronterizos a lo largo de un espectro normativo, en función de su grado de restricción —desde los que adoptan un enfoque "de baja injerencia" a un enfoque "prescriptivo", "restrictivo" o "cauteloso"— y, a continuación, se explican las tendencias existentes. Por último, en la sección D se presentan algunas conclusiones.

B. MEDIDAS NACIONALES SOBRE LOS FLUJOS DE DATOS TRANSFRONTERIZOS Y SUS IMPLICACIONES POLÍTICAS

Partiendo de un análisis de las normativas sobre los flujos de datos transfronterizos[1], en esta sección se examinan, en primer lugar, las diversas razones que llevan a la regulación de los flujos de datos transfronterizos desde tres perspectivas distintas —la política de protección de la ciudadanía, la seguridad nacional y el desarrollo económico—, que abarcan diversos objetivos reguladores, como la protección de

[1] Al seleccionar la muestra de países para el examen, se han tenido en cuenta diversos factores con el objetivo de garantizar que resultase representativa: geografía/ubicación del país, nivel de desarrollo del país, tipo de regulación de los datos, motivos para la regulación y accesibilidad de la información. También se realizó una revisión exhaustiva de las fuentes bibliográficas y, a continuación, se comprobó la exactitud de las referencias a las leyes y políticas pertinentes. La lista de los textos normativos examinados figura en el anexo en línea del capítulo V (disponible en https://unctad.org/system/files/official-document/der2021_ annex2_en.pdf). Como se indica en el capítulo IV, el Informe refleja la situación que existía a principios de 2021.

datos, la ciberseguridad, la protección de los secretos de Estado, la salvaguardia de los datos públicos/del Estado frente a la vigilancia extranjera, la garantía del acceso a los datos por los órganos reguladores y las fuerzas del orden y la facilitación del desarrollo del sector digital nacional. A continuación se proponen diferentes formas de clasificar dichas normativas, utilizando ejemplos de diversos países. Por último, se analizan las consecuencias de la normativa sobre los flujos de datos transfronterizos para las políticas nacionales desde diferentes perspectivas y se expone la diversidad y la complejidad de las decisiones políticas relacionadas con la adopción de un marco de gobernanza de los flujos de datos transfronterizos.

1. Razones políticas que justifican la regulación de los flujos de datos transfronterizos

En esta sección se exponen las diferentes razones políticas que llevan a los Gobiernos a regular los flujos de datos transfronterizos, a fin de aportar una visión general de las consideraciones geopolíticas y sociopolíticas que influyen actualmente en la forma en que los países abordan esta cuestión. Para facilitar una visión más sistemática, se examinan las razones políticas subyacentes desde tres perspectivas distintas: a) la política de protección de la ciudadanía, b) la seguridad nacional y c) el desarrollo económico. En la práctica, el marco regulador de los flujos de datos transfronterizos de un país puede basarse en razones políticas que implican una superposición de esas perspectivas.

a) Perspectiva de la política de protección de la ciudadanía

Con frecuencia, la regulación de los flujos de datos transfronterizos responde a objetivos del Estado relacionados con la protección de los intereses de la ciudadanía, como la privacidad y la protección de datos, la ciberseguridad, la supervisión reguladora reforzada y la aplicación de la ley. Muchos países restringen o regulan los flujos de datos transfronterizos para garantizar el cumplimiento de sus leyes nacionales de protección de datos. En la práctica, son muy pocos los países que restringen expresamente la transferencia transfronteriza de datos no personales, a menos que dichos datos afecten a sectores especialmente sensibles. Si bien los conjuntos de datos anónimos transferidos en el marco de las transacciones digitales se consideran datos no personales, varias leyes nacionales incluyen en la definición de datos personales cualquier información relativa a una persona "identificable" (por ejemplo el Reglamento General de Protección de Datos (RGPD), artículo 4, párr. 1). Las herramientas de análisis de datos han facilitado la desanonimización de los individuos en estos conjuntos de datos (Ohm, 2010); por lo tanto, el alcance de los datos personales puede ser amplio.

Normalmente, las restricciones a la transferencia transfronteriza de datos personales están motivadas por dos objetivos: a) garantizar que las empresas (extranjeras o nacionales) que tratan con datos personales de la ciudadanía no puedan eludir las obligaciones previstas en las leyes nacionales de protección de datos, por ejemplo, transfiriendo los datos a países con leyes más permisivas (Bygrave, 2002; Kuner, 2013); y b) proteger el derecho a la privacidad de los particulares (incluidos sus derechos constitucionales, cuando proceda) y proporcionarles recursos adecuados en caso de que se vulneren sus derechos como consumidores, lo que incluye las situaciones en que sufran pérdidas económicas y se cometan vulneraciones en masa de la privacidad. Este último objetivo es especialmente crucial para sectores sensibles como el sanitario y el financiero; por ello, varios países imponen requisitos de localización o transferencia condicionada en estos sectores.

Algunos países —como China, Viet Nam, Indonesia, Arabia Saudita y Turquía— exigen la localización de los datos relacionados con sectores de infraestructuras críticas o, con carácter más general, de los datos del Estado. Dada la importancia de la seguridad de los datos del Estado y de las infraestructuras críticas, y su creciente dependencia de las redes informáticas, estos Gobiernos prefieren el almacenamiento local de los datos para garantizar el mayor grado de seguridad de los mismos y la resiliencia de sus infraestructuras nacionales. De hecho, a medida que van creciendo las tecnologías impulsadas por los datos, especialmente en el contexto de la Internet de las cosas y la IA, se espera que varios países introduzcan también restricciones estrictas a la transferencia de datos en sus leyes y políticas de ciberseguridad a fin de proteger la seguridad de los datos[2].

[2] Véanse, por ejemplo, los Controles Esenciales de Ciberseguridad (Arabia Saudita).

Hasta cierto punto, no es extraño que exista un temor a las consecuencias que puedan tener las tecnologías basadas en la Internet de las cosas y la IA para la seguridad, puesto que estas tecnologías están todavía en ciernes; son muy susceptibles a las ciberamenazas; y afectan drásticamente a varios sectores —como las comunicaciones, el transporte y las finanzas— que muchos países consideran, con acierto, sensibles (Ciuriak, 2019). No obstante, conviene distinguir entre las normativas destinadas a abordar preocupaciones relacionadas con la seguridad técnica de las tecnologías digitales (por ejemplo, para proteger las redes frente a las ciberamenazas o garantizar la integridad de las redes, que puede referirse a amenazas comerciales corrientes o a amenazas más graves para las ciberinfrastructuras críticas) y las que abordan preocupaciones políticas y de seguridad nacional más amplias, incluidas las relacionadas con la seguridad nacional y la soberanía económica, como se explica a continuación. Aunque existe cierto solapamiento entre las preocupaciones relativas a la seguridad técnica y las relacionadas con la seguridad nacional (por ejemplo, las ciberamenazas a las infraestructuras críticas o de defensa también son preocupaciones legítimas desde la perspectiva de la seguridad nacional), la seguridad nacional puede entenderse como un concepto más amplio que incluye ideas de estabilidad social, seguridad económica y autosuficiencia, así como de control político sobre los usuarios nacionales (Mishra, 2020a; Tomiura y otros, 2019).

Además, varios países imponen restricciones a los flujos de datos transfronterizos —como requisitos explícitos de localización (estricta o parcial) en sectores sensibles— para garantizar un acceso inmediato y previsible a los datos siempre que lo necesiten sus órganos de supervisión reglamentaria o sus fuerzas del orden. Un problema al que se enfrentan a menudo muchos organismos encargados de hacer cumplir la ley en todo el mundo es el de obtener acceso inmediato a los datos almacenados en jurisdicciones extranjeras, dado el engorroso proceso necesario para acceder a los datos almacenados en otros países[3]. La Ley CLOUD de los Estados Unidos (véase el capítulo IV) ilustra los problemas que se plantean cuando los datos se encuentran en jurisdicciones extranjeras. Se ha señalado también en la literatura especializada que las medidas de localización de los datos pueden ser necesarias para "aumentar la eficacia de las fuerzas del orden" y "conceder a los Estados un mayor control jurisdiccional sobre los datos" (Sargsyan, 2016:2223). Además, puede preocupar a los Estados que los datos personales de su ciudadanía queden sujetos a leyes de jurisdicciones extranjeras que no proporcionan el mismo nivel de protección que el que conceden a los usuarios de esos países. Por ejemplo, en su estrategia de transformación digital, los miembros de la Unión Africana establecieron el objetivo de adoptar leyes nacionales sobre localización de los datos para proteger la privacidad de su ciudadanía y sus residentes (African Union, 2020). Los países de América Latina no imponen requisitos de presencia local, pero las fuerzas del orden nacionales, especialmente en el caso del Brasil en los últimos años, son cada vez más favorables a este enfoque. No obstante, esta tendencia suele referirse a la ubicación de la conducta más que a la ubicación donde se almacenan los datos (ECLAC e I&JPN, 2020).

b) Perspectiva de la seguridad/soberanía nacional

Varias normativas relativas a los flujos de datos transfronterizos pueden examinarse desde el punto de vista de la seguridad y la soberanía nacionales. A medida que las tecnologías de datos se generalizan y se integran en diversas esferas de la vida, muchos Gobiernos muestran un interés creciente por los datos como activo estratégico. El control de los flujos de datos por un país puede ser parte importante de sus medidas de defensa nacional contra la vigilancia extranjera ilegítima, ya sea comercial o gubernamental, así como una herramienta útil para controlar las actividades digitales de sus residentes. Esto puede incluir además el control de los contenidos digitales en las redes nacionales (Sacks y Sherman, 2019). Como se ha explicado en el capítulo IV, los enfoques de China y la Federación de Rusia respecto de la gobernanza de los flujos de datos se basan en esta idea, y van más allá de las preocupaciones de seguridad técnica para abarcar cuestiones de estabilidad social, autosuficiencia tecnológica/económica y control político. Es más, la Federación de Rusia ha llegado a modificar su legislación vigente para permitir al Gobierno desconectar la Internet rusa de la red mundial desviando todo el tráfico a través de servidores locales.

Desde que en 2013 Edward Snowden reveló la existencia de programas de vigilancia a escala mundial, varios Estados han aplicado restricciones a los flujos de datos transfronterizos para garantizar la protección contra la vigilancia extranjera (Hill, 2014). Además, algunos Estados aspiran a mantener su

[3] *The Economist*, 5 de noviembre de 2016, "Online governance: Lost in the splinternet".

control soberano sobre los datos con el objetivo de proteger sus valores económicos, políticos, sociales, culturales y religiosos, aunque estas medidas extremas de localización puedan tener consecuencias graves para los derechos humanos (Taylor, 2020). Por ejemplo, la imposición de obligaciones de localización de los datos a los proveedores de servicios de medios/redes sociales podrían facilitar a los Estados el acceso a los datos de los usuarios[4]. Un mal uso de esos datos podría dar lugar a violaciones de los derechos humanos, dado el refuerzo de la capacidad de vigilancia de los Estados y el incremento de las posibilidades de los organismos nacionales de seguridad e inteligencia de seguir la pista de los ciudadanos y, en particular, de atacar a la disidencia política[5].

c) Perspectiva del desarrollo económico

Además de las perspectivas basadas en la política/seguridad y la protección de la ciudadanía expuestas anteriormente, las normativas en materia de flujos de datos transfronterizos también pueden obedecer a razones de desarrollo económico. Como se ha explicado en el capítulo IV, el enfoque de la India en lo que respecta a la regulación de los flujos de datos transfronterizos está cada vez más condicionado por cuestiones relacionadas con el desarrollo económico. Esta motivación política de promover el desarrollo económico nacional y crear referentes locales en materia de datos también está implícita en las leyes y políticas de otros países en desarrollo, como Kenya[6], Sudáfrica (Barnes y otros, 2019), el Pakistán[7] y Rwanda[8]. Incluso los países desarrollados digitalmente imponen a veces ciertas restricciones a los flujos de datos transfronterizos, probablemente para proteger a sus empresas nacionales de la competencia extranjera, entre otras cosas[9].

El hecho de que los mercados digitales suelan basarse en una dinámica de "todo para el vencedor" (Farrell y Newman, 2019; Ciuriak, 2018), unido a la falta de desarrollo de la economía digital inclusiva en muchos países en desarrollo (World Bank, 2016; UNCTAD, 2019a), ha llevado a algunos países a considerar que la adopción de políticas industriales específicas en la esfera de la economía digital resulta esencial para recuperar terreno (Azmeh y Foster, 2016) y evitar una dependencia perniciosa de las empresas tecnológicas estadounidenses y chinas (Elmi, 2020; Sherman y Morgus, 2018). Además, como las inversiones en el sector digital tienden a necesitar pocas estructuras físicas, muchas empresas que tienen su sede en países desarrollados no realizan grandes inversiones en infraestructuras locales, a pesar de que obtienen importantes beneficios de la prestación de servicios en el mercado nacional (Casella y Formenti, 2018). Por ejemplo, África y América Latina juntas representan tan solo el 4 % del conjunto de centros de datos coubicados del mundo (véase el capítulo I). Además, a excepción de algunas plataformas chinas, ninguna empresa tecnológica de los países en desarrollo ha sido capaz de imponerse en el mercado mundial.

Dada la importancia de los grandes volúmenes de datos para el desarrollo de la IA y otras tecnologías impulsadas por los datos, algunos países en desarrollo, como la India, se están centrando en desarrollar las capacidades de datos nacionales como medio de captar una proporción mayor de los beneficios que

4 Véanse, por ejemplo, las restricciones a los medios sociales aplicadas en la Federación de Rusia, el Pakistán y Turquía.

5 Véase el Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, A/HRC/27/37 (30 de junio de 2014), párrs. 2, 3, 14 y 42; y el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, A/HRC/23/40 (17 de abril de 2013), párr. 33.

6 La Ley de Protección de Datos de Kenya contiene una disposición que autoriza al Gobierno a exigir que se localicen los datos personales a fin de proteger los ingresos. Véase el artículo 50 de la Ley de Protección de Datos de 2019 (Kenya).

7 La Política de Comercio Electrónico del Pakistán, de 2019, prevé varias medidas para la localización de los datos y la regulación de los flujos de datos transfronterizos en sectores relacionados con la Internet de las cosas y los datos comerciales (disponible en www.commerce.gov.pk/wp-content/uploads/2019/08/Draft-E-Commerce-Policy-Framework-Final-23-8-19.pdf).

8 En su Política de Revolución de los Datos, Rwanda considera los datos como un "activo soberano nacional". El documento también enuncia el propósito de Rwanda de construir una industria de datos sólida. Véase la Política de Revolución de Datos (Rwanda), disponible en http://statistics.gov.rw/file/5410/download?token=r0nXaTAv.

9 Véase, por ejemplo, la iniciativa "Hecho en China 2025" (disponible en www.csis.org/analysis/made-china-2025); "Announcing the Expansion of the Clean Network to Safeguard America's Assets", 5 de agosto de 2020 (disponible en https://mr.usembassy.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/).

se dirigen a las empresas digitales extranjeras, e impulsar así el crecimiento de sus sectores digitales nacionales (Singh, 2018b; Jain y Gabor, 2020). Esos países consideran que impedir la transferencia de enormes volúmenes de datos de sus residentes a empresas extranjeras mediante leyes y políticas estrictas de localización de los datos puede ser un medio de promover el crecimiento de los centros de datos y los conjuntos de datos masivos nacionales. Este aumento de las capacidades de datos puede, a su vez, facilitar el desarrollo de productos y servicios digitales nacionales para responder a la creciente demanda de los consumidores internos, impulsando con ello el crecimiento de las empresas digitales autóctonas. Sin embargo, como se explica más adelante, la localización de los datos no puede facilitar por sí sola el desarrollo de plataformas digitales de éxito en los países en desarrollo.

En el cuadro V.1 se presenta un resumen de las diversas razones por los que los países regulan los flujos de datos transfronterizos con arreglo a las tres perspectivas enunciadas.

Cuadro V.1. Razones de los países para regular los flujos de datos transfronterizos

Protección de la ciudadanía	Seguridad/soberanía nacional	Desarrollo económico
Protección de los datos y la privacidad	Hacer frente a la vigilancia extranjera	Crear referentes locales en materia de datos
Ciberseguridad	Proteger las infraestructuras críticas	Garantizar el acceso equitativo a los datos
Supervisión de los sectores sensibles por el órgano regulador	Refozar el control soberano de Internet a nivel nacional	Responder a la demanda interna mediante productos y servicios digitales nacionales
Acceso a los datos por las fuerzas del orden	Estabilidad social/cultural	
Ética de los datos	Estabilidad política	

Fuente: UNCTAD.

2. Categorías de medidas nacionales de regulación de los flujos de datos transfronterizos

Las normativas sobre los flujos de datos transfronterizos pueden plantearse y aplicarse de diversas formas. A partir de un amplio análisis de las medidas de regulación adoptadas en todo el mundo, en esta sección se realiza una clasificación de las normativas conforme a diversos criterios: a) ámbito de aplicación: aplicables con carácter general o específicas para los flujos de datos transfronterizos de sectores concretos; b) alcance de la restricción: localización estricta; localización parcial; transferencia condicionada: estricta, intermedia y flexible; libre circulación de los datos y c) con respecto a las restricciones específicas de los flujos transfronterizos de datos personales: enfoque de responsabilidad y de adecuación.

a) Ámbito de aplicación

Las normativas sobre los flujos de datos transfronterizos pueden aplicarse con carácter general a la totalidad/mayoría de los sectores o pueden limitarse a los datos recopilados y tratados en sectores concretos. Varios países han adoptado leyes de protección de datos que regulan las transferencias transfronterizas de datos personales; como los flujos de datos personales son comunes a la mayoría de los sectores, estas medidas tienen un ámbito de aplicación "general". El RGPD representa un ejemplo destacado (capítulo IV). Asimismo, como ya se ha comentado, varios países reproducen parcial o totalmente el enfoque de la Unión Europea en lo que respecta a la regulación de los flujos transfronterizos de datos personales[10]. Por ejemplo, en América Latina, los marcos normativos de protección de datos son los principales instrumentos que abordan expresamente la cuestión de los flujos de datos transfronterizos. En general, en los países en que existe una legislación nacional de protección de datos (que representan más de la mitad de la región) existe un régimen de restricciones condicionadas de los flujos de datos transfronterizos.

[10] Por ejemplo la Argentina, Armenia, Bahrein, Barbados, el Brasil, Colombia, Georgia, Israel, Malasia, el Perú, Sudáfrica, Suiza, Turquía y Ucrania.

Además, algunos países imponen requisitos de autorización para las transferencias transfronterizas de datos personales[11]. En algunos casos excepcionales, también se impone el requisito estricto de almacenar y/o procesar los datos personales dentro del país. Por ejemplo, una disposición del proyecto de ley de protección de datos de Rwanda exige a los responsables/encargados del tratamiento de los datos que alojen/almacenen los datos personales en Rwanda[12]; si se aprueba esta ley, aunque los datos personales se traten en el extranjero, las empresas estarán obligadas a almacenarlos en el país. En el proyecto de ley de protección de datos de China (capítulo IV) también se proponen requisitos específicos para el almacenamiento y el tratamiento local de los datos personales[13].

Por otra parte, varios países aplican normas sectoriales a los flujos de datos transfronterizos. Por ejemplo, Australia, China, los Emiratos Árabes Unidos y el Reino Unido prohíben expresamente los flujos de datos transfronterizos en el sector sanitario con el objetivo de preservar la confidencialidad de los pacientes[14]. Otras normas sectoriales relacionadas con la confidencialidad y la seguridad de los datos son las restricciones a la transferencia transfronteriza de datos cartográficos en la web impuestas por China y la República de Corea[15]. Asimismo, los Estados Unidos exigen que los datos relacionados con la defensa se almacenen en servidores nacionales en la nube (capítulo IV)[16]. Por último, varios países exigen el almacenamiento local de los datos en los sectores que requieren un mayor control reglamentario, como los datos financieros[17], los datos relacionados con los seguros[18], los pagos electrónicos[19], los datos de telecomunicaciones[20] y los datos relacionados con los juegos de azar[21].

---

11 Véase, por ejemplo, el artículo 44 de la Ley núm. 18-07, de 10 de junio de 2018, de Protección de las Personas Físicas en relación con el Tratamiento de los Datos Personales (Argelia); el artículo 43 de la Ley núm. 09-08, de 18 de febrero de 2009 (Marruecos); y el artículo 54 del proyecto de ley de protección de datos (Rwanda).

12 Artículo 55 del proyecto de ley de protección de datos (Rwanda).

13 Artículo 40 de la Ley de Protección de la Información Personal (China) (aplicable a los operadores de infraestructuras críticas y a los gestores de información personal con notificación previa).

14 Véase, por ejemplo, el artículo 77 de la Ley de Registros Sanitarios Electrónicos Controlados Personalmente (Australia); el artículo 10 de las Medidas de Gestión de la Información Sanitaria de la Población (China); la Ley de Datos Sanitarios de 2019 (Emiratos Árabes Unidos); y "National Health Service and social care data: off-shoring and the use of public cloud services guidance 2018" (Reino Unido) (disponible en https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services).

15 Véase, por ejemplo, el artículo 16 de la Ley de Establecimiento, Gestión, etc., de Datos Espaciales (República de Corea); y el artículo 34 del Reglamento sobre la Gestión de Mapas (China).

16 Departamento de Defensa de los Estados Unidos, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, DFARS Case 2013-D018 (disponible en www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reportingand-contracting-for).

17 Véase, por ejemplo, el artículo 12 de la Ley Consolidada núm. 648 de 15 de junio de 2006 (Dinamarca); y el artículo 6 del *Aviso por el que se insta a las instituciones financieras bancarias a proteger la información financiera personal* (China).

18 Véase, por ejemplo, el artículo 18 del Reglamento de la IRDAI (Externalización de las actividades por las compañías de seguros indias), 2017 (India) (aplicable a los titulares de pólizas de las compañías de seguros).

19 Véase, por ejemplo, el párr. D6.1 del Marco Normativo para los Valores Almacenados y los Sistemas de Pago Electrónico (Emiratos Árabes Unidos); la *Notificación relativa al almacenamiento de datos del sistema de pagos del Banco de la Reserva de la India (RBI)* (India); y el artículo 23 de la Ley núm. 6493, de Sistemas de Pago y Liquidación de Valores, Servicios de Pago y Entidades de Dinero Electrónico (Turquía).

20 Véase, por ejemplo, "German Bundestag Passes New Data Retention Law", 16 de octubre de 2015 (disponible en www.gppi.net/2015/10/16/german-bundestag-passes-new-data-retention-law); la *Ley Federal núm. 374, por la que se modifica la Ley Federal relativa a la lucha contra el terrorismo y a determinadas disposiciones legislativas de la Federación de Rusia relativas a la formulación de medidas adicionales para la lucha contra el terrorismo y la protección de la seguridad pública* (2016) (Federación de Rusia); y las *Directrices para la creación de contenido nigeriano en el sector de las tecnología de la información y las comunicaciones* (Nigeria), disponible en https://nitda.gov.ng/regulations/.

21 Véase, por ejemplo, el artículo 15B vi) de la *Ley núm.124, de mayo de 2015, por la que se aprueba la Orden Gubernamental de Emergencia núm. 92/2014, que regula las medidas fiscales y la modificación de las leyes* (Rumania).

b) Nivel de restricción

Las normativas también pueden clasificarse en función de su grado de restricción.

i) Localización estricta

Por localización estricta se entiende la obligación jurídica de almacenar y/o procesar los datos en el país, y puede incluir una prohibición total de las transferencias transfronterizas de datos (incluso a efectos de tratamiento). Algunos países imponen requisitos de localización estricta que pueden afectar a la economía en general. Por ejemplo, China ha impuesto obligaciones estrictas de localización de los datos para la información personal y los datos importantes recopilados por los operadores de infraestructuras críticas[22], lo que puede afectar a un gran volumen de flujos de datos transfronterizos. La Ley de Ciberseguridad de Viet Nam contiene una disposición amplia y estricta de localización que exige a todos los proveedores extranjeros y nacionales de telecomunicaciones, así como a los servicios de Internet (incluidos los servicios de libre transmisión) ofrecidos en línea, que almacenen los datos localmente[23].

En otros países, los requisitos de localización pueden aplicarse de forma muy amplia, a discreción del organismo de reglamentación. Por ejemplo, en Kenya, el Gobierno está facultado para exigir que los datos personales se traten "exclusivamente a través de servidores o centros de datos localizados en Kenya sobre la base de intereses estratégicos del Estado o de protección de los ingresos". Si se aplicase de forma muy ambigua o general, esta disposición podría llegar a convertirse en un requisito general de localización[24]. Asimismo, la India y el Pakistán prevén prohibir expresamente las transferencias transfronterizas de "datos personales críticos" y exigir que dichos datos se almacenen y procesen localmente, sin proporcionar una definición específica de este término[25]; por lo tanto, si posteriormente los Gobiernos definiesen el término "datos personales críticos" de manera amplia, este requisito afectaría a grandes volúmenes de flujos de datos.

Algunos países imponen requisitos estrictos de localización a determinadas categorías de datos, como los datos relacionados con la salud[26], la defensa[27], la Internet de las cosas[28] y la cartografía[29] y, con carácter más general, los datos gubernamentales y públicos críticos[30]. Otros requisitos estrictos de localización

22 Artículo 37 de la Ley de Ciberseguridad (China).

23 Artículo 6, párr. 3, de la Ley de Ciberseguridad (Viet Nam). Sin embargo, un informe reciente indica que la intención del Gobierno es aplicar esta disposición únicamente a las empresas que no adopten medidas cuando se les notifique que han vulnerado la ley. Véase *The Business Times*, 15 de octubre de 2019, "Data localisation requirements narrowed in Vietnam's cybersecurity law".

24 Artículo 50 de la Ley de Protección de Datos de 2019 (Kenya).

25 Artículo 33, párr. 2, del proyecto de ley de protección de los datos personales (India); y artículo 14, párr. 1, del proyecto de ley de protección de datos (Pakistán).

26 Véase, por ejemplo, el artículo 77 de la Ley de Registros Sanitarios Electrónicos Controlados Personalmente (Australia); NHS, *NHS and Social Care Data: Off-Shoring and the Use of Public Cloud Services Guidance 2018* (Reino Unido).

27 Departamento de Defensa de los Estados Unidos, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, DFARS Case 2013-D018 (disponible en www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reportingand-contracting-for).

28 Véase, por ejemplo, el párr. 7 del Marco Regulador de la Internet de las Cosas (Arabia Saudita).

29 Artículo 16 de la Ley de Establecimiento, Gestión, etc., de Datos Espaciales (República de Corea); y artículo 34 del Reglamento sobre la Gestión de Mapas (China).

30 Véase, por ejemplo, la Circular Presidencial sobre las Medidas de Seguridad de la Información y la Comunicación (julio de 2019) (Turquía) (aplicable a la información y los datos críticos, como el registro civil, la información sanitaria y de las comunicaciones, así como los datos genéticos y biométricos); el artículo 17 de la Orden Ministerial núm. 001/MINICT/2012, de 12 de marzo de 2012 (Rwanda); los Controles Esenciales de Ciberseguridad (Arabia Saudita) 27; y Departamento de Estado de los Estados Unidos, *2020 Investment Climate Statements: Algeria* (disponible en www.state.gov/reports/2020-investment-climate-statements/algeria/).

hacen referencia a los registros empresariales[31], los registros fiscales[32] y los registros contables[33]. Los requisitos de localización relativos a los registros empresariales o contables suelen corresponder a leyes heredadas, es decir, aplicadas en una época en la que todos los registros se almacenaban en papel o en computadoras locales en lugar de en servidores en la nube. Por ese motivo, algunas voces expertas sostienen que esas leyes pueden no estar muy adaptadas a la actual era digital, en la que la mayoría de los registros se almacenan en la nube (WEF, 2020b:13).

ii) Localización parcial

La localización parcial se refiere a la obligación legal de almacenar los datos localmente, pero no incluye la prohibición de transferir o almacenar copias de los datos en el extranjero, aunque puede abarcar requisitos específicos para la transferencia y el almacenamiento transfronterizos de datos. Por ejemplo, la Federación de Rusia y Kazajstán exigen a las empresas que almacenen una copia local de los datos personales, aunque estos pueden transferirse al extranjero[34]. Turquía y el Pakistán obligan a las empresas de medios sociales a almacenar localmente todos los datos de los usuarios, aunque no existe una prohibición expresa de las transferencias transfronterizas[35]. Algunas provincias del Canadá exigen que la información personal recopilada por los organismos públicos se almacene localmente, aunque permiten que estos datos se transfieran al extranjero en determinados casos, por ejemplo, tras obtener el consentimiento del titular de los datos[36].

iii) Transferencia condicionada (estricta, intermedia o flexible)

Los requisitos de transferencia condicionada implican que los datos pueden transferirse al extranjero a condición de que el responsable de su tratamiento cumpla con los requisitos previstos. En función de cómo se planteen esos requisitos, las transferencias condicionadas podrán clasificarse como estrictas, intermedias o flexibles.

Los requisitos para la transferencia transfronteriza de datos son extremadamente frecuentes en las leyes de protección de datos. Las transferencias condicionadas estrictas implican un régimen de cumplimiento amplio que incluye aprobaciones de las transferencias a países específicos (por ejemplo, un enfoque de adecuación), autorizaciones del órgano regulador para la realización de transferencias[37] y contratos aprobados para la transferencia (por ejemplo, las cláusulas contractuales tipo y normas corporativas

---

31 Véase, por ejemplo, el Código de Comercio de Alemania, artículo 257, núms. 1 y 4 (Handelsgesetzbuch § 257) (Alemania).

32 Véase, por ejemplo, el artículo 315 del Código del Impuesto sobre la Renta (Bélgica); y el artículo 60 del Código del IVA (Bélgica).

33 Véase, por ejemplo, el artículo 388, párr. 2, de la Ley de Sociedades de 2006 (Reino Unido); y la Ley de Contabilidad (1336/1997) (Finlandia).

34 Véase, por ejemplo, el artículo 18, párr. 5, de la Ley Federal núm. 152-FZ, de Datos Personales, modificada en julio de 2014 por la *Ley Federal núm. 242-FZ, por la que se modifican determinadas disposiciones legislativas de la Federación de Rusia para aclarar el tratamiento de datos personales en las redes de información y telecomunicaciones* (Federación de Rusia); y el artículo 12, párr. 2, de la Ley de Datos Personales (Kazajstán).

35 Enmiendas al Reglamento sobre Transmisiones por Internet y Prevención de los Delitos Cometidos en el marco de Esas Emisiones, Ley núm. 5651, octubre de 2020 (Turquía), disponible en https://iapp.org/news/a/turkish-data-localization-rules-in-effect-for-social-media-companies/; y artículo 5 d) de las Normas de Protección de los Ciudadanos (frente a los Daños en Internet), 2020 (Pakistán).

36 Artículo 30, párr. 1, de la Ley de Libertad de Información y Protección de la Privacidad, R.S.B.C. 1996 (Columbia Británica, Canadá); y artículo 5, párr. 1, de la Ley de Protección frente a la Divulgación Internacional de Información Personal, S.N.S. 2006 (Nueva Escocia, Canadá).

37 Véase, por ejemplo, el artículo 9 de la Ley núm. 6698, de Protección de Datos Personales (Turquía) (aplicable cuando se realizan transferencias a un país con un nivel insuficiente de protección de datos); el artículo 14 de la Ley núm. 151, de Protección de Datos Personales (Egipto); el artículo 44 de la Ley núm. 18-07, de 10 de junio de 2018, de Protección de las Personas Físicas en relación con el Tratamiento de los Datos Personales (Argelia); el artículo 48 de la Ley núm. 2004-63, de 27 de julio de 2004, de Protección de los Datos Personales (Túnez); y el artículo 5 de la Ley núm.2013-450, de 19 de junio de 2013, de Protección de los Datos Personales (Côte d'Ivoire).

vinculantes previstas en el RGDP), y están sujetas a una estricta supervisión del órgano regulador[38]. En los casos en que se autorizan las transferencias por contrato, el organismo regulador puede exigir al responsable del tratamiento de los datos que demuestre que el receptor ha aplicado las medidas adecuadas para garantizar el cumplimiento de la legislación nacional sobre protección de datos[39]. Un requisito aplicado por varios países africanos es el mantenimiento de un registro de todas las personas e instituciones que recopilan datos personales, en particular a los efectos de la recopilación de datos y de la transferencia transfronteriza de datos[40].

Aunque existan requisitos de cumplimiento estrictos, los países suelen permitir las transferencias transfronterizas de datos personales en determinadas circunstancias, por ejemplo en los casos en que la legislación nacional de protección de datos prevé excepciones por motivos de necesidad (por ejemplo, la necesidad de ejecutar un contrato, de proteger el interés público o de proteger los intereses vitales del titular de los datos), o cuando se obtiene el debido consentimiento de los titulares de los datos[41]. Algunas leyes de protección de datos también contienen exenciones específicas para las transferencias transfronterizas de datos con fines de Estado o de orden público[42], para la investigación médica[43], para las transferencias bancarias o bursátiles[44], o en cumplimiento de un tratado internacional[45].

Con la expresión "requisitos de transferencia condicionada intermedia o flexible" se hace referencia a requisitos más fáciles de cumplir, como la obtención del consentimiento implícito de los titulares o requisitos limitados de notificación a los titulares, o a casos en que los encargados del tratamiento de los datos pueden realizar transferencias transfronterizas de datos en función de una evaluación personal del marco de protección de datos en el país receptor con la celebración de los contratos necesarios (es decir, con arreglo a lo dispuesto en la ley). Por ejemplo, para la transferencia de datos personales al extranjero, la Ley de Protección de Datos de México solo exige el consentimiento de los titulares y la celebración de los contratos necesarios entre los encargados del tratamiento de los datos y las partes extranjeras que gestionan los datos personales, y no existe ningún otro requisito de aprobación previa por el órgano regulador[46]. Además, se permiten expresamente las transferencias transfronterizas de

38 A este respecto, algunos países exigen el registro de todas las bases de datos o las transferencias transfronterizas de datos. Véase, por ejemplo, el artículo 21 de la Ley núm. 25326 (Ley de Protección de los Datos Personales) (Argentina); y el artículo 16 de la Ley núm. 6698, de Protección de Datos Personales (Turquía). Véase también el artículo 22 del Reglamento Ministerial núm. 20, de 2016, relativo a la protección de los datos personales en los sistemas electrónicos (Indonesia); y el artículo 6 del Reglamento Gubernamental núm. 71 de 2019 (Indonesia) (impone a todos los operadores de sistemas electrónicos privados de Indonesia la obligación de obtener la aprobación del Estado para gestionar, tratar y almacenar sus datos fuera del país).

39 Véase, por ejemplo, el artículo 26 del Decreto núm. 1377/2013 (Colombia); y el artículo 48 de la Ley de Protección de Datos de 2019 (Kenya).

40 Véase, por ejemplo, el artículo 29 de la Ley de Protección de Datos y Privacidad de 2019 (Uganda); y el artículo 21 de la Ley de Protección de Datos de 2019 (Kenya).

41 Véase, por ejemplo, el artículo 49 del RGPD; el artículo 12 de la Ley núm. 25326 (Ley de Protección de los Datos Personales) (Argentina); el artículo 76 de la Ley de Protección de Datos de 2018 (Reino Unido); el artículo 29 de la Ley núm. 2297 VI, de Protección de los Datos Personales (Ucrania); y el artículo 48 c) de la Ley de Protección de Datos de 2019 (Kenya).

42 Véase, por ejemplo, el artículo 12, párr. 2 e), de la Ley núm. 25326 (Ley de Protección de los Datos Personales) (Argentina); el artículo 12, párr. 1 j), de la Ley de Protección de Datos del Centro Financiero Internacional de Dubai (Ley núm. 1 de 2007); el artículo 20, párr. 3, de la Ley de Protección de los Datos Personales (Ley 8/2005) (Macao, China); y el artículo 31, párr. 2 b) iii), de la Ley de Protección de Datos de 2004 (Ley núm. 13 de 2004) (Mauricio).

43 Véase, por ejemplo, el artículo 15 de la Ley núm. 29733, de Protección de Datos Personales (Perú).

44 Véase, por ejemplo, el artículo 12 de la Ley núm. 25326 (Ley de Protección de los Datos Personales) (Argentina).

45 Véase, por ejemplo, el artículo 15 de la Ley núm. 29733, de Protección de Datos Personales (Perú); el artículo 12 de la Ley núm. 25326 (Ley de Protección de los Datos Personales) (Argentina); el artículo 45 de la Ley núm. 18-07, de 10 de junio de 2018, de Protección de las Personas Físicas en relación con el Tratamiento de los Datos Personales (Argelia); y el artículo 41, párr. 2, de la Ley de Protección de Datos (Georgia).

46 Artículo 8, leído junto con el artículo 36, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México).

datos dentro de los grupos empresariales[47]. Asimismo, en la República de Corea, las empresas están obligadas a obtener el consentimiento de los titulares antes de "exportar"[48] datos personales, pero no existen otras prohibiciones expresas en relación con las transferencias de datos[49].

iv) Libre circulación de los datos

Con la expresión "libre circulación de los datos" se suele hacer referencia a las normativas que no imponen ninguna restricción específica a los flujos de datos transfronterizos, si bien pueden contener normas de responsabilidad *ex post* para las empresas, es decir, los encargados del tratamiento tienen la responsabilidad de garantizar que todo el tratamiento que realizan en el extranjero sea conforme con la legislación nacional pertinente. Por ejemplo, en el Canadá, las empresas que transfieran datos personales al extranjero son responsables de garantizar el cumplimiento de la legislación nacional, pero no existen restricciones expresas a dichas transferencias. En su lugar, las organizaciones deben designar a una persona que se haga responsable de garantizar el cumplimiento de las leyes nacionales de protección de datos[50]. No se necesita el consentimiento explícito del titular para la transferencia de datos al extranjero, pero las organizaciones deben incluir información sobre la transferencia a países extranjeros en sus políticas de privacidad[51]. Asimismo, Australia[52], Singapur[53] y Filipinas[54] han respaldado el principio de responsabilidad, facilitando así un entorno relativamente libre para los flujos transfronterizos de datos personales. Muchos PMA todavía no han implantado un marco regulador para la protección de datos y, por lo tanto, no han impuesto ninguna normativa que afecte a los flujos de datos transfronterizos, es decir, los datos circulan libremente a través de las fronteras por defecto, dado que no están regulados[55].

c) El enfoque geográfico frente al enfoque de responsabilidad en la gestión de los flujos de datos personales

Las normativas suelen aplicarse específicamente a los datos personales, y en líneas generales se pueden clasificar en función de que adopten: a) un enfoque de adecuación (o enfoque geográfico), en el que las transferencias de datos se regulan tomando como base las normas/leyes de protección de datos del país receptor (por ejemplo, el Estado puede determinar qué países extranjeros tienen marcos de protección de datos "adecuados", "suficientes" o "equivalentes", permitiendo así expresamente las transferencias de datos a dichos países o aprobando las transferencias en función de cada caso particular); b) un enfoque de responsabilidad (o dependiente de la organización), en el que las transferencias de datos se basan en que el "exportador" de datos se haga responsable ante el Gobierno nacional y, por extensión, ante los usuarios, del cumplimiento de las normas de protección de datos, con independencia de dónde se transfieran, almacenen o procesen (Kuner, 2013). El enfoque de responsabilidad requeriría la aplicación transfronteriza de la ley; es decir, en los casos en que el encargado del tratamiento de los datos ubicado en el extranjero incumpla las prescripciones de la legislación nacional. Por ejemplo, en América Latina, la tendencia se basa en el enfoque de la adecuación.

---

47 Artículo 37, párr. III, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México).

48 Se añaden comillas para señalar que esta es la formulación del país, no del presente Informe, ya que los flujos de datos no son exportaciones, sino flujos de salida. Este es el enfoque que se ha seguido a lo largo de este Informe.

49 Artículo 17, párr. 3, de la Ley de Protección de la Información Personal (República de Corea).

50 Principio 1, anexo I, artículo 4.1.3, de la Ley de Protección de la Información Personal y los Documentos Electrónicos (S.C. 2000, c. 5) (Canadá).

51 Oficina de la Comisionada de Protección de la Privacidad del Canadá, *Guidelines for Processing Personal Data Across Borders*, enero de 2009 (disponible en www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf).

52 Principio de privacidad núm. 8 de la Ley de Privacidad de 1988 (Australia).

53 Artículo 26 de la Ley de Protección de los Datos Personales (Singapur).

54 Artículo 21 de la Ley de Privacidad de los Datos de 2012 (Ley de la República núm. 10173) (Filipinas).

55 Para consultar ejemplos de PMA que no han adoptado ningún marco de protección de datos, véase UNCTAD, Cyberlaw Tracker (disponible en: https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide).

En la práctica, cualquier marco de protección de datos podría incorporar un enfoque tanto de adecuación como de responsabilidad. Por ejemplo, las empresas de la Unión Europea, además de basarse en una decisión favorable de adecuación, pueden llevar a cabo transferencias transfronterizas de datos mediante el uso de cláusulas contractuales tipo, normas corporativas vinculantes u otros mecanismos de certificación aprobados, o en las condiciones en que las leyes nacionales autoricen tales transferencias (Kuner, 2013). Lo mismo ocurre con muchos países que han adoptado un enfoque de adecuación[56]. Otros países —como el Canadá, Singapur y Australia— se basan en un enfoque de responsabilidad para las transferencias transfronterizas de datos personales, como se ha comentado anteriormente.

3. Consecuencias de la regulación de los flujos de datos transfronterizos para la política nacional

En esta sección se examinan las diversas ventajas e inconvenientes de los diferentes tipos de normativas sobre los flujos de datos transfronterizos desde una perspectiva reguladora, de desarrollo económico y de gobernanza mundial de los datos.

a) Perspectiva reguladora: ventajas e inconvenientes

Aunque muchas normativas sobre los flujos de datos transfronterizos se adoptan con el fin de alcanzar objetivos políticos o reguladores legítimos, no deja de ser necesario evaluar hasta qué punto estas medidas pueden ser eficaces para alcanzar esos objetivos, y si son proporcionales a los riesgos políticos que entrañan y a los costos asociados a su aplicación.

En general, las normativas sobre los flujos de datos transfronterizos presentan algunos problemas de aplicación. En primer lugar, como los organismos públicos responsables de gestionar las diferentes dimensiones de los flujos de datos transfronterizos (por ejemplo, comercio, telecomunicaciones, industria nacional y desarrollo, asuntos internos y regulación de Internet) son múltiples, el posible solapamiento, junto con la falta de coordinación entre estos organismos, puede dar lugar a normativas o posiciones políticas nacionales incoherentes y descoordinadas en relación con los flujos de datos transfronterizos (Chen y otros, 2019). Así, los organismos reguladores, a pesar de que se ocupan de muchas cuestiones que se solapan en relación con la economía impulsada por los datos, la protección de datos y las tecnologías de la información y las comunicaciones (TIC), en la práctica casi nunca colaboran (ITU, 2018). Una propuesta reciente publicada por el Ministerio de Electrónica y Tecnología de la Información de la India sobre los datos no personales, que exige que los datos anonimizados recopilados por las grandes empresas tecnológicas se compartan con el Gobierno, la ciudadanía y otras empresas, pone de manifiesto esa falta de coordinación entre los distintos organismos públicos. La propuesta suscitó preocupación por posibles conflictos con la jurisdicción de la Comisión de la Competencia de la India[57].

En segundo lugar, muchos países formulan sus normativas sobre los flujos de datos transfronterizos de forma deliberadamente ambigua para permitir una discrecionalidad administrativa ilimitada. Por ejemplo, términos como “datos críticos”, “datos importantes”, “datos personales sensibles”, “infraestructuras críticas”, “soberanía sobre los datos”, “soberanía digital/cibersoberanía” —aunque se utilizan en muchos documentos normativos y reguladores— pueden tener significados y contextos diferentes. Por ejemplo, ni la India ni el Pakistán han definido lo que entienden por datos personales críticos. Algunas voces expertas han señalado también que la posición de la Unión Europea sobre la “soberanía digital” es ambigua y hace que su postura en relación con la localización de los datos resulte confusa (Christakis, 2020). La definición de infraestructuras críticas también varía entre las diferentes jurisdicciones (OECD, 2019c). En

[56] Véase, por ejemplo, el artículo 26 de la Ley 1581/2012 (Colombia); el artículo 14 de la Ley núm. 29733, de Protección de Datos Personales (Perú); el artículo 33 de la Ley General de Protección de Datos (LGPD), Ley Federal núm. 13, 709/2018 (Brasil); el artículo 74 de la Ley de Protección de Datos de 2018 (Reino Unido); el artículo 29 de la Ley núm. 2297 VI, de Protección de los Datos Personales (Ucrania); el artículo 12, párr. 1, de la Ley núm. 30, de 2018, de Protección de los Datos Personales (Bahrein); el artículo 1 del Reglamento de Protección de la Privacidad (Transferencia de Datos a Bases de Datos en el Extranjero), 5761-2001 (Israel); el artículo 28 de la Ley de Protección de los Datos Personales (Tailandia); el artículo 129, párr. 1, de la Ley de Protección de los Datos Personales (Malasia); y el artículo 41 de la Ley de Protección de Datos (Georgia).

[57] *Bloomberg*, 22 de septiembre de 2020, “Mandatory Sharing Of Non-Personal Data At Odds With Competition Law”.

consecuencia, la falta de definiciones claras y coherentes de términos clave como "datos personales" o "información personal" puede generar incertidumbre y afectar negativamente a los intereses tanto de los consumidores como de las empresas, sobre todo por el aumento de los costos de cumplimiento para las multinacionales, pero también para las empresas más pequeñas que participan en el comercio internacional.

En tercer lugar, otro problema de aplicación conexo es la medida en que las leyes de protección de datos se aplican a los datos no personales. Como la mayoría de los conjuntos de datos utilizados en los trámites comerciales contienen un mínimo de datos personales[58], muchas pequeñas empresas, al carecer de los recursos necesarios para almacenar estos dos tipos de datos en espacios separados, se ven obligadas a adoptar el nivel de protección más alto para todo el conjunto de datos, lo que conlleva costos adicionales y reduce en general su competitividad (WEF, 2020b; Casalini y López González, 2019).

En cuarto lugar, las normativas sectoriales pueden plantear problemas de aplicación de carácter práctico. Por ejemplo, algunos países restringen la salida de datos sanitarios de carácter personal. Sin embargo, no está claro si los datos sanitarios se limitan a los historiales médicos o incluyen información relacionada con la salud que puede ser recopilada por productos de la Internet de las cosas como los relojes inteligentes, u obtenerse a partir de un estudio de los datos de navegación en Internet de los particulares (Kavacs y Ranganathan, 2019)[59]. Por último, hay problemas de aplicación y verificación del cumplimiento a nivel institucional que se deben a limitaciones presupuestarias y a una falta de voluntad política. Por ejemplo, en América Latina estos problemas no se deben tanto a la falta de un instrumento normativo o regulador como a las dificultades para aplicar y hacer cumplir algunas leyes sin contar con el apoyo humano e institucional necesario[60].

Desde el punto de vista tecnológico, el lugar en el que se almacenan/tratan los datos no garantiza por sí mismo la protección o seguridad de estos. La privacidad/protección de datos depende más bien de las tecnologías y normas en que se apoyan los sectores impulsados por los datos (Chander y Lê, 2014; Komaitis, 2017; Mishra, 2020b). Las ciberamenazas son de naturaleza mundial e incluso pueden tener un origen nacional. Por lo tanto, almacenar los datos en el país no reduce necesariamente la vulnerabilidad frente a los ciberataques. De hecho, la localización puede incluso resultar más perjudicial para la seguridad de los datos cuando se impone en países con una infraestructura digital deficiente. En cambio, unas normas estrictas de privacidad y ciberseguridad pueden ayudar a proteger los datos de las intrusiones, con independencia del lugar en el que se almacenen. Además, el almacenamiento forzoso de los datos en países donde el Gobierno puede exigir un acceso encubierto a tales datos facilita la vigilancia del Estado. Por otra parte, los datos personales pueden estar mejor protegidos con normas de cifrado estrictas, independientemente del lugar en que las empresas almacenen los datos (Chander y Lê, 2014). Otras preocupaciones que se plantean es que puedan producirse desastres naturales a gran escala que destruyan servidores de datos ubicados en regiones específicas (Leviathan Security Group, 2015). Por último, los conjuntos de datos localizados que resultan de las restricciones impuestas a los flujos de datos, a diferencia de los conjuntos de datos globales que combinan datos de todos los países, plantean nuevos riesgos políticos; por ejemplo, los conjuntos de datos locales dificultan a las empresas la detección de pautas de actividades delictivas como el blanqueo de capitales, la financiación del terrorismo y el fraude (Chander y Ferracane, 2019; GSMA, 2019c).

Los países con una legislación sólida en materia de protección de datos tienen más posibilidades de considerarse destinos seguros para las salidas de datos, sobre todo ante la falta de un enfoque internacional uniforme en lo que respecta a la protección de datos (lo que justifica el sentido de un

[58] Un estudio realizado por la OCDE puso de manifiesto que la mayoría de las empresas manejaban cantidades significativas de datos personales, especialmente en sectores como las telecomunicaciones, las TIC y las finanzas (Casalini y López González, 2019).

[59] Por supuesto, es posible que en determinadas leyes nacionales se defina específicamente el alcance de estas normas.

[60] De hecho, en respuesta a esta situación, en 2019 la Red Iberoamericana de Protección de Datos emitió un comunicado especial en el que expresaba su "preocupación" por "los cada vez más frecuentes procesos de falta de apoyo institucional y presupuestario" a las autoridades de protección de datos por parte de los respectivos Gobiernos. *Declaración del XVII EIPD sobre el estado de las Autoridades Iberoamericanas de Protección de Datos* (disponible en www.redipd.org/sites/default/files/2020-01/declaracion-ripd-estado-autoridades-xvii-encuentro.pdf).

enfoque de adecuación). En la práctica, un enfoque de adecuación puede politizarse y suele requerir largos períodos de negociación, como demuestra la experiencia reciente de las negociaciones relativas a la adecuación entre la Unión Europea y el Japón[61]. Además, es probable que la mayoría de los países en desarrollo, en particular los PMA, tengan dificultades para negociar un acuerdo de adecuación con la Unión Europea o con la mayor parte de los países desarrollados, ya que carecen del poder económico y de las capacidades necesarias para realizar los ajustes normativos requeridos (por ejemplo, lograr la equivalencia con el RGPD).

La aplicación de las normativas sobre los flujos de datos transfronterizos también conlleva costos que los países deben tener en cuenta al formular su normativa nacional; por ejemplo, para garantizar el cumplimiento de los requisitos de localización dispuestos en las leyes de protección de datos, los países deben destinar una cantidad considerable de recursos a supervisar y auditar los centros de datos de estos proveedores de servicios. Son pocos los PMA y otros países en desarrollo que disponen de los recursos necesarios para llevar a cabo un escrutinio regulador tan intenso. Por ejemplo, aunque Nigeria ha impuesto varios requisitos de localización de los datos, el Estado ha experimentado dificultades para supervisar su aplicación o imponer sanciones en caso de infracción debido a la falta de capacidad y recursos para supervisar los flujos de datos[62]. Además, algunos mecanismos contractuales y de certificación para la transferencia transfronteriza de datos —como las normas corporativas vinculantes, las cláusulas contractuales tipo y las normas transfronterizas de privacidad del Foro de Cooperación Económica de Asia y el Pacífico (APEC)— son inasequibles para las microempresas y las pequeñas y medianas empresas (mipymes), y requieren plazos de tramitación largos (Mattoo y Meltzer, 2018; WEF, 2020b), lo que afecta significativamente a las oportunidades económicas de las empresas impulsadas por datos más pequeñas de los países en desarrollo.

A pesar de las dificultades de aplicación de las normativas sobre los flujos de datos, estas pueden ser necesarias por diversos motivos y conllevar ventajas normativas específicas en sectores concretos o en determinados ámbitos de gobierno. Por ejemplo, algunas medidas de localización de los datos son esenciales para que los órganos reguladores puedan realizar una supervisión adecuada (al facilitar el acceso inmediato y sin obstáculos a los datos)[63] y también para las actividades de las fuerzas del orden (como la investigación de delitos penales dentro del territorio nacional). Un estudio de la Comisión Europea indica que más de la mitad de las investigaciones penales que se llevan a cabo actualmente en el mundo requieren el acceso a pruebas electrónicas más allá de las fronteras nacionales, lo que se traduce en un aumento drástico de las solicitudes de transferencia transfronteriza de datos a las principales plataformas digitales y empresas de alojamiento de datos por los Estados[64]. Esta cuestión sigue, en gran medida, pendiente de resolverse, ya que procedimientos como los tratados de asistencia judicial recíproca y las comisiones rogatorias[65] resultan lentos y muy anticuados para el mundo digital. Existen pocas iniciativas

[61] Las negociaciones entre la Unión Europea y el Japón comenzaron en enero de 2017, y la decisión de adecuación se adoptó finalmente el 23 de enero de 2019, tras un período de dos años. Véase Comisión Europea, "La Comisión propone estrictas normas de privacidad para todas las comunicaciones electrónicas y actualiza las normas sobre protección de datos para las instituciones de la UE" (disponible en https://ec.europa.eu/commission/presscorner/detail/es/IP_17_16); y Comisión Europea, Decisión de Ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la Protección de la Información Personal, C/2019/304/, DO L 76, 19 de marzo de 2019.

[62] Representante de los Estados Unidos para Asuntos Comerciales, *2020 Investment Climate Statements: Nigeria* (disponible en https://www.state.gov/reports/2020-investment-climate-statements/nigeria/).

[63] En ese sentido, los memorandos de entendimiento suscritos por los reguladores financieros de Singapur con sus homólogos de los Estados Unidos y Australia para garantizar el acceso a los datos constituyen ejemplos interesantes. Véase www.mas.gov.sg/news/media-releases/2000/mas-signs-memorandum-of-understanding-with-the-australian-securities-and-investments-commission--16-may-2000.

[64] Comisión Europea, Recomendación de Decisión del Consejo por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal, COM(2019) 70 final, 5 de febrero de 2019.

[65] Las comisiones rogatorias son solicitudes oficiales realizadas por el tribunal de un país al tribunal de otro país para que le preste asistencia en los procedimientos judiciales, por ejemplo, en relación con las pruebas.

legales para abordar las solicitudes de transferencia transfronteriza de datos, lo que explica en parte la adopción de la Ley CLOUD por los Estados Unidos (capítulo IV).

Varias normativas sobre los flujos de datos transfronterizos tienen como objetivo garantizar que los datos que circulan a través de las fronteras gocen del mismo nivel de protección, seguridad y confidencialidad que los que circulan dentro del territorio nacional. Los Gobiernos pueden querer garantizar que los residentes tengan un acceso adecuado a los recursos nacionales disponibles si se produce una filtración de datos en el extranjero. Este desafío es especialmente difícil para los PMA y otros países en desarrollo con escasa capacidad para hacer cumplir la ley, aun cuando existan contratos vigentes entre los consumidores/empresas locales y las empresas extranjeras que procesan los datos personales de sus nacionales en el extranjero. Ante la falta de un marco internacional vinculante[66], la aplicación transfronteriza de la legislación sobre privacidad sigue siendo uno de los mayores desafíos, incluso para los países más desarrollados, en un mundo digitalmente interconectado (Greze, 2019). Por ello, los Gobiernos pueden ver la restricción de las transferencias de datos personales como la única forma práctica de proteger la privacidad de su ciudadanía si no existe un régimen más amplio de protección de datos común entre los países interesados (Panday, 2017).

Las consideraciones relacionadas con la seguridad nacional cada vez condicionan más las medidas de regulación adoptadas por los países en materia de flujos de datos transfronterizos. La estrecha "interdependencia" digital que caracteriza el mundo actual hace que los países que albergan las empresas tecnológicas y los servidores de Internet más importantes tengan la capacidad de "extraer ventajas informativas respecto de sus adversarios" e incluso de eliminar a determinados "adversarios de los flujos de la red" (Farrell y Newman, 2019:46). Debido al predominio de las empresas digitales de China y los Estados Unidos, así como al gran número de centros de datos de hiperescala ubicados en estos dos países (capítulo I), el volumen de datos que pasan por esas regiones supera los flujos de datos recibidos por todos los demás países (Mueller y Grindal, 2019)[67]. Por lo tanto, es lógico que algunos países traten de tener un mayor control de sus flujos de datos nacionales —y de infraestructuras físicas como los centros de datos, los cables submarinos y transatlánticos y los puntos de intercambio de tráfico de Internet— para protegerse de la vigilancia de otros países, reducir su dependencia de las redes extranjeras y mejorar su posición en la gobernanza mundial de Internet (Woods, 2018; Farrell y Newman, 2019; Ciuriak, 2019; Bagchi y Kapilavai, 2018; Hesselman y otros, 2020). Además, la localización de los datos suele facilitar las labores de inteligencia de los Estados (Selby, 2017) permitiéndoles mejorar el control sobre los asuntos internos, lo que puede considerarse una ventaja reguladora para algunos países.

Al elaborar una normativa sobre los flujos de datos, los Estados deben escoger con cuidado sus herramientas y utilizar con moderación las medidas de localización estrictas (por ejemplo, limitándolas a sectores muy sensibles y redactándolas con claridad) para evitar consecuencias negativas desde el punto de vista económico, social, político y tecnológico, y aumentar las posibles ventajas reguladoras. Por ejemplo, los Estados pueden utilizar una medida que exija la localización de todos los datos personales para vigilar y perseguir ilegalmente a los disidentes u opositores políticos, lo que contraviene las normas internacionales de derechos humanos (Freedom House, 2020). Por otro lado, puede haber motivos que justifiquen la restricción de los flujos de datos a un país con antecedentes conocidos de ciberdelincuencia y violaciones de la privacidad. Además, el análisis de los costos y beneficios de la normativa sobre los flujos de datos debe tener en cuenta los costos del control de la red y la infraestructura de datos, especialmente en el caso de las economías en desarrollo más pequeñas. Una preocupación fundamental es que una normativa injustificadamente compleja sobre los flujos de datos pueda dar lugar a la asunción prematura de cargas, y desvíe los recursos que deberían destinarse a funciones del Estado más importantes. Además, como se señala más adelante, las normativas sobre datos que interfieren con la arquitectura de red subyacente (por ejemplo, los protocolos de enrutamiento de datos), como las medidas de localización forzada, pueden

[66] Por ejemplo, el Acuerdo Transfronterizo de Privacidad del APEC, uno de los pocos marcos disponibles, es un sistema completamente voluntario. Véase APEC, *Cross-Border Privacy Enforcement Arrangement*, 2015 (disponible en www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement).

[67] *Nikkei Asia*, 24 de noviembre de 2020, "China Rises as World's Data Superpower as Internet Fractures" (disponible en https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures?utm_source=CSIS+All&utm_campaign%E2%80%A6).

causar graves perjuicios a la gobernanza mundial de Internet, en particular aumentar los riesgos que afectan a la seguridad de los datos y a otros aspectos de la gestión de estos. Estos riesgos son especialmente graves para los países que carecen de una infraestructura nacional de datos y redes sólida.

b) Perspectiva económica: necesidades y riesgos relacionados con el desarrollo

Las normativas sobre los flujos de datos transfronterizos pueden estar estrechamente vinculadas a los objetivos de desarrollo económico, especialmente en el caso de las economías emergentes y en desarrollo. Para encontrar la mejor manera de aprovechar las oportunidades que ofrecen los sectores impulsados por los datos a los países, los Gobiernos deben tener en cuenta diversos factores —como su nivel de preparación digital, las capacidades tecnológicas autóctonas, la infraestructura digital y normativa, el tamaño de sus mercados y la identificación de nichos de mercado— en los que las empresas nacionales emergentes tienen más probabilidades de éxito que sus homólogas extranjeras (UNCTAD, 2017 y 2019a).

Las normas restrictivas, como las medidas de localización o los requisitos estrictos de transferencia condicionada de datos, pueden conducir a la ineficiencia económica. Por ejemplo, los países que compitan en esos mercados quizá tengan que destinar una importante cantidad de recursos a replicar o almacenar los datos en centros de datos locales y reestructurar sus operaciones de datos para ajustarse a las leyes nacionales (Bennett y Raab, 2020; Internet Society, 2020c). En América Latina se ha comprobado que las disposiciones relativas a la localización de los datos son uno de los principales factores que limitan el crecimiento del sector de las tecnofinanzas (Aguerre, 2019). Es probable que en los países que carecen de infraestructuras suficientes (y con costos de electricidad elevados), los centros de datos locales sean también menos fiables y seguros y generen escasos beneficios económicos para la economía nacional (Chander y Lê, 2015; Leviathan Security Group, 2015), aunque dichos países podrían obtener ventajas de la mejora de otras infraestructuras (como se analiza en el capítulo III). Además, las empresas multinacionales suelen mostrarse reacias a ubicar sus centros de datos en países con antecedentes conocidos de vigilancia ilegal o prácticas de ciberseguridad inseguras (Lee, 2018), o con escasas competencias en el mercado nacional (Badran, 2018; African Union, 2020). Otros estudios también han demostrado que las restricciones a los flujos de datos transfronterizos pueden reducir la productividad y la rentabilidad económica en varios sectores, incluidas las industrias manufactureras (Bauer y otros, 2016). La localización puede incluso afectar negativamente a las empresas nacionales, especialmente a las más pequeñas, que dependen de que las instalaciones y servicios de almacenamiento de datos mantengan precios competitivos.

Al mismo tiempo, en determinadas situaciones, el almacenamiento local de los datos puede ser una solución conveniente en términos de costos, eficiencia y rendimiento; por ejemplo, para aplicaciones como los dispositivos de control de la salud o los vehículos autónomos, el acceso inmediato a los datos y la capacidad de respuesta rápida son aspectos que se pueden conseguir mediante el almacenamiento local de los datos (Komaitis, 2017). Se podrían aportar razones similares en favor del uso de soluciones de *software* como servicio (SaaS) en el marco de la computación en la nube, ya que el acceso en tiempo real facilitado por las soluciones de almacenamiento local puede mejorar la calidad de los servicios digitales que se ofrecen a las empresas nacionales más pequeñas (Kathuria y otros, 2019). Además, los costos de latencia y ancho de banda necesarios para transmitir volúmenes enormes de datos para las tecnologías de nueva generación —como los productos de la Internet de las cosas— a través de largas distancias podrían resultar significativamente más elevados que los necesarios para almacenar los datos a nivel local. Estas soluciones de almacenamiento local no solo podrían ser rentables, sino también cumplir otros objetivos de los órganos reguladores, como reducir la dependencia de los servicios en la nube extranjeros y garantizar la privacidad y la seguridad[68]. Por lo tanto, existen algunos incentivos económicos para facilitar el almacenamiento local de los datos en los países en desarrollo, especialmente en África y América Latina.

Algunos estudios han mostrado que las restricciones a los flujos de datos transfronterizos pueden favorecer el éxito económico en contextos muy específicos. Por ejemplo, China ha desarrollado su sector digital con un gran éxito, pero este no puede atribuirse únicamente a sus estrictas leyes de localización de los datos, sino a diversos factores, como el enorme tamaño de su mercado, las intervenciones estratégicas del

[68] Véase "What is edge computing and why it matters", 13 de noviembre de 2019 (disponible en https://www.networkworld.com/ article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html).

Estado para aumentar las inversiones en el sector digital, su gran capacidad reguladora y la disponibilidad de recursos tecnológicos. Asimismo, un estudio realizado en la India puso de manifiesto que —debido al tamaño inusualmente grande del mercado, junto con la presencia de empresas tecnológicas emergentes y de un número adecuado de especialistas en ingeniería— la localización puede disminuir la presión de los competidores extranjeros y mejorar las oportunidades de mercado para las empresas nacionales. Sin embargo, el estudio también permitió constatar que estas medidas conllevan perjuicios para los consumidores, como la reducción de la oferta, el aumento de los precios o la disminución de la calidad de los servicios digitales (Potluri y otros, 2020). Otro estudio realizado en la India (Kathuria y otros, 2019) mostró que los requisitos de localización de los datos implicarían costos elevados, especialmente para los servicios de comunicaciones y financieros, ya que las opciones nacionales no eran tan eficientes o rentables como los servicios en la nube proporcionados por Amazon y Google. Algunos de los costos de la migración a centros de datos nacionales pueden repercutirse en los consumidores. No obstante, el estudio también apuntó a la posibilidad de que, con la apertura de un mayor número de centros de datos de empresas extranjeras en la India, la calidad de los servicios basados en la nube disponibles para las empresas nacionales experimentase una mejora en el futuro.

Al elaborar sus normativas sobre los flujos de datos, los países deberían tener en cuenta los marcos más adecuados a sus necesidades de desarrollo digital. En ese sentido, los modelos de desarrollo digital adoptados por China y la India podrían no ser adecuados para otros países en desarrollo y PMA con mercados más pequeños, capacidades digitales limitadas y una capacidad reguladora restringida. Por ejemplo, las mipymes de las economías en desarrollo más pequeñas podrían tener más oportunidades de crecer si utilizan plataformas digitales internacionales y servicios en la nube, en lugar de plantearse soluciones locales (Chen y otros, 2019). En América Latina, varios responsables políticos y empresariales han reconocido que hay más posibilidades de obtener beneficios de la economía digital si se opta por integrar las pequeñas y medianas empresas (pymes) en la cadena mundial de suministro, en lugar de crear empresas unicornio digitales nacionales recurriendo a medidas proteccionistas (Aguerre, 2019). Además, especialmente en los mercados más pequeños, los conjuntos de datos muy localizados pueden no resultar muy útiles para la creación de macrodatos y productos de IA de alta calidad, que por naturaleza se basan en el volumen, la velocidad y la variedad de los datos[69]. Por lo tanto, en estos mercados pequeños, si el Estado trata de crear referentes de datos locales restringiendo los flujos de datos, puede acabar reduciendo la calidad y la funcionalidad de los productos y servicios digitales disponibles a nivel nacional, y perjudicando con ello a los consumidores (Potluri y otros, 2020; Aguerre, 2019). Por último, en el caso de los mercados pequeños con políticas estrictas de localización de los datos y una gobernanza e infraestructura deficientes, algunas empresas extranjeras pueden decidir abstenerse de acceder al mercado para evitar los riesgos y los costos derivados de dichas políticas (WEF, 2020b).

En cambio, los países que adoptan una legislación firme en materia de protección de datos sin imponer restricciones injustificadas o inviables a los flujos de datos transfronterizos pueden ser más atractivos para las empresas extranjeras (Kuner, 2013). Los países con una reputación sólida de buena infraestructura reguladora, lo que incluye entornos empresariales de confianza, pueden beneficiarse de mayores flujos de datos y, en última instancia, obtener acceso a datos de mayor calidad en el futuro (Open Data Institute, 2019b; Chen y otros, 2019). Además, el cumplimiento de las políticas estrictas de localización de los datos y las normativas complejas sobre datos que tienen por objetivo limitar el poder de las grandes empresas tecnológicas en realidad puede ser más asumible para esas grandes empresas que para las empresas más pequeñas con recursos limitados (Christakis, 2020). Un buen ejemplo de esta paradoja es la incapacidad de algunas mipymes para operar en la Unión Europea debido a los complejos requisitos previstos en el RGPD (Martin y otros, 2019). Por lo tanto, los países deben tratar de evitar normativas sobre datos que puedan afectar negativamente al crecimiento de las empresas más pequeñas o perjudicar los intereses de los consumidores en su economía nacional.

No obstante, al mismo tiempo, los países en desarrollo deben seguir gozando de libertad para llevar a cabo intervenciones adecuadas con el fin de promover el crecimiento digital, mejorar sus capacidades

[69] El volumen, la velocidad y la variedad son las cualidades de los datos que más se mencionan en las publicaciones especializadas. Véase, por ejemplo, *ZdNet*, 21 de marzo de 2018, "Volume, velocity, and variety: Understanding the three V's of big data". Sin embargo, se han destacado otras muchas características en relación con los datos; véase, por ejemplo, Kitchin y McArdle (2016) y Arockia y otros (2017).

en materia de datos y facilitar el desarrollo digital inclusivo a nivel nacional. Esto garantizaría un acceso equitativo a los datos para las empresas nacionales, así como una distribución justa de las ganancias en su economía. Por ejemplo, los Estados pueden promover el desarrollo de las empresas nacionales que gocen de una ventaja competitiva en determinados sectores impulsados por los datos (por ejemplo, la capacidad de ofrecer soluciones personalizadas basadas en el idioma o las preferencias culturales), o incentivar la inversión en las capacidades nacionales en materia de datos para allanar el terreno a las tecnologías digitales de nueva generación. Asimismo, algunos países podrían optar por gravar impuestos digitales a las empresas extranjeras que utilizan los datos de su ciudadanía, o garantizar un acceso equitativo a los datos y la interoperabilidad mediante la aplicación de las leyes de competencia pertinentes, a fin de mejorar las posibilidades competitivas de las empresas nacionales.

c) *Perspectiva tecnológica: consecuencias para la gobernanza mundial de los datos*

La gobernanza de los flujos de datos transfronterizos está inextricablemente ligada a la gobernanza mundial de los datos e Internet. Las empresas que almacenan y procesan los datos en servidores distribuidos por todo el mundo obtienen distintos beneficios en términos de eficiencia tecnológica, como una mejor protección contra la pérdida de datos y la piratería informática, y la garantía de acceso oportuno a los datos, por ejemplo mediante el uso de cachés de borde para almacenar el contenido más cerca de los usuarios finales[70]. Además, los flujos de datos transfronterizos también facilitan el cumplimiento de las normas internacionales básicas de derechos humanos, como la libertad de expresión y el acceso a los datos (Taylor, 2020). Distintas voces expertas de la comunidad de Internet han expresado preocupación, sobre todo por las medidas de localización forzada, ya que pueden reducir la resiliencia y el rendimiento de las redes de Internet (que no se construyeron para ceñirse a las fronteras territoriales), afectar a la integridad de los protocolos subyacentes (por ejemplo, para el enrutamiento y la transferencia de datos) y obstaculizar la apertura y la accesibilidad universal inherentes a Internet (Internet Society, 2020c; Komaitis, 2017; Dai y otros, 2016). Además, como se explica en el capítulo IV, la creciente fragmentación digital y de Internet resultante de la falta de consenso mundial sobre la gobernanza de los flujos de datos, las tensiones tecnológicas entre las principales potencias digitales, como los Estados Unidos y China, y los modelos de regulación contrapuestos en materia de flujos de datos serán especialmente perjudiciales para los países en desarrollo y afectarán negativamente a su bienestar y crecimiento económicos en los próximos años.

En el cuadro V.2. se presenta un resumen de los objetivos y riesgos de los diferentes tipos de normativas sobre los flujos de datos transfronterizos desde una perspectiva reguladora, de desarrollo económico y de gobernanza mundial de los datos.

En conclusión, los Estados deben evaluar cuidadosamente tanto los beneficios como los costos que pueden resultar de la regulación de los flujos de datos transfronterizos. Los países tienen motivos políticos diversos para regular los flujos de datos transfronterizos, como proteger los intereses vitales de la ciudadanía, lo que incluye garantizar la privacidad de las personas y la seguridad de los flujos de datos. Algunos Estados consideran que la regulación de los datos es una herramienta importante para estimular el desarrollo económico, crear oportunidades competitivas para las empresas nacionales y garantizar una distribución equitativa de las ganancias dentro del país. En otros casos, el Estado considera que cierta regulación es necesaria debido a la inexistencia de mecanismos internacionales adecuados para hacer cumplir en otros países sus leyes de privacidad/protección de datos. Por último, dependiendo de sus contextos políticos y socioculturales, algunos países pueden optar por regular estrictamente los flujos de datos transfronterizos para garantizar la seguridad nacional o mantener un mayor control político dentro de sus fronteras. Ante la falta de consenso internacional sobre un marco regulador de los flujos de datos a nivel mundial, muchos países se ven obligados a adoptar normativas y políticas restrictivas sobre los flujos de datos para hacer frente a los fallos del mercado de la economía digital y proteger sus intereses económicos y políticos nacionales. A largo plazo, tanto la regulación insuficiente como la regulación excesiva de los flujos de datos transfronterizos conducen a resultados insatisfactorios, por lo que el diálogo y la elaboración de políticas sobre los flujos de datos a escala internacional siguen siendo muy deseables para encontrar otras soluciones políticas que favorezcan el desarrollo.

[70] *Lawfare*, 22 de mayo de 2017, "Where Is Your Data, Really? The Technical Case Against Data Localization" (disponible en https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization).

Cuadro V.2. Objetivos y riesgos de las restricciones de los flujos de datos transfronterizos

Objetivos	Riesgos
Garantizar la protección de los datos y la privacidad	Agravar la incertidumbre de las empresas
Reducir los riesgos relacionados con la seguridad y proteger los datos críticos del Estado de la injerencia extranjera	Aumentar los costos de cumplimiento que asumen las empresas, lo que resulta especialmente inasequible para las mipymes
Crear uno o dos referentes locales en materia de datos en las economías más grandes (aunque quizá no siempre sean suficientemente competitivos)	Es posible que la supervisión y la aplicación resulten costosas para los reguladores
Facilitar la tramitación de denuncias de vulneración de la privacidad de los usuarios por empresas extranjeras en el marco de la legislación nacional, por ejemplo con arreglo a leyes de protección de datos	Es posible que aumenten los precios al consumo y/o disminuya la oferta para los consumidores, incluidas las empresas nacionales, en los mercados menos competitivos
Permitir una supervisión más estricta de los sectores sensibles por el órgano regulador	Pueden facilitar la vigilancia ilegal del Estado y la vulneración del derecho a la privacidad de las personas
Facilitar el acceso de los reguladores a los datos a fin de garantizar la aplicación de la ley	Pérdida de datos en el contexto de desastres naturales, cuando se impone la localización obligatoria de los datos
Reducir la dependencia de las redes y servicios extranjeros, y abordar las preocupaciones de soberanía digital	Dificultar la detección de fraudes, por ejemplo en los servicios de pago electrónico
Reducir los costos de latencia y de ancho de banda de la transmisión de datos a larga distancia	Pueden afectar a la arquitectura de red y reducir la interoperabilidad de Internet
	Asunción prematura de cargas por los PMA (por ejemplo, cuando las normativas son demasiado complejas)
	Pueden crear una falsa impresión de confianza y seguridad en el ecosistema nacional

Fuente: UNCTAD.

C. ESQUEMA DE LAS NORMATIVAS NACIONALES SOBRE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

Partiendo del examen de los marcos normativos nacionales sobre los flujos de datos transfronterizos, en esta sección se procede a situar los países analizados en este capítulo en un espectro condicionado por el grado de restricción general de los flujos de datos transfronterizos (teniendo en cuenta tanto el alcance como la profundidad de las medidas reguladoras pertinentes en cada país). A continuación se ofrecen algunas perspectivas de alto nivel sobre las tendencias en lo que respecta a la regulación de los flujos de datos transfronterizos.

1. Espectro normativo de los flujos de datos transfronterizos

El espectro normativo de los flujos de datos transfronterizos, empezando por el nivel más bajo de restricción, abarca los siguientes enfoques:

- *Enfoque de baja injerencia:* implica que, en general, todos los datos, incluidos los datos personales, pueden circular libremente a través de las fronteras con unos requisitos mínimos (en caso de que los haya), y por tanto se refiere a las medidas que imponen el menor número de restricciones a los flujos de datos transfronterizos, es decir, la libre circulación de los datos. Los Estados Unidos destacan como el principal defensor de este enfoque. Otras economías —como México, Australia y Singapur— también se ajustan en mayor o menor medida a este enfoque. Los países que adoptan un enfoque de baja injerencia pueden imponer, no obstante, ciertas restricciones excepcionales a los flujos de datos transfronterizos, por ejemplo, en sectores sensibles como la defensa o la sanidad.

- *Enfoque normativo prescriptivo:* implica que los flujos de datos transfronterizos están sujetos a requisitos rigurosos, por ejemplo, en las leyes nacionales de protección de datos/privacidad. La mayoría de los países de esta categoría tienden a centrarse en los datos personales. El enfoque prescriptivo se sitúa en el centro del espectro normativo y suele incluir requisitos de transferencia condicionada. La Unión Europea es el ejemplo más conocido de este enfoque en el contexto de las transferencias transfronterizas de datos personales. Como ya se ha comentado, otros países han empezado también a imponer requisitos estrictos a las transferencias transfronterizas de datos personales en sus leyes de protección de datos/privacidad.
- *Enfoque normativo restrictivo:* implica la prohibición total o parcial de los flujos de datos transfronterizos por razones de seguridad pública o seguridad nacional y el establecimiento de un control político absoluto sobre Internet en el territorio nacional, lo que incluye los datos a los que accede y que produce la ciudadanía. Suele denominarse "soberanía sobre los datos".
- Por último, algunos países adoptan un *enfoque cauteloso*: ante el desigual impacto económico de la digitalización mundial ilimitada de la economía, estos países adoptan las medidas reguladoras necesarias para poder obtener beneficios económicos significativos de la economía digital, poniendo así en manos del país y de su pueblo la llave de su futuro digital y su desarrollo (Jain y Gabor, 2020). Tanto el enfoque restrictivo como el cauteloso tienden a favorecer principalmente la adopción de medidas de localización, aunque sus principales motivaciones políticas son bastante distintas.

La diferencia entre los enfoques cauteloso, restrictivo y prescriptivo no siempre está clara en la práctica; por ejemplo, las economías emergentes, que tienen una mayor capacidad reguladora, pueden optar por imponer requisitos normativos más estrictos, en lugar de medidas de localización, para proteger los datos personales. Además, la imposición de algunos requisitos muy prescriptivos a los flujos de datos transfronterizos puede equivaler en la práctica a un enfoque restrictivo cuando, básicamente, se prohíben dichos flujos. Asimismo, es posible que algunos países que adoptan un enfoque cauteloso para obtener la mayor cantidad posible de beneficios económicos pretendan también tomar el control político de los datos nacionales y viceversa. Por último, los países que adoptan un enfoque de baja injerencia pueden imponer requisitos de localización en sectores sensibles.

Estos enfoques suelen relacionarse con tipos concretos de medidas reguladoras en función de su grado de restricción, por lo que pueden ajustarse al tipo de medida o medidas correspondientes, como se muestra en la siguiente sección.

2. Esquema de las normativas sobre los flujos de datos transfronterizos en el espectro regulador

Esta sección se centra en el modo en que los marcos reguladores sobre los flujos de datos transfronterizos se están aplicando en todo el mundo. En el cuadro V.3 se ofrece un panorama general de los marcos reguladores y se elabora un esquema de las diferentes economías con relación al espectro regulador tomando como base el examen de las leyes, normativas y políticas nacionales pertinentes en lo que respecta a los flujos de datos transfronterizos. Respecto del enfoque prescriptivo (centro del espectro), en el cuadro se distingue entre los países que imponen requisitos condicionales flexibles o intermedios para los flujos de datos transfronterizos (lo que los hace menos prescriptivos; véase el lado derecho del espectro) y los que imponen requisitos condicionales estrictos (lo que los hace más prescriptivos; véase el lado izquierdo del espectro). Además, dado que tanto el enfoque cauteloso como el restrictivo se basan principalmente en medidas de localización, ambos figuran en el extremo izquierdo del espectro; no obstante, en el cuadro se indica el enfoque específico de cada país para mayor claridad.

Mientras que solo unos pocos países han optado por un enfoque de escasa injerencia o restrictivo/cauteloso, la mayor parte de los países que figuran en el cuadro V.3 han adoptado algún tipo de marco regulador prescriptivo sobre los flujos de datos transfronterizos. Las economías con un enfoque prescriptivo están repartidas por todas las regiones y presentan diferentes niveles de desarrollo: Argelia, Argentina, Bahrein, Belarús, Brasil, Colombia, Côte d'Ivoire, Israel, Malasia, Túnez y Unión Europea, por nombrar algunas. En estos casos, en lugar de restringir por completo los flujos de datos transfronterizos,

Cuadro V.3. Esquema de las normativas sobre los flujos de datos transfronterizos

Localización de datos estricta	Localización de datos parcial	Transferencia condicionada: estricta	Transferencia condicionada: intermeda/flexible	Libre circulación de los datos
Enfoque restrictivo (R) o cauteloso (C)		Enfoque prescriptivo		Enfoque de baja injerencia
Arabia Saudita (R)		Algeria	Azerbaiyán	Australia
China (R)		Argentina	Bahrein	Canadá
Federación de Rusia (R)		Armenia	Belarús	Estados Unidos
India (C)		Brasil	Emiratos Árabes Unidos	Filipinas
Indonesia (R/C)		Colombia	Ghana	México
Kazajstán (R)		Côte d'Ivoire	Japón	Singapur
Nigeria (R)		Egipto	Kirguistán	
Pakistán (R/C)		Georgia	Nueva Zelandia	
Rwanda (C)		Israel	República de Corea	
Turquía (R)		Kenya		
Viet Nam (R)		Malaysia		
		Marruecos		
		Perú		
		Reino Unido		
		Sudáfrica		
		Suiza		
		Tailandia		
		Túnez		
		Ucrania		
		Unión Europea		

Fuente: UNCTAD.
Nota: La lista de normativas examinadas figura en el anexo en línea del capítulo V (disponible en https://unctad.org/system/files/official-document/der2021_annex2_en.pdf).

las normativas incorporan requisitos para las transferencias de datos transfronterizas (normalmente para los datos personales). Estos requisitos pueden ser desde muy prescriptivos hasta moderadamente prescriptivos, generalmente en función de los intereses y objetivos reguladores específicos de cada país: enfoque de adecuación estricto (junto con excepciones limitadas); mecanismos contractuales o de certificación aprobados para las transferencias transfronterizas de datos; evaluación caso por caso de las transferencias de datos por el órgano regulador; transferencias de datos basadas en el consentimiento (ya sea expreso o implícito); y transferencias basadas en consideraciones jurídicas (por ejemplo, el cumplimiento de la legislación nacional o de un tratado internacional), o para proteger intereses públicos esenciales. En particular, la mayor parte de los marcos reguladores prescriptivos se refieren a los datos personales; sin embargo, como se indicó anteriormente, estas normativas pueden tener una aplicación amplia, ya que la mayoría de los conjuntos de datos contienen un mínimo de datos personales identificables. A pesar de la falta de consenso internacional sobre la protección de datos y la privacidad, varios países están adoptando o actualizando sus leyes de protección de datos conforme a algunos principios comunes, como los establecidos en el RGPD[71].

[71] De 120 países no pertenecientes a la Unión Europea, 67 han adoptado una legislación similar al RGPD (Srikrishna Committee Report, 2018).

En el cuadro V.3 también se observan otras tendencias reguladoras. En primer lugar, son pocos los países que han adoptado un enfoque de baja injerencia. Este enfoque parece ser elegido mayoritariamente por países con entornos reguladores sólidos y recursos de regulación suficientes para supervisar el cumplimiento de las leyes nacionales, especialmente por las grandes empresas extranjeras. Además, economías como Australia, Singapur y el Canadá han sido tradicionalmente economías abiertas y liberales, por lo que no extraña que adopten un enfoque de baja injerencia en lo que respecta a los flujos de datos transfronterizos. La dependencia de la economía de Filipinas del sector de la subcontratación puede explicar que el país haya adoptado un enfoque de baja injerencia. Por último, los Estados Unidos, por ser una de las principales potencias digitales y un firme defensor de la Internet libre y abierta, son partidarios de este enfoque.

En segundo lugar, el enfoque restrictivo, adoptado por China y la Federación de Rusia desde principios de este siglo, es cada vez más popular en otros países en desarrollo, como Turquía, Viet Nam, Kazajstán y el Pakistán. En estos países, la protección de datos suele hacer referencia a la seguridad de los datos/información más que a la protección del derecho a la privacidad de los particulares. El contexto político y sociocultural específico suele ser la razón principal de que se adopte un enfoque restrictivo. Por ejemplo, en los países menos democráticos puede existir una mayor tendencia al control soberano de las actividades de la ciudadanía, lo que incluye los contenidos disponibles en Internet, así como la expresión de ideas en línea (Freedom House, 2020a)[72]. Esta forma de regulación de los datos ha suscitado una gran preocupación en la comunidad internacional, especialmente por lo que respecta a los derechos humanos.

Por último, algunas economías digitales emergentes, entre las que destaca la India, parecen estar optando por un enfoque cauteloso. Aunque algunas normativas sobre datos pueden beneficiar de forma indirecta al sector nacional (por ejemplo, al hacer más engorroso el procesamiento de datos en el extranjero), la mayor parte de los países no imponen normas para restringir los flujos de datos con el objetivo principal de proteger su sector nacional de la competencia extranjera. Las políticas de restricción de los flujos de datos transfronterizos pueden dar resultados satisfactorios en algunos contextos, pero no son una solución milagrosa para todas las economías en desarrollo. Por ejemplo, puede que algunos países en desarrollo no dispongan de la capacidad adecuada para crear plataformas digitales locales de alta calidad y, por lo tanto, quizá tengan más posibilidades de desarrollo económico si adoptan normativas para facilitar las transferencias de datos transfronterizas que sean seguras y respeten la privacidad, de manera que las empresas locales puedan acceder a los servicios prestados por las plataformas digitales extranjeras. El diseño de estas normativas dependerá de la cultura reguladora y los recursos del país, la creación de valor local que se requiera de la economía digital y otras consideraciones, como la conectividad digital y la interdependencia con los mercados digitales mundiales.

Los países pueden ir pasando de un grupo a otro; por ejemplo, con la mejora de los recursos reguladores, un país que aplica un enfoque "cauteloso" puede pasar a adoptar un enfoque "prescriptivo" para reducir al mínimo las pérdidas económicas e integrarse mejor en la economía digital mundial. Los países con una regulación mínima o nula de los flujos de datos transfronterizos pueden actualizar sus leyes para adoptar enfoques más prescriptivos, cautelosos o restrictivos en función de sus necesidades económicas y políticas específicas.

D. CONCLUSION

Los países regulan los flujos de datos transfronterizos teniendo en cuenta diversos intereses políticos que conciernen a diferentes esferas de la acción reguladora del Estado, a menudo con el objetivo de lograr una serie de resultados que se basan en una compleja interacción de factores nacionales e internacionales. En muchos casos, los flujos de datos transfronterizos se regulan por motivos legítimos desde el punto de vista de la soberanía nacional que, en la mayoría de los casos, se basan en la protección de la

[72] Véase, en general, Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (A/HRC/38/35); Human Rights Watch, 23 de abril de 2020, "Vietnam: Facebook, Pressured, Censors Dissent" (disponible en www.hrw.org/news/2020/04/23/vietnam-facebook-pressured-censors-dissent).

ciudadanía, la seguridad nacional y la promoción del desarrollo económico nacional. Sin embargo, existen diferencias entre los países en función de la prioridad que otorgan a cada una de estas razones. Las normativas sobre los flujos de datos transfronterizos pueden encontrarse en diferentes tipos de leyes y reglamentos. Los diversos instrumentos normativos nacionales sobre los flujos de datos transfronterizos que se analizan en este capítulo comprenden: leyes de protección de datos; leyes, reglamentos y políticas sobre ciberseguridad; leyes y reglamentos sobre Internet; reglamentos sobre *hardware* y *software*; leyes de contratación pública; leyes relacionadas con la protección de secretos de Estado; leyes del impuesto sobre la renta; leyes y reglamentos sobre las empresas y la contabilidad; políticas relacionadas con el comercio electrónico y el desarrollo digital; y estrategias de datos. Por tanto, al abarcar diferentes esferas de la acción política, el enfoque compartimentado de la regulación lleva a que se adopten medidas incoherentes en diferentes ministerios. Esto pondría de manifiesto la necesidad de adoptar un enfoque pangubernamental de la gobernanza de los flujos de datos transfronterizos.

Al evaluar la pertinencia de los distintos marcos reguladores en el ámbito nacional, las instancias normativas deberían tener en cuenta diversos factores de manera integral. A nivel nacional, los países deben tener en cuenta su situación económica, sus preferencias políticas y socioculturales, su capacidad de regulación interna y su estado de desarrollo tecnológico. Desde una perspectiva transnacional/mundial, los países deben tener en cuenta la política exterior que desean desarrollar, lo que incluye sus relaciones/compromisos comerciales internacionales, su grado de integración con la economía digital mundial y, más ampliamente, la arquitectura distribuida de Internet y la naturaleza mundial de algunos problemas normativos relacionados con Internet. En última instancia, la decisión sobre cuál es el modelo adecuado para regular los flujos de datos en cada país sigue siendo una cuestión política compleja. Este ejercicio de equilibrio integral es especialmente necesario para que las economías en desarrollo puedan aprovechar al máximo los beneficios potenciales de la economía digital y garantizar un mayor grado de bienestar a su ciudadanía.

En conjunto, los capítulos IV y V muestran que los marcos reguladores nacionales sobre los flujos de datos transfronterizos son extremadamente diversos y evolucionan rápidamente con el aumento de la digitalización de la economía mundial. La diversidad de enfoques, medidas y motivaciones dificulta la tarea de encontrar pautas normativas entre los países, aunque se puede intentar realizar mediante el examen de sus motivaciones económicas y características. Entre los países desarrollados, hay un país grande y con un alto nivel de desarrollo —los Estados Unidos— que alberga plataformas digitales globales con un gran poder de mercado y propugna la libre circulación de los datos a través de las fronteras para que esas empresas puedan obtener los máximos beneficios de los datos recopilados en sus operaciones en todo el mundo. Los países desarrollados más pequeños, cuyos mercados internos no son suficientemente grandes para beneficiarse de las restricciones, tienden a apoyar la libre circulación de los datos a través de las fronteras. La Unión Europea es un caso particular, ya que prioriza aspectos como la privacidad y la protección de datos. Entre los países en desarrollo, los que tienen mercados nacionales grandes se muestran mayoritariamente a favor de la localización de los datos para promover el desarrollo de sus economías digitales. En el caso de China, las razones de seguridad nacional también tienen un papel importante. En cuanto al resto, que son países en desarrollo más pequeños, el panorama es variado. Es probable que la localización de los datos no sea útil, dado el pequeño tamaño de sus mercados, pero la libre circulación de los datos a través de las fronteras implica entregar un recurso nacional sin obtener nada a cambio.

Las principales razones de esta diversidad son la inexistencia de un marco normativo internacional en esferas clave de la regulación de los datos (como la privacidad y la protección de datos, la ciberseguridad y la regulación de los contenidos en línea), así como las preocupaciones relacionadas con la distribución equitativa de los beneficios en la economía digital. Además, las preferencias políticas, culturales y económicas particulares de cada país, junto con su estado de desarrollo tecnológico/digital, afectan profundamente al diseño de la normativa nacional sobre los flujos de datos transfronterizos. Por ejemplo, un país con fuertes valores comunitarios puede atribuir a la privacidad un significado diferente del que le daría uno que hace especial hincapié en la vida privada; esta diferencia de perspectivas podría conducir a enfoques contrapuestos en lo que respecta a la regulación de los flujos transfronterizos de datos personales. Asimismo, determinados sectores —como la sanidad, la administración pública o las finanzas— pueden considerarse más sensibles en algunos países que

en otros, lo que daría lugar a una regulación más estricta de dichos sectores. Por último, algunos países pueden tener condiciones óptimas para desarrollar su sector digital nacional mediante políticas industriales específicas, por lo que tenderían a imponer restricciones en los sectores en que consideren que tienen una ventaja competitiva.

No obstante, aunque la creciente importancia económica de los datos para el desarrollo ha dado lugar a una mayor regulación de los flujos de datos transfronterizos (principalmente en forma de medidas de localización de los datos, cuyos beneficios no son tan evidentes), son pocos los países que cuentan con estrategias adecuadas para desarrollar su economía digital y procesar sus datos a nivel nacional. Algunas excepciones son India Digital y el Nuevo Proyecto de Política Nacional de Datos y Servicios en la Nube de Sudáfrica. Como se explicó en el capítulo III, el acceso a los datos es una condición necesaria pero no suficiente para el desarrollo; también es necesario desarrollar capacidades nacionales para procesar los datos y convertirlos en inteligencia digital que pueda ser monetizada o utilizada con valor social.

> Las normativas sobre los flujos de datos transfronterizos deberían lograr un equilibrio integrador entre las necesidades de desarrollo digital particulares del país, su capacidad reguladora y tecnológica y las consideraciones relativas a sus relaciones exteriores.

Dada la variedad de aspectos que condicionan la regulación de los flujos de datos transfronterizos, no es probable que trasplantar ciegamente los modelos normativos de gobernanza de los datos de los países desarrollados a los países en desarrollo, e incluso de un país en desarrollo a otro, produzca resultados deseables. Más bien, las circunstancias específicas de cada país deberían ser un factor fundamental al determinar el modo en que este regula los flujos de datos. Por lo tanto, no tiene mucho sentido defender ni la adopción de políticas de localización estrictas y generalizadas que puedan ser económica y tecnológicamente ineficientes, ni los flujos de datos sin restricciones, sin las garantías de privacidad y seguridad necesarias y sin prestar la debida atención a las preocupaciones relacionadas con el desarrollo económico y la distribución equitativa de las ganancias obtenidas de la economía digital. Además, los diferentes países deberían poder optar por marcos normativos prescriptivos (por ejemplo en sus leyes nacionales de protección de datos y ciberseguridad) en función de sus capacidades reguladoras específicas y de las necesidades de sus políticas nacionales.

Idealmente, las normativas sobre los flujos de datos transfronterizos deberían lograr un equilibrio integrador entre las necesidades de desarrollo digital particulares del país, su capacidad reguladora y tecnológica y las consideraciones relativas a sus relaciones exteriores, como la forma en que el país puede integrarse de forma significativa en la economía digital mundial y adoptar las normas y soluciones políticas pertinentes para abordar problemas mundiales en relación con Internet, en particular los problemas relacionados con la protección transnacional de la privacidad en la red y la ciberseguridad. Dada la relevancia de los objetivos políticos que inspiran la mayor parte de las normativas sobre los flujos de datos transfronterizos, un enfoque universal parece inviable e indeseable. Es importante que todos los países busquen, tanto individual como colectivamente, las herramientas más eficaces y equitativas —y menos perturbadoras— para regular los flujos de datos transfronterizos. Además, la naturaleza dinámica de la economía digital impulsada por los datos requiere que todos los países (ya sean desarrollados o en desarrollo) reformulen constantemente sus decisiones políticas sobre los flujos de datos transfronterizos, de modo que puedan encontrar un equilibrio óptimo entre la promoción del desarrollo económico nacional, la protección de los intereses esenciales de las políticas públicas y la garantía de un ecosistema digital mundial integrado. En este sentido, podría resultar útil contar con algún tipo de marco o instrumento normativo internacional de alto nivel que oriente a todos los países en lo que respecta a los flujos de datos transfronterizos contribuyendo a una mayor armonía entre sus respectivos marcos reguladores y mejorando la confianza, la interconectividad y la interoperabilidad en el ecosistema digital mundial. Sin embargo, como se explica

en el siguiente capítulo, los marcos reguladores regionales e internacionales no han logrado responder al desafío de permitir la circulación de los datos a través de las fronteras garantizando un reparto equitativo de los beneficios del desarrollo económico y, al mismo tiempo, abordar adecuadamente cuestiones como la privacidad, la protección de los derechos humanos y la seguridad nacional.

> Podría resultar útil contar con algún tipo de marco o instrumento normativo internacional de alto nivel que oriente a todos los países en lo que respecta a los flujos de datos transfronterizos contribuyendo a una mayor armonía entre sus respectivos marcos reguladores y mejorando la confianza, la interconectividad y la interoperabilidad en el ecosistema digital mundial.

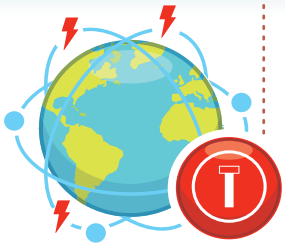
La expansión de los flujos de datos transfronterizos ha hecho que los Estados manifiesten un interés creciente por complementar su legislación nacional con compromisos a nivel regional e internacional. No obstante, hasta la fecha ha resultado difícil lograr un consenso, lo que refleja la existencia de diferentes prioridades y posiciones entre los países. Incluso entre los países del G20 existen puntos de vista contrapuestos, tanto en cuestiones de fondo como de forma.

Aunque inicialmente los debates regionales e internacionales en relación con los flujos de datos se centraron en la necesidad de proteger la privacidad, en los últimos tiempos la atención se ha trasladado a la esfera comercial. En la actualidad, cada vez son más los acuerdos comerciales bilaterales y regionales que incluyen cláusulas relacionadas con los datos y el comercio digital, y también se están celebrando negociaciones en el marco de la Iniciativa de Declaración Conjunta sobre el comercio electrónico en la Organización Mundial del Comercio. El presente capítulo pone de manifiesto que los enfoques internacionales y regionales de la regulación de los flujos de datos transfronterizos son o bien demasiado restringidos, al centrarse solo en aspectos como el comercio o la privacidad, o bien demasiado limitados geográficamente, como en el caso de los enfoques regionales. Se destaca que, para abordar los flujos de datos de forma integral y multidimensional, las normas mundiales en este ámbito deberán ir más allá del comercio, y tener en cuenta las dimensiones económicas y no económicas de los datos.

VI

ENFOQUES REGIONALES E INTERNACIONALES DE LA REGULACIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

CAPÍTULO VI LOS FLUJOS DE DATOS TRANSFRONTERIZOS ESTÁN CADA VEZ MÁS REGULADOS A NIVEL INTERNACIONAL, PERO NO SE ABORDAN DE MANERA INTEGRAL



Cada vez se presta una mayor atención a la gobernanza de los datos a nivel internacional. Sin embargo, las **opiniones y posiciones divergentes** en lo que respecta a su regulación han dado lugar a una situación de bloqueo en el debate político internacional sobre los flujos de datos transfronterizos

Los flujos de datos transfronterizos no son comercio y deben regularse de forma integral, teniendo en cuenta todas sus dimensiones

Acuerdos internacionales y regionales sobre flujos de datos

Sistema de comercio

Multilateral

- OMC/Iniciativa de Declaración Conjunta

Bilateral

Diversos acuerdos bilaterales de libre comercio y asociación económica

Otros

- Tratado Integral y Progresista de Asociación Transpacífico (TIPAT)
- Asociación Económica Integral Regional (RCEP)
- Acuerdo sobre el Comercio de Servicios
- Alianza del Pacífico
- Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC)

Otros acuerdos e iniciativas

- Directrices sobre privacidad de la OCDE
- Principios relativos a la formulación de políticas de Internet de la OCDE
- Convenio 108 y 108+ del Consejo de Europa
- Iniciativas sobre privacidad del Foro de Cooperación Económica de Asia y el Pacífico (APEC)
- Marcos relativos a los datos de la Asociación de Naciones de Asia Sudoriental (ASEAN)
- Convención de Malabo de la Unión Africana
- Acuerdo de Asociación de Economía Digital
- Red Iberoamericana de Protección de Datos (RIPD)
- Agenda digital para América Latina y el Caribe (eLAC)
- Circulación de Datos Libre y de Confianza del G20

Los marcos reguladores regionales e internacionales actualmente vigentes tienden a ser o demasiado restringidos en su alcance o demasiado limitados geográficamente, y no logran facilitar una circulación de los datos a través de las fronteras que resulte en un reparto equitativo de los beneficios para el desarrollo económico abordando a la vez adecuadamente los riesgos

ES NECESARIO ADOPTAR UN NUEVO MARCO REGULADOR

- Con miras a llegar a una solución de avenencia
- Que tenga en cuenta tanto la dimensión económica como la no económica

¿Qué foro internacional cuenta con más recursos para facilitar el desarrollo de la gobernanza mundial de los datos?

A. INTRODUCCIÓN

Como se indicó en el capítulo anterior, el aumento de las normativas nacionales en materia de datos es reflejo de la voluntad de los Estados de lograr diversos objetivos políticos. Al mismo tiempo, estas normativas suelen entrar en conflicto con la naturaleza mundial de Internet y de la economía digital, para las que resulta esencial que no existan obstáculos a las transferencias de datos a través de las fronteras. La proliferación de diferentes enfoques nacionales de la regulación de los flujos de datos transfronterizos podría contribuir a la fragmentación de Internet, lo que repercutiría en su correcto funcionamiento (capítulo IV), limitando los beneficios potenciales para el desarrollo resultantes de la compartición de datos. Los llamamientos a establecer mecanismos adecuados para la coordinación internacional de las normativas sobre los flujos de datos a fin de invertir esa tendencia son cada vez más numerosos (Leblond y Aaronson, 2019; Fay, 2019; Meltzer, 2019; véase también el capítulo VII). Sin embargo, no existe acuerdo sobre cuál es el foro apropiado para abordar esa gobernanza ni sobre el tipo de normas y métodos de aplicación necesarios para este fin. Las cuestiones relativas a los flujos de datos se han debatido en diversos foros bilaterales, regionales y multilaterales.

Los debates sobre los flujos de datos se iniciaron en la década de 1970 para abordar preocupaciones relacionadas con la privacidad. Los primeros resultados intergubernamentales llegaron en 1980, con las Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales[1], y en 1981, con el Convenio 108 del Consejo de Europa. Desde entonces, el tema de los flujos de datos ha ocupado un lugar importante en la agenda internacional, sobre todo en el contexto de la gobernanza de Internet, como en el marco del Grupo de Trabajo de las Naciones Unidas sobre la Gobernanza de Internet, creado en 2004, y más recientemente, en la esfera del comercio internacional.

En este capítulo se examina la evolución de la regulación de los flujos de datos transfronterizos a escala regional e internacional, prestando especial atención a sus consecuencias para los países en desarrollo. En los últimos tiempos, los debates sobre regulación han sido objeto de especial atención en el marco de la agenda del comercio internacional. Sin embargo, como se explicó en los capítulos anteriores, los flujos de datos transfronterizos son un tipo de flujo económico internacional diferente, por lo que no deben asimilarse al comercio internacional sin un examen previo de los regímenes pertinentes. Partiendo de este contexto, en la sección B se examinan los motivos para regular los flujos de datos transfronterizos en los acuerdos comerciales. A continuación, la sección C se centra en las iniciativas de regulación de estas cuestiones en el marco del sistema de comercio a diferentes niveles. En la sección D se examinan algunas iniciativas internacionales y regionales que van más allá del ámbito comercial. Por último, en la sección E se presentan las conclusiones.

B. ¿HAY MOTIVOS PARA REGULAR LOS FLUJOS DE DATOS TRANSFRONTERIZOS COMO COMERCIO INTERNACIONAL?

Los flujos de datos transfronterizos se han convertido en un componente esencial de los debates relacionados con el "comercio digital", y han llegado a ser una cuestión clave en las negociaciones comerciales a nivel multilateral, regional y bilateral (Meltzer, 2019; Pohle y otros, 2020; Azmeh y otros, 2020; Aaronson, 2019b; Ciuriak y Ptashkina, 2018; Kelsey, 2018).

En respuesta a las demandas de sus empresas digitales, los Estados Unidos han sido el principal defensor de la inclusión de los flujos de datos transfronterizos en el sistema de comercio. En 2016, el Acuerdo de Asociación Transpacífico (TPP) (rebautizado posteriormente como Tratado Integral y Progresista de Asociación Transpacífico (TIPAT), tras la retirada de los Estados Unidos) se convirtió en el primer acuerdo comercial que preveía normas vinculantes en relación con los flujos de datos transfronterizos. Posteriormente, otros acuerdos regionales y bilaterales han incluido cláusulas similares (Burri, 2016; Janow y Mavroidis, 2019). Además, los debates sobre el comercio digital en el marco de la Organización Mundial

[1] Las Directrices están disponibles en https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

del Comercio (OMC) se han ampliado en los últimos años, y muchos países están a favor de la inclusión de disposiciones que aborden los flujos de datos transfronterizos a nivel multilateral (UNCTAD, 2021b; Azmeh y otros, 2020).

Esta inclusión se justifica por el papel cada vez más importante que desempeñan los flujos de datos en la facilitación del comercio mundial de bienes y servicios, y por los efectos que tienen las políticas nacionales sobre los datos que están adoptando los diferentes países. El papel de los flujos de datos en la facilitación del comercio es innegable. De hecho, hay muchos bienes y servicios cuyo comercio se lleva a cabo íntegramente a través de flujos de datos transfronterizos o depende en gran medida de dichos flujos. Es probable que su importancia aumente con la expansión de las tecnologías que implican un uso intensivo de datos, como la conducción autónoma, la inteligencia artificial (IA) y la Internet de las cosas.

Asimismo, las políticas de datos adoptadas por los países tienen importantes consecuencias para el comercio. La localización de los datos, por ejemplo, afecta a los flujos comerciales de bienes y servicios. Las restricciones a los flujos de datos pueden hacer que los proveedores decidan no servir a un mercado específico, debido a los costos relacionados con el cumplimiento de las medidas impuestas. La decisión de bloquear el acceso a determinadas aplicaciones web también tiene importantes consecuencias comerciales, ya que el acceso a esos sitios es una condición previa para acceder a los bienes y servicios que se venden en ellos o a través de ellos. La normativa sobre la privacidad y la protección de los datos personales también está estrechamente relacionada con el comercio. Así, por ejemplo, el hecho de que un país imponga restricciones a la recopilación y el almacenamiento de datos sobre su ciudadanía por empresas extranjeras podría afectar significativamente a la capacidad de esas empresas de vender productos en ese mercado. No obstante, aunque los flujos de datos transfronterizos están estrechamente vinculados al comercio, los argumentos a favor de regularlos prioritariamente en el marco de acuerdos comerciales son poco convincentes, en el mejor de los casos.

Hay que tener en cuenta dos cuestiones fundamentales. En primer lugar, como se explicó en los capítulos I y III, los datos tienen características diferentes a los bienes y servicios, por lo que los flujos de datos transfronterizos deben considerarse como un nuevo tipo de flujos internacionales; estos son distintos del comercio, y tratarlos del mismo modo puede resultar problemático por diversos motivos. Aunque muchos de los datos que se producen, almacenan e intercambian a nivel mundial están relacionados con transacciones comerciales, hay una gran parte de ellos que se relacionan con otros aspectos de la vida humana, y la distinción entre los diversos tipos de transacciones plantea ciertas dificultades (National Telecommunications and Information Administration (Estados Unidos), 2016). Los procesos de producción, recopilación, almacenamiento y transferencia de datos afectan a cuestiones relacionadas con la privacidad, los datos personales, las relaciones sociales y la seguridad, entre otras, y abordar esos aspectos limitándose a una "perspectiva comercial" implicaría adoptar un enfoque demasiado limitado. Además, sucede lo mismo con los productos de datos, que pueden regularse en el marco del comercio de servicios, lo que apunta a la posibilidad de que la regulación comercial de los datos deba llevarse a cabo en un contexto más amplio. En palabras de Rodrik (2020): "El sistema de comercio internacional que tenemos actualmente, plasmado en las normas de la Organización Mundial del Comercio y otros acuerdos, no es de este mundo... es totalmente inadecuado para hacer frente a los tres desafíos principales que plantean estas nuevas tecnologías". Los tres desafíos son la geopolítica y la seguridad nacional, la preocupación por la privacidad de las personas y la economía.

> Aunque los flujos de datos transfronterizos están estrechamente vinculados al comercio, los argumentos a favor de regularlos prioritariamente en el marco de acuerdos comerciales son poco convincentes, en el mejor de los casos.

Además, los datos se recopilan y almacenan en múltiples ubicaciones y son utilizados simultáneamente por usuarios de todo el mundo —de modo que la propiedad y la soberanía resultan conceptos difíciles

de aplicar (capítulo III)—, lo que dificulta la regulación de los flujos de datos transfronterizos con arreglo a las modalidades de comercio centradas en los Estados. Para reflejar esta complejidad, muchas de las nuevas propuestas de definición del "comercio digital" no incluyen los flujos de datos transfronterizos entre sus componentes. De hecho, el *Manual para la medición del comercio digital*, publicado en 2020, define el comercio digital como "todo el comercio que se encarga o entrega digitalmente", es decir, se excluyen los flujos de datos que no están vinculados a los intercambios específicos de bienes o servicios (OECD, WTO e IMF, 2020).

En segundo lugar, aun prescindiendo del hecho de que los flujos de datos transfronterizos son diferentes del comercio, existen dudas acerca de la idoneidad de regular dichos flujos en el marco del sistema comercial (Leblond y Aaronson, 2019). La historia del sistema de comercio se basa en que los países negocian concesiones recíprocas en ámbitos como los aranceles aduaneros y los contingentes. Aunque en los últimos decenios se han incorporado otras cuestiones, el sistema de comercio se sigue basando en gran medida en el intercambio de beneficios entre los distintos países. Las cuestiones que no se ajustan fácilmente a este planteamiento, como las normas laborales y ambientales, resultan difíciles de abordar en el marco del sistema de comercio (Suranovic, 2002). Los datos guardan relación con cuestiones como la protección personal y la privacidad, por lo que constituyen un ejemplo de esta situación. Además, el sistema de comercio ha sido históricamente menos transparente que los sistemas multilaterales, y se sostiene fundamentalmente en las relaciones bilaterales entre Estados. Estos sistemas quizá resultaban más pertinentes cuando las negociaciones se centraban en cuestiones como los aranceles aduaneros y los contingentes, pero la inclusión de nuevas cuestiones está haciendo que las negociaciones comerciales resulten más difíciles.

Por ejemplo, en los últimos años, el debate público y la movilización de las sociedades en respuesta a acuerdos comerciales vigentes o propuestos ha ido en aumento, debido principalmente a cuestiones como las consecuencias de dichos acuerdos en ámbitos como el medio ambiente, el trabajo, la salud y la agricultura. El aumento de la atención pública a las cuestiones reguladas en el marco del sistema de comercio está haciendo que cada vez sea más difícil lograr acuerdos sin más participación pública y procesos más transparentes (Gheyle y De Ville, 2017; Organ, 2017).

El principal factor en que se basa la incorporación de cuestiones adicionales —incluidos los flujos de datos transfronterizos— en las negociaciones comerciales es que estas se desarrollan en un foro que acoge a un gran número de países y aporta reglas y normas en vigor y bien asentadas, así como un nivel relativamente alto de aplicabilidad, en comparación con otros foros. Además, al analizar los motivos por los que la gobernanza de los datos nunca se ha abordado como una cuestión independiente, Nussipov (2020b) señala que las razones para vincular la regulación de los flujos de datos transfronterizos a la política comercial mundial siguen siendo un enigma, y argumenta que "se debió principalmente a que los Estados Unidos consiguieron trasladar los debates sobre la política de datos de su sistema nacional al sistema de comercio internacional al incluirlos en las negociaciones del Acuerdo General sobre Aranceles Aduaneros y Comercio... Los Estados Unidos utilizaron estratégicamente la búsqueda de un foro de conveniencia para replantear los flujos de datos como una cuestión de política comercial". Este replanteamiento "hizo que la política de datos pasase de abordarse en el marco de los sistemas de telecomunicaciones, redes de datos y desarrollo económico al sistema de comercio internacional. Los tres primeros sistemas se centraban en aspectos técnicos y en medidas de política nacional relativas a asuntos internos. El sistema de comercio internacional priorizaba la apertura, el libre comercio y el crecimiento económico".

Aparte de estas cuestiones más generales, en la esfera del comercio, los países en desarrollo se enfrentan a un panorama especialmente complejo, en el que las asimetrías de poder tienen un peso importante en la configuración de los resultados. Una de las razones de la expansión del sistema de comercio ha sido la presión ejercida por las economías más avanzadas para vincular nuevas cuestiones al sistema de comercio, con el objetivo de aprovechar el mayor tamaño de su mercado para obtener resultados beneficiosos en esferas como la propiedad intelectual y los regímenes de inversión (Sell, 2009). En lo que respecta a los datos, su vinculación con cuestiones como el acceso a los mercados podría poner a las economías en desarrollo en la difícil situación de elegir entre ceder su derecho (o margen de actuación) a regular los flujos de datos para preservar su acceso a los mercados de las economías avanzadas o procurarse un mayor acceso a algunos sectores económicos (Steinberg, 2002). También

se ha comprobado que los países en desarrollo se encuentran en una posición más vulnerable en lo que respecta a la solución de diferencias en el marco de los acuerdos comerciales internacionales (Mosoti, 2006; Abbott, 2009).

> En la esfera del comercio, los países en desarrollo se enfrentan a un panorama especialmente complejo, en el que las asimetrías de poder tienen un peso importante en la configuración de los resultados.

Algunos países y organizaciones no gubernamentales han puesto en tela de juicio las presiones para ampliar el sistema de comercio. Han señalado que los negociadores comerciales, en particular los de los países en desarrollo más pequeños, no tienen capacidad para negociar una agenda cada vez más amplia, que abarca cuestiones complejas y sumamente técnicas. Como sus economías tienen la capacidad de ofrecer mayores ventajas a los países con los que suscriben acuerdos bilaterales y regionales, los países más poderosos pueden servirse de ese tipo de acuerdos para promover normas que les resultaría difícil imponer en el marco multilateral. En consecuencia, el poder de las economías desarrolladas tiende a ser mayor en los foros bilaterales y regionales, dado que es más probable que los países en desarrollo acepten individualmente determinadas normas que se resistirían a aceptar como grupo. Esta capacidad se ve reforzada por lo que algunas voces expertas han llamado el miedo a la exclusión, que es la preocupación que experimentan los países en desarrollo por la posibilidad de que otros países en desarrollo logren una mayor participación en el comercio y las inversiones a su costa, como resultado de la firma de acuerdos comerciales bilaterales (Shadlen, 2008). Estos factores sitúan a las economías desarrolladas en una posición de fuerza en las negociaciones comerciales internacionales, ya que les permiten utilizar el tamaño de sus mercados para promover determinadas normas, y alternar entre el marco multilateral y los diversos marcos regionales/bilaterales para debilitar la resistencia frente a determinadas normas. Esta dinámica pone a los países en desarrollo "entre la espada y la pared", ya que si se resisten a determinadas medidas en el marco multilateral podrían dar lugar a que se adoptasen nuevos acuerdos regionales y bilaterales que debilitasen todavía más su posición como grupo.

En general, preocupa que la regulación de los flujos de datos transfronterizos mediante acuerdos comerciales dificulte la consideración de la naturaleza multidimensional de los datos y la plena participación de todas las partes potencialmente afectadas. Como la mayoría de los países en desarrollo tienen un poder de mercado relativamente escaso, también existe el riesgo de que los resultados de las negociaciones reflejen principalmente los intereses de las empresas de las economías más avanzadas, que son las que actualmente están en mejor posición de generar valor con la expansión de los flujos de datos. Aunque esto podría reducir la incertidumbre con respecto a los flujos de datos transfronterizos, también reafirmaría y reforzaría los desequilibrios existentes en la economía digital impulsada por los datos.

> Preocupa que la regulación de los flujos de datos transfronterizos mediante acuerdos comerciales dificulte la consideración de la naturaleza multidimensional de los datos y la plena participación de todas las partes potencialmente afectadas.

Por ejemplo, la Argentina, Colombia y Costa Rica[2] han indicado que prefieren que el alcance de los debates sobre las negociaciones comerciales en el marco de la OMC se limite a los aspectos relacionados con el

[2] Véase la comunicación de la Argentina, Colombia y Costa Rica "Negociaciones de la OMC sobre los aspectos del comercio electrónico relacionados con el comercio. Elementos de un posible enfoque en el marco de la Declaración Conjunta sobre el Comercio Electrónico" (JOB/GC/174), OMC, 5 de abril de 2018 (disponible en https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=S&CatalogueIdList=252606&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.)

comercio; que desean que se reafirme el derecho de los Miembros a reglamentar con miras a garantizar la protección de la intimidad de los particulares y la seguridad y la confidencialidad de la información; y que los participantes deben guiarse por las normas internacionales pertinentes cuando existan.

El Brasil ha señalado que entre los temas fundamentales que requerirán la elaboración de normas están "la medida y las condiciones en que se permitirá el flujo de datos digitales"[3], e indicado que los "organismos de reglamentación se encontrarán en situaciones en las que la limitación del flujo de datos es inevitable... Las excepciones generales y las excepciones relativas a la seguridad de los artículos XIV y XIV *bis* del AGCS son disposiciones útiles... pero ni unas ni otras se redactaron específicamente para el entorno digital. Por consiguiente, podría ser conveniente examinar de qué forma se podrían aclarar mediante disciplinas mejoradas las excepciones generales y las excepciones relativas a la seguridad adaptándolas al entorno digital". Entre las cuestiones a las que debería prestarse atención, el Brasil ha destacado las siguientes: si el uso de macrodatos requerirá también un debate sobre la jurisdicción, la propiedad de los datos generados en diferentes jurisdicciones y la portabilidad de datos y el acceso no discriminatorio. Posteriormente, el Brasil apoyó la disposición "típica" sobre la transferencia transfronteriza de información: el derecho a las propias prescripciones reglamentarias, la autorización de las transferencias transfronterizas cuando estas se hagan en el marco de actividades empresariales y la excepción relativa a los objetivos legítimos de política, siempre que la medida no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable o un obstáculo encubierto[4].

China ha declarado que cada vez se hace más alusión a cuestiones como la ciberseguridad, la seguridad de los datos y la privacidad, ya que plantean riesgos de seguridad y problemas de reglamentación a los Miembros a los que nunca antes se habían enfrentado[5]. El país ha señalado que los Miembros difieren en cuanto a las condiciones nacionales y las etapas de desarrollo, y que tienen diferentes desafíos y preocupaciones, y que "habida cuenta de esas diferencias, los Miembros deberían respetar las modalidades de desarrollo del comercio electrónico que conciba cada uno y el derecho legítimo a adoptar medidas de reglamentación para cumplir objetivos razonables de su política pública". Côte d'Ivoire ha sugerido que se establezca un foro de cooperación interinstitucional que ayude a promover, entre otras cosas, los marcos nacionales de utilización de datos[6].

Sin embargo, como se explicó en los anteriores capítulos, dado el carácter multidimensional de los datos, las implicaciones de los flujos de datos transfronterizos van mucho más allá de las cuestiones de comercio internacional, y tienen efectos complejos e interrelacionados para la sociedad en muchas esferas, tanto económicas como no económicas. Además, como se señaló en el capítulo III, no existen propiamente mercados multilaterales de datos (brutos) que permitan a los proveedores de datos (normalmente los titulares) intercambiar estos datos por dinero con quienes los demandan (ya que la mayoría de los datos brutos se extraen de forma gratuita). Por lo tanto, no existen ni exportaciones ni importaciones de datos. Tampoco existe un registro de los flujos de datos que cruzan las fronteras, como en el caso del comercio internacional. Cuando se examina la economía digital impulsada por los datos, en el marco de las relaciones internacionales entre los países se producen flujos de datos de salida y de entrada, que son un tipo de flujo internacional diferente del comercio, y que implica mucho más que el comercio. Por último, una de las principales deficiencias del sistema de comercio en este contexto es el hecho de que no distingue

[3] Véase "Trabajos exploratorios sobre el comercio electrónico. Documento no oficial del Brasil" (JOB/GC/176), OMC, 11 de abril de 2018 (disponible en https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=S&CatalogueIdList=244463&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True).

[4] Véase "Comunicación del Brasil. Declaración conjunta sobre el comercio electrónico" (INF/ECOM/27), OMC, 30 de abril de 2019 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/INF/ECOM/27.pdf&Open=True).

[5] Véase "Comunicación de China. Declaración conjunta sobre el comercio electrónico" (INF/ECOM/19), OMC, 24 de abril de 2019 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/INF/ECOM/19.pdf&Open=True).

[6] Véase "Comunicación presentada por Côte d'Ivoire. Declaración conjunta sobre el comercio electrónico" (INF/ECOM/46), OMC, 14 de noviembre de 2019 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/INF/ECOM/46.pdf&Open=True).

entre los flujos de datos brutos, que indudablemente no son comercio, y los flujos de productos de datos, que podrían considerarse comercio de servicios, pero posiblemente requieran una adaptación de sus normas al nuevo contexto de la economía digital (véase el capítulo I), ya que el tratamiento de los datos se ha ido entremezclando cada vez más con otros aspectos de la sociedad, como la privacidad y otros derechos humanos, así como con cuestiones de seguridad. Así pues, los flujos de datos transfronterizos deben abordarse desde una perspectiva normativa más amplia, integrada y equilibrada.

C. REGULACIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS EN LOS ACUERDOS COMERCIALES

En esta sección se examinan los diferentes regímenes comerciales que regulan los flujos de datos transfronterizos a nivel multilateral, regional y bilateral.

1. Tratamiento de los flujos de datos en los acuerdos comerciales multilaterales

Con la evolución de la economía digital impulsada por los datos, en los últimos años el tema de la aplicabilidad de las normas de la OMC y otros acuerdos comerciales vigentes a los flujos de datos transfronterizos ha ganado importancia en el marco del debate económico internacional. Esta cuestión se ha planteado porque los principales acuerdos del sistema de comercio multilateral se adoptaron antes de la expansión de la economía digital y el rápido aumento de los flujos de datos transfronterizos. En consecuencia, los intentos de someter el tratamiento de los flujos de datos transfronterizos a los acuerdos y principios vigentes del sistema multilateral de comercio se han tropezado con dificultades.

La distinción entre bienes y servicios es uno de los pilares del sistema multilateral de comercio. Dentro del sistema de la OMC, los bienes se rigen por el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT), mientras que los servicios se rigen por el Acuerdo General sobre el Comercio de Servicios (AGCS).

Es importante destacar que tanto el GATT como el AGCS incluyen cláusulas de "excepción general" que son aplicables a los flujos de datos transfronterizos. El artículo XX del GATT permite a los Estados miembros adoptar las medidas "necesarias para proteger la moral pública", en tanto que el artículo XXI permite a cada uno de los miembros adoptar "las medidas que estime necesarias para la protección de los intereses esenciales de su seguridad". Del mismo modo, el artículo XIV del AGCS permite a los miembros adoptar las medidas "necesarias para proteger la moral o mantener el orden público", así como las medidas necesarias para "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". La principal condición prevista en estas disposiciones es que dichas medidas 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".

No obstante, las condiciones que deben cumplir los países para acogerse a las excepciones pueden ser bastante difíciles de cumplir. La "prueba de necesidad" prevista tanto en el artículo XX del GATT como en el artículo XIV del AGCS no resulta fácil de superar. Si un grupo especial de solución de diferencias determina que había otra medida disponible, esta se considerará preferible aunque fuese más costosa y gravosa para el país que la impone.

Meltzer (2019) explica cómo se podría aplicar esto a una medida de localización de los datos. La cláusula de excepción y la prueba de necesidad conexa han sido resumidas por Geist (2018) del siguiente modo: "La excepción general debe, por tanto, cumplir cuatro requisitos: i. tiene que lograr un objetivo legítimo de política pública; ii. no puede aplicarse de manera que constituya un medio de discriminación arbitraria o injustificable; iii. no puede constituir una restricción encubierta al comercio; y iv. no debe imponer más restricciones de las necesarias para lograr el objetivo (es decir, un requisito de impedimento mínimo en relación con el uso o la ubicación de las instalaciones informáticas)". Este autor señala también que "los antecedentes históricos indican que el recurso a esta excepción casi nunca se acepta... ya que en la práctica solo ha prosperado 1 de cada 40 intentos de invocar las excepciones del GATT y del AGCS

para defender una medida impugnada", y concluye que "las ventajas de la excepción general pueden ser ilusorias, ya que los requisitos son tan complejos (deben cumplirse todos los aspectos) que los países casi nunca han logrado reunir las condiciones necesarias".

Además, por lo general, el hecho de que las excepciones se definan de forma imprecisa hace que en última instancia sean los mecanismos de solución de diferencias previstos en estos acuerdos los que determinen qué "objetivo legítimo de política pública" puede justificar la restricción de los flujos de datos transfronterizos. Lo mismo ocurre con la disposición relativa a la "necesidad": por ejemplo, el requisito de que "no imponga restricciones sobre el uso o ubicación de las instalaciones informáticas mayores a las que se requieren para alcanzar el objetivo" haría que cuestiones tan importantes como la regulación de los datos quedasen sujetas a la decisión de grupos especiales de tres especialistas en los casos en que los Estados miembros planteasen una diferencia.

Las consecuencias de estas medidas para los flujos de datos transfronterizos todavía no están del todo claras (UNCTAD, 2017). En principio, un gran número de medidas que los países están adoptando para restringir los flujos de datos transfronterizos pueden justificarse por razones de seguridad o de moral pública (Mitchell y Hepburn, 2017). Las medidas de localización de los datos, por ejemplo, que exigen el almacenamiento de los mismos en el territorio nacional, suelen adoptarse por motivos relacionados con la seguridad, ya sea para preservar la seguridad del país o para limitar la vigilancia extranjera. El interés público por la cuestión de los flujos de datos transfronterizos, por ejemplo, ha aumentado a raíz de que se publicase la información revelada por Edward Snowden, el antiguo analista de la Agencia de Seguridad Nacional de los Estados Unidos que denunció que la agencia y otros organismos de inteligencia realizaban actividades de vigilancia en línea a gran escala en todo el mundo. Estas actividades socavaban la privacidad de muchas personas en los Estados Unidos y en el extranjero, lo que llevó a algunos países a adoptar estrategias para restringir el flujo de los datos (Aaronson, 2015).

Los debates sobre estas cuestiones en el marco de la OMC comenzaron relativamente pronto, y se incorporaron a la agenda del Programa de Trabajo sobre el Comercio Electrónico, adoptado en 1998. Desde entonces se han producido pocos avances sustanciales en el marco de dicho programa. No obstante, algunos miembros de la OMC han presentado propuestas con el objetivo de ampliar la labor en este ámbito. En 2011, los Estados Unidos y la Unión Europea presentaron una comunicación conjunta que incluía una serie de "principios relacionados con el comercio [...] a fin de promover la expansión de las redes y servicios de tecnología de la información y las comunicaciones (TIC) y potenciar el desarrollo del comercio electrónico"[7]. Los principios incluían "los flujos de información transfronterizos" y establecían que "los Gobiernos no impedirán que los proveedores de servicios de otros países o los clientes de esos proveedores transfieran información por vía electrónica en su territorio o más allá de sus fronteras, accedan a información disponible públicamente o accedan a su propia información almacenada en otros países".

Este concepto se desarrolló más en los años posteriores. En 2014, por ejemplo, los Estados Unidos presentaron una comunicación al Programa de Trabajo en la que argumentaban que los requisitos de localización de datos restringen los flujos de datos transfronterizos, y que "los países que adoptan medidas en que se exige que se procese y almacene dentro de sus fronteras la información personal de los consumidores pueden tener buenas intenciones, pero esas medidas pueden frenar la actividad económica y no proporcionar forzosamente la seguridad de la información que, en teoría, tratan de lograr". Según la comunicación, la seguridad de la información "puede ser mayor cuando se almacena externamente, ya que las economías de escala que pueden lograrse mediante la seguridad especializada de los mejores procesadores de datos puede ser superior a la que ofrecen las instalaciones de almacenamiento disponibles en un territorio determinado". En cuanto a la privacidad y la protección de datos, los Estados Unidos reconocían que "todos los Miembros tienen el interés en proteger la privacidad y la seguridad de la información", pero afirmaban que estas medidas debían estar sujetas a disciplinas adecuadas. "En opinión de los Estados Unidos, hay pocos elementos de juicio que justifiquen la necesidad de restringir la exportación de datos al territorio de un país determinado simplemente porque el país de destino no tiene

[7] Véase la comunicación de los Estados Unidos y la Unión Europea "Contribución al Programa de Trabajo sobre el Comercio Electrónico" (S/C/W/338), OMC, 13 de julio de 2011 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=S:/S/C/W338.pdf&Open=True).

el mismo régimen formal de privacidad o seguridad de los datos que el país de origen". Los miembros, por lo tanto, "deben velar por que toda medida que impida la exportación de datos u obligue a almacenar los datos en su territorio no constituya un obstáculo injustificado al comercio ni discrimine indebidamente contra los proveedores extranjeros de cualquier servicio basado en el uso intensivo de la información, incluido, entre otros, el procesamiento de datos"[8].

Los Estados Unidos consolidaron estas propuestas en un documento no oficial presentado en 2016[9], en el que exponían ejemplos de "contribuciones positivas a una economía digital floreciente". Entre estos ejemplos se incluía "permitir las corrientes transfronterizas de datos" para que las empresas y consumidores puedan "transferir datos como consideren", y se instaba a la adopción de normas para evitar los obstáculos discriminatorios a la libre circulación de los datos protegiendo la transferencia de datos, con sujeción a salvaguardias razonables como la protección de los datos de los consumidores al ser exportados. Otro ejemplo importante era el de evitar los obstáculos relacionados con la localización de los datos que imponen "costos y cargas innecesarios a los proveedores y los consumidores por igual", para lo cual se instaba a adoptar normas comerciales que ayudasen "a promover el acceso a las redes y el procesamiento eficiente de los datos".

Estas propuestas contaron con el apoyo de otros miembros. En 2016, el llamado grupo MIKTA (México, Indonesia, República de Corea, Turquía y Australia) celebró un taller sobre comercio electrónico en el marco de la OMC, y emitió una declaración en la que señalaba que la Organización debería prestar más atención al comercio digital. En opinión del grupo, este esfuerzo debería abarcar también "cuestiones más nuevas relacionadas con el comercio electrónico que no han empezado a tener interés para la política comercial hasta hace unos años, como los flujos de datos y la localización de los datos" (MIKTA, 2016). Los debates sobre comercio electrónico en el marco de la OMC se intensificaron en el marco de los preparativos de la 11ª Conferencia Ministerial, celebrada en Buenos Aires en 2017.

Sin embargo, las propuestas a favor de los flujos de datos transfronterizos sin restricciones en el sistema de la OMC contaron con la oposición de algunos países en desarrollo miembros —como la India, Indonesia y Sudáfrica— y el Grupo Africano. Estos miembros señalaron con preocupación que las normas vinculantes sobre los flujos de datos transfronterizos limitarían su margen de actuación para adoptar políticas de datos y digitales que pudiesen ayudar a sus economías a lograr la industrialización y el desarrollo tecnológico. El Grupo Africano, por ejemplo, señaló que "resulta sorprendente que algunos Miembros defiendan la adopción de nuevas normas multilaterales sobre el comercio electrónico", y añadió que "las normas multilaterales existentes limitan nuestro margen de actuación nacional y nuestra capacidad de industrializarnos"[10]. La comunicación del Grupo Africano destacaba su firme oposición a las nuevas normas multilaterales en materia de datos, en particular a la libre circulación de los datos y a la prohibición de las obligaciones de localización de los datos. Además de las cuestiones relacionadas con el margen de actuación y la política industrial digital, algunos países expresaron también su temor a que la defensa de la libre circulación de los datos facilitase un acceso libre a los mercados a los bienes y servicios suministrados digitalmente, lo que privaría a las economías en desarrollo de importantes ingresos arancelarios y amenazaría a sus sectores de servicios nacionales por el incremento del comercio de bienes y servicios en línea.

Las propuestas de adoptar normas para exigir la libre circulación de los datos a través de las fronteras tampoco contaron con el apoyo de algunas economías avanzadas. Aunque la Unión Europea en su conjunto se mostró, en general, a favor de ir en esta dirección, algunos países europeos influyentes, en particular Alemania y Francia, expresaron dudas sobre la conveniencia de aprobar cláusulas que

[8] Véase la comunicación de los Estados Unidos "Programa de Trabajo sobre el Comercio Electrónico" (S/C/W/359), OMC, 17 de diciembre de 2014 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/S/C/W359.pdf&Open=True).

[9] Véase el documento no oficial de los Estados Unidos "Programa de Trabajo sobre Comercio Electrónico" (JOB/GC/94), OMC, 4 de julio de 2016.

[10] Véase la declaración del Grupo Africano "Programa de Trabajo sobre el Comercio Electrónico" (WT/MIN(17)/21), OMC, 6 de diciembre de 2017 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/WT/MIN17/21.pdf&Open=True).

establecieran la libre circulación de los datos (Azmeh y otros, 2020). Esa falta de apoyo reflejaba tanto las preocupaciones económicas y tecnológicas de esos países por los efectos de tales cláusulas para la economía europea —en el contexto del dominio de las grandes empresas digitales de los Estados Unidos— como su preocupación por las consecuencias de esas normas para la privacidad y la protección de datos en Europa, que se refleja en la adopción del Reglamento General de Protección de Datos (RGPD).

Ante las dificultades para alcanzar un consenso de los miembros de la OMC en relación con la ampliación de los debates en esta esfera, los defensores de las normas de comercio electrónico (que potencialmente abarcarían los flujos de datos transfronterizos) empezaron a favorecer las negociaciones plurilaterales sobre esta cuestión. Con motivo de la Conferencia Ministerial de Buenos Aires, celebrada en 2017, 71 países emitieron la Declaración Conjunta sobre el Comercio Electrónico, en la que reafirmaban la importancia del comercio electrónico y el objetivo de avanzar la labor sobre el comercio electrónico en la OMC. Bajo la dirección de Australia, el Japón y Singapur, el grupo anunció que iniciarían trabajos exploratorios con miras a futuras negociaciones en la OMC sobre los aspectos del comercio electrónico relacionados con el comercio. A lo largo de 2019, el grupo mantuvo negociaciones a través de diferentes grupos de discusión con el objetivo de llegar a un resultado antes de la 12ª Conferencia Ministerial, que iba a celebrarse en Kazajstán en 2020, pero tuvo que ser pospuesta debido a la COVID-19 y ahora se espera que se celebre en Ginebra a finales de 2021.

Los flujos de datos transfronterizos son una de las cuestiones importantes de esas negociaciones (Ismail, 2020). En una comunicación de Singapur, por ejemplo, se proponían dos cláusulas fundamentales en relación con los flujos de datos transfronterizos. La primera es que “los Miembros permitirán la transferencia transfronteriza de información por medios electrónicos, incluida la información personal, cuando esta se haga en el marco de la actividad empresarial”, con la salvedad de que “ninguna disposición del presente artículo impedirá que un Miembro adopte o mantenga medidas incompatibles con el párrafo 2 para alcanzar un objetivo legítimo de política pública, siempre que la medida no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable o una restricción encubierta del comercio”. En segundo lugar, en lo que respecta a la ubicación de las instalaciones informáticas (localización de los datos), la cláusula establece que “los Miembros no exigirán la utilización o ubicación de instalaciones informáticas en su territorio como condición para llevar a cabo actividades en ese territorio”, con una salvedad similar a la de la cláusula anterior.[11]

La participación de los PMA y de los miembros de las regiones de África, el Caribe y el Pacífico en el proceso de la Iniciativa de Declaración Conjunta ha sido escasa (cuadro VI.1). Esto podría reflejar no solo preocupaciones relacionadas con los temas específicos abordados en las negociaciones, sino también preocupaciones más amplias relativas a la naturaleza plurilateral del proceso y a la justificación de que se dé prioridad al comercio electrónico frente a otros temas de negociación. Algunas cuestiones que se han destacado como motivo de esta participación escasa son[12]:

- El temor a que la tendencia a adoptar un enfoque plurilateral resulte en un debilitamiento del multilateralismo: como se señala en la comunicación, “ese enfoque permite a los Miembros hacer caso omiso de los intereses en materia de desarrollo de los países de ingresos bajos, cuya participación en esos acuerdos tiene escaso interés comercial para las grandes potencias comerciales. De ese modo, nuestros países corren el riesgo de verse en la tesitura de tener que aceptar o rechazar algo que haya sido decidido por los demás”.
- El temor a que un acuerdo aislado sobre comercio electrónico, sin avances en otras cuestiones importantes para los países en desarrollo, como la agricultura, comprometa el sistema multilateral inclusivo.

[11] Véase la comunicación de Singapur “Declaración Conjunta sobre el Comercio Electrónico” (INF/ECOM/25), 30 de abril de 2019, (disponible en https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=S&CatalogueIdList=253794&CurrentCatalogueIdIndex=0&FullTextHash=371857150&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True).

[12] Véase la comunicación de Côte d’Ivoire “Declaración conjunta sobre el Comercio Electrónico” (INF/ECOM/49), OMC, 16 de diciembre de 2019 (disponible en https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/INF/ECOM/49.pdf&Open=True).

Cuadro VI.1. Participantes en la Iniciativa de Declaración Conjunta de 2019 (a noviembre de 2020)

Países desarrollados	Economías en transición	América Latina	Asia	África
Australia	Albania	Argentina	Arabia Saudita	Benin*
Canadá	Federación de Rusia	Brasil	Bahrein	Burkina Faso*
Estados Unidos	Georgia	Chile	Brunei Darussalam	Camerún
Islandia	Kazajstán	Colombia	China	Côte d'Ivoire
Israel	Macedonia del Norte	Costa Rica	Emiratos Árabes Unidos	Kenya
Japón	Montenegro	Ecuador	Filipinas	Nigeria
Liechtenstein	República de Moldova	El Salvador	Hong Kong (China)	
Noruega	Ucrania	Guatemala	Indonesia	
Nueva Zelandia		Honduras	Kuwait	
Reino Unido		México	Malasia	
Suiza		Nicaragua	Mongolia	
Unión Europea (27 países miembros)		Panamá	Myanmar*	
		Paraguay	Provincia China de Taiwán	
		Peru	Qatar	
		Uruguay	República de Corea	
			República Democrática Popular Lao*	
			Singapur	
			Tailandia	
			Turquía	

Fuente: UNCTAD (2021b).
Nota: Los países marcados con un asterisco (*) son PMA.

- Los escasos beneficios que obtienen los países de ingresos bajos de la digitalización del comercio para su desarrollo económico.
- La capacidad de negociación limitada de los países en desarrollo que tienen delegaciones pequeñas en Ginebra y no pueden permitirse enviar especialistas en todas las esferas de negociación ni recurrir al apoyo técnico en la misma medida que las economías más avanzadas. Por lo tanto, es comprensible que concentren esos recursos limitados en cuestiones de mayor importancia para sus economías, en lugar de abordar las cuestiones relacionadas con el comercio electrónico.

Quienes defienden la inclusión de medidas destinadas a preservar los flujos de datos transfronterizos sin restricciones en el marco de la OMC han adoptado diversos enfoques para lograr su objetivo, entre ellos, afirmar que estos flujos ya están abarcados en los acuerdos y compromisos vigentes (como el Modo 1 del AGCS), a pesar de que quienes redactaron esos acuerdos no podrían haber previsto los tipos de flujos que existen en la actualidad. Ante la resistencia de muchos miembros de la OMC a aceptar esta línea de argumentación, estos defensores han pasado a proponer negociaciones (en un primer momento, negociaciones multilaterales y, posteriormente, la Iniciativa de Declaración Conjunta) para establecer nuevas normas comerciales que aborden estos flujos de datos. Con independencia del foro en el que se lleven a cabo esas iniciativas, los debates se siguen desarrollando en un contexto de escaso conocimiento de las cuestiones en juego, incluidas las que van más allá del ámbito comercial. Las opiniones sobre este asunto son muy divergentes y tienen un fuerte componente político. Además, la complejidad de estas cuestiones, la falta de definiciones comunes y las dificultades de medición hacen que no exista una base suficientemente sólida para el desarrollo de los debates. En consecuencia, existe el riesgo de que los

responsables políticos tomen decisiones que no estén adecuadamente fundamentadas en las estadísticas o respaldadas por análisis apropiados.

El resultado de las negociaciones puede tener consecuencias importantes para el desarrollo del comercio electrónico y la evolución del sistema de comercio multilateral en el futuro. La gran diversidad de capacidades digitales y preferencias normativas que existe entre los miembros de la OMC participantes hace que llegar a posiciones comunes en lo que respecta a cuestiones como los flujos de datos transfronterizos constituya un enorme desafío. El hecho de que un número significativo de países en desarrollo se abstenga de participar también plantea interrogantes sistémicas sobre el tipo de formato que podría adoptar un futuro acuerdo dentro de la estructura de la OMC, y los efectos que podría tener para los países que no tomen parte en él (UNCTAD, 2021b).

Es difícil predecir el resultado de estos procesos en el marco de la OMC. Sin embargo, un factor importante será la medida en la que se incluyan cláusulas similares en los acuerdos regionales y bilaterales. Como ya se ha comentado, es posible que los países en desarrollo que acepten por separado este tipo de cláusulas en el marco de acuerdos comerciales regionales y bilaterales obtengan mayores beneficios, lo que podría debilitar la oposición a estas normas a nivel multilateral.

2. Tratamiento de los flujos de datos en los acuerdos comerciales preferenciales

Los acuerdos comerciales regionales, bilaterales y transnacionales se han convertido en instrumentos cada vez más importantes para abordar las cuestiones relacionadas con los flujos de datos transfronterizos (Monteiro y Teh, 2017). Esta tendencia es especialmente visible en los acuerdos firmados por las economías desarrolladas, en tanto que los países de ingresos bajos casi nunca suscriben acuerdos que aborden los flujos de datos. El contenido de los acuerdos comerciales preferenciales puede indicar en qué dirección podría avanzar el debate multilateral sobre los flujos de datos, teniendo en cuenta el papel de algunas grandes potencias en la configuración de las relaciones económicas internacionales. A continuación se analizan las cláusulas relativas a los datos incluidas en los acuerdos comerciales de algunas de las principales economías. Se presta especial atención a las adoptadas por los Estados Unidos y la Unión Europea, ya que son muy activos en la negociación y firma de acuerdos regionales y bilaterales que abarcan los flujos de datos transfronterizos.

a) Acuerdos comerciales de los Estados Unidos

Como líder de la economía digital y país donde se radican las empresas digitales más poderosas del mundo, los Estados Unidos han ejercido presión para que se establezcan normas comerciales vinculantes en relación con los flujos de datos. En las últimas décadas, las principales empresas digitales de este país se han expandido sin que existiera un marco normativo claro que regulase sus operaciones en todo el mundo. Aunque estaban sujetas a la legislación nacional de los Estados Unidos, estas empresas carecían de un marco normativo claro en muchas regiones en las que operaban y en las que se estaban expandiendo rápidamente. Esto las exponía a un alto grado de incertidumbre como resultado de los cambios normativos que podrían adoptar los Estados de todo el mundo. Aunque una empresa como Google, por ejemplo, puede invertir grandes sumas en almacenamiento de datos e infraestructuras de cable, los cambios normativos de los Estados podrían tener importantes consecuencias para la viabilidad económica de dichas inversiones.

Por ese motivo, estas empresas han estado entre las más tempranas defensoras de la incorporación de los flujos de datos transfronterizos en los acuerdos comerciales de los Estados Unidos (Azmeh y otros, 2020). A modo de ejemplo, Google argumentó en un documento publicado en 2010 que “los Estados deberían dejar de tratar la política de Internet y el comercio internacional como compartimentos estancos, y reconocer que muchas acciones relacionadas con la censura en Internet constituyen obstáculos injustos para el comercio” (Google, 2010:16). En 2012, la Alianza del Sector del *Software* (BSA), grupo de presión de esa rama de producción, publicó un informe en el que se presentaban algunos de los problemas a los que se enfrentan los sectores digitales, como el “proteccionismo digital”, y se señalaba que esos problemas deberían formar parte de la agenda comercial a nivel regional, bilateral

y multilateral (BSA, 2012). El Representante de Comercio de los Estados Unidos incluyó esas demandas en el marco de la "agenda de comercio digital". Entre otras medidas, la libre circulación de los datos y la prohibición de su localización eran cláusulas fundamentales de esa agenda (Azmeh y otros, 2020).

El primer éxito de esta agenda fue la inserción de estas cláusulas en un capítulo sobre el comercio digital del Acuerdo de Asociación Transpacífico (TPP); este fue firmado en 2016 por los Estados Unidos con varios países de Asia y el Pacífico (Australia, Brunei Darussalam, Canadá, Chile, Japón, Malasia, México, Nueva Zelandia, Perú, Singapur y Viet Nam) que representan el 40 % del producto interno bruto mundial. Constituyó un paso importante hacia la ampliación de este tipo de normas. La posterior retirada de los Estados Unidos del acuerdo socavó en cierta medida esta iniciativa, aunque las cláusulas sobre los flujos de datos y la economía digital se mantuvieron sin apenas cambios en el Tratado Integral y Progresista de Asociación Transpacífico (TIPAT). Además del TPP/TIPAT, el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC) revisado incluía un compromiso vinculante relativo a la libre circulación de los datos y la prohibición de su localización.

En el TPP/TIPAT, el artículo 14.11 prevé el compromiso de las partes con "la transferencia transfronteriza de información por medios electrónicos, incluida la información personal, cuando esta actividad sea para la realización de un negocio de una persona cubierta". Sin embargo, las partes pueden adoptar medidas incompatibles con la libertad de circulación transfronteriza "para alcanzar un objetivo legítimo de política pública", siempre que la medida "no se aplique de manera que constituya un medio de discriminación arbitraria o injustificable, o una restricción encubierta del comercio", y "no imponga restricciones a las transferencias de información mayores que las necesarias para alcanzar el objetivo". Del mismo modo, en el artículo 14.13 las partes se comprometen a no "exigir a una persona cubierta usar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la realización de negocios en ese territorio", con excepción de las medidas incompatibles con esta cláusula que vayan destinadas a "alcanzar un objetivo legítimo de política pública, siempre que la medida no se aplique de forma que constituya un medio de discriminación arbitrario o injustificable, o una restricción encubierta al comercio; y no imponga restricciones sobre el uso o ubicación de las instalaciones informáticas mayores a las que se requieren para alcanzar el objetivo". El T-MEC contiene disposiciones similares sobre la transferencia transfronteriza de datos (artículo 19.11), pero elimina la cláusula de excepción para la ubicación de las instalaciones informáticas (artículo 19.12).

Los Estados Unidos negociaron cláusulas similares con la Unión Europea en el marco del proyecto de Asociación Transatlántica de Comercio e Inversión. Cabe esperar que los futuros acuerdos comerciales que negocien los Estados Unidos incluyan este tipo de cláusulas. Los anuncios recientes relativos a un acuerdo de libre comercio entre los Estados Unidos y Kenya incluían la economía digital entre los temas de negociación (Foster, 2020). Los objetivos de negociación publicados por los Estados Unidos incluyen el establecimiento de "normas avanzadas para garantizar que Kenya no imponga medidas que restrinjan los flujos de datos transfronterizos ni exija el uso o el establecimiento de instalaciones informáticas locales" (United States Trade Representative, 2020).

La inclusión de cuestiones relativas a los datos en un futuro acuerdo bilateral entre los Estados Unidos y Kenya es significativa, ya que será la primera vez que un país africano firme un acuerdo que incluya un compromiso de libre circulación de los datos a través de las fronteras. Los Estados Unidos ven este acuerdo "como un modelo para los acuerdos de libre comercio de los Estados Unidos con otros países africanos". Teniendo en cuenta lo que se ha comentado anteriormente sobre las concesiones costo-beneficio entre los acuerdos multilaterales y los regionales/bilaterales, este tipo de acuerdo podría resultar atractivo para Kenya. Los beneficios resultantes de la firma de un acuerdo bilateral con los Estados Unidos podrían ser significativamente mayores de los que obtendría adhiriéndose a un acuerdo multilateral o incluso regional. Esto es especialmente cierto porque Kenya es una de las principales economías digitales de África.

A pesar de los importantes beneficios potenciales, resulta clave determinar cuál de las partes captaría las ganancias asociadas a los flujos de datos transfronterizos. Dados los diferentes grados de desarrollo digital de los Estados Unidos y Kenya, es muy probable que los flujos de datos entre ambas economías permitan a las plataformas digitales globales de los Estados Unidos acceder a los datos de Kenya y sacar provecho de ellos, mientras que las empresas de Kenya podrían tener una capacidad más limitada para recopilar

y monetizar los datos generados en los Estados Unidos. Además, teniendo en cuenta el desarrollo de la Zona de Libre Comercio Continental Africana y su objetivo de reforzar el comercio electrónico y digital regional, esas plataformas podrían aprovechar el grado relativamente alto de digitalización de Kenya como punto de acceso a los datos del resto de África.

b) Acuerdos comerciales de la Unión Europea

Al contrario que en los Estados Unidos, donde existe una posición clara de promoción de la libre circulación de los datos, en el caso de la Unión Europea la cuestión de los flujos de datos, y en particular su inclusión en los acuerdos comerciales, ha sido más controvertida (Yakovleva e Irion, 2020). La existencia de firmes opositores a la inclusión de cláusulas vinculantes sobre la libre circulación de los datos en los acuerdos comerciales refleja varios factores. En primer lugar, en la Unión Europea se llevó a cabo una fuerte campaña en contra de esas cláusulas por motivos de privacidad y protección de los datos personales, ya que algunas organizaciones no gubernamentales se movilizaron en este sentido y varios países miembros influyentes adoptaron una posición prudente al respecto[13]. Ello contribuyó a la adopción del RGPD, que tuvo importantes consecuencias para la inclusión de cláusulas sobre la libre circulación de los datos en los acuerdos comerciales internacionales. Como se explicó en el capítulo IV, el RGPD prohíbe la transferencia de datos personales europeos fuera de la Unión Europea, salvo en determinadas condiciones. La más general de estas condiciones es la adopción de una decisión de "adecuación" por la Comisión Europea, que determina de ese modo que una jurisdicción concreta es segura para que se le transfieran datos personales. Si no se adopta tal decisión de adecuación, existen ciertos mecanismos que las empresas o los particulares pueden adoptar para transferir datos personales. Dado el escaso número de países que han obtenido una decisión de adecuación favorable, el RGPD tiene importantes consecuencias para los flujos de datos transfronterizos y el comercio digital de bienes y servicios.

En segundo lugar, algunos Estados miembros expresaron preocupaciones económicas, destacando que ese tipo de cláusulas probablemente beneficiarían a las empresas digitales de los Estados Unidos que dominan la economía de datos europea y obstaculizarían los esfuerzos de la Unión por recuperar terreno en la economía digital (Azmeh y otros, 2020). El Consejo Digital Francés, comisión asesora independiente sobre cuestiones digitales creada por el Presidente de Francia, publicó un informe en el que aportaba recomendaciones para abordar las cuestiones digitales en el contexto de las negociaciones de la Asociación Transatlántica de Comercio e Inversión con los Estados Unidos, y recomendaba a Europa que tratase de ganar tiempo en las negociaciones, que avanzase en la elaboración de la estrategia digital europea y que reforzase la capacidad de negociación de la Unión (CNNum, 2014).

Estas reflexiones hicieron que en los acuerdos comerciales bilaterales y regionales europeos se adoptase un enfoque diferente en lo que respecta a la inclusión de cuestiones relacionadas con los datos y la economía digital. La posición inicial de la Unión Europea —reflejada en el Acuerdo de Asociación Económica entre la Unión Europea y el Japón, y en las negociaciones de un acuerdo de libre comercio entre México y la Unión Europea— fue insertar una cláusula de reserva sobre los flujos de datos transfronterizos para que las partes pudieran volver a examinar esta cuestión en un plazo de tres años. Paralelamente, en 2018, los debates internos en la Unión Europea sobre la mejor manera de facilitar el comercio mediante los flujos de datos transfronterizos sin comprometer la privacidad y la protección de datos dieron lugar a la adopción de las "disposiciones horizontales sobre flujos de datos transfronterizos para la protección de datos personales" (Yakovleva e Irion, 2020). Con estas disposiciones, diseñadas para incluirse en futuros acuerdos comerciales de la Unión Europea, se pretende permitir la libre circulación de los datos a través de las fronteras pero manteniendo al mismo tiempo una fuerte protección de la privacidad.

Consisten en tres artículos. El artículo A, relativo a los flujos de datos transfronterizos, compromete a las partes a "garantizar los flujos de datos transfronterizos para facilitar el comercio en la economía digital", y presenta cuatro mecanismos que las partes se comprometen a no utilizar: a) exigir el uso de instalaciones informáticas o elementos de red en el territorio de la parte para el tratamiento de los datos, así como imponer el uso de instalaciones informáticas o elementos de red certificados o aprobados en el territorio de una de las partes; b) exigir la localización de los datos en el territorio de la parte para

[13] Véase, por ejemplo, EDRi (2015) y Open Rights Group (2014).

su almacenamiento o tratamiento; c) prohibir el almacenamiento o el tratamiento en el territorio de la otra parte; d) condicionar la transferencia transfronteriza de datos al uso de instalaciones informáticas o elementos de red en el territorio de las partes, o a requisitos de localización en el territorio de las partes. El artículo A también incluye un mecanismo para revisar la aplicación de esta disposición tres años después de la entrada en vigor del acuerdo.

El artículo B compromete a las partes a reconocer que la protección de los datos personales y de la privacidad es un derecho fundamental, y que "unas normas estrictas a este respecto contribuyen a la confianza en la economía digital y al desarrollo del comercio". Los datos personales se definen en el acuerdo como "cualquier información relativa a una persona física identificada o identificable". El artículo permite a cada parte adoptar y mantener las salvaguardias que considere adecuadas para garantizar la protección de los datos personales y la privacidad, "incluso mediante la adopción y aplicación de normas para la transferencia transfronteriza de datos personales", y en él se subraya que "nada de lo dispuesto en el presente acuerdo afectará a la protección de los datos personales y la privacidad que ofrecen las salvaguardias respectivas de las partes".

El último artículo de las disposiciones compromete a las partes a "mantener un diálogo sobre las cuestiones en materia de regulación que plantea el comercio digital", como el reconocimiento y la facilitación de servicios fiduciarios y de autentificación electrónicos interoperables a nivel transfronterizo, el tratamiento de las comunicaciones de *marketing* directo, la protección de los consumidores en el ámbito del comercio electrónico y cualquier otra cuestión pertinente para el desarrollo del comercio digital. Esta cooperación se centrará en el intercambio de información sobre las legislaciones respectivas de las partes en relación con estas cuestiones, así como en la aplicación de dicha legislación. Es importante señalar que este artículo excluye expresamente de este diálogo las disposiciones relacionadas con la protección de los datos personales y la privacidad, así como con las transferencias transfronterizas de datos personales.

Esa exclusión refleja la opinión general de la Unión Europea de que las negociaciones comerciales y las decisiones de adecuación en materia de datos en el marco del régimen del RGPD son independientes y no deben considerarse parte del mismo proceso. La decisión de adecuación en el marco del RGPD se adopta mediante una propuesta de la Comisión Europea, seguida de un dictamen del Comité Europeo de Protección de Datos, la aprobación de los representantes de los países de la Unión Europea y la adopción definitiva por la Comisión. Al comentar la decisión de conceder la adecuación al Japón, la Comisión Europea destacó que "para la UE, la privacidad no es una mercancía con la que se pueda comerciar. Los diálogos sobre la protección de datos y las negociaciones comerciales con terceros países tienen que seguir vías separadas" (European Commission, 2019). A través de este mecanismo, la Unión Europea pretende avanzar hacia la libre circulación de los datos con sus interlocutores comerciales, pero manteniendo al mismo tiempo sus medidas relativamente estrictas en el ámbito de la privacidad y la protección de los datos personales.

c) *Otros acuerdos comerciales*

Además de los acuerdos comerciales de los Estados Unidos y la Unión Europea que se encuentran en proceso de firma o negociación, hay otros acuerdos comerciales que están empezando a incluir capítulos relativos a los flujos de datos transfronterizos.

En noviembre de 2020, 15 países de la región de Asia y el Pacífico —los 10 países de la Asociación de Naciones de Asia Sudoriental (ASEAN) (Brunei Darussalam, Camboya, Filipinas, Indonesia, Malasia, Myanmar, República Democrática Popular Lao, Singapur, Tailandia y Viet Nam) y 5 asociados (Australia, China, Japón, Nueva Zelandia y República de Corea)— firmaron la Asociación Económica Integral Regional (RCEP). La RCEP es significativa en este sentido, ya que reúne a países en desarrollo y menos adelantados con países mucho más avanzados económicamente (incluidos los tres coorganizadores de las negociaciones de la Iniciativa de Declaración Conjunta), que también son firmes defensores de la inclusión del comercio digital en los acuerdos comerciales. Además, es el primer acuerdo comercial en el que China ha aceptado medidas relativas a los flujos de datos transfronterizos. La sección D del capítulo 12 de la RCEP aborda la cuestión de los flujos de datos transfronterizos.

El artículo 12.14 trata de la ubicación de las instalaciones informáticas, mientras que el artículo 12.15 se centra en los flujos de datos transfronterizos. En general, estas cláusulas se basan en el acuerdo

TPP/TIPAT, pero incorporan cambios con el objetivo de otorgar a los Estados miembros el poder necesario para adoptar medidas que restrinjan los flujos de datos transfronterizos (Leblond, 2020). El artículo 12.15 compromete a las partes a no evitar la transferencia transfronteriza de información por medios electrónicos, cuando esta actividad sea para la realización de un negocio de una persona cubierta, con la salvedad de que dicho compromiso no impide que una parte adopte o mantenga las medidas incompatibles que considere necesarias para alcanzar un objetivo legítimo de política pública, siempre que la medida no se aplique en forma que constituya un medio de discriminación arbitrario o injustificable o una restricción encubierta del comercio. Sin embargo, a diferencia del TPP/TIPAT, en este artículo se añade que nada de lo dispuesto en él impide que una parte adopte "cualquier medida que considere necesaria para la protección de sus intereses esenciales de seguridad" y que "dichas medidas no serán discutidas por otras partes". El artículo 12.14 dispone que ninguna "parte exigirá a una persona cubierta usar o ubicar las instalaciones informáticas en el territorio de esa parte como condición para la realización de negocios en su territorio". Sin embargo, el artículo incluye salvedades similares a las del artículo 12.15; en particular, reconoce a los miembros el derecho de adoptar medidas que sean incompatibles con este compromiso si consideran que estas son "necesarias para la protección de sus intereses esenciales de seguridad", y que "tales medidas no serán discutidas por otras partes".

En resumen, la RCEP difiere del TIPAT en varios aspectos clave. En primer lugar, aunque reitera el compromiso del TIPAT con la circulación de los datos, preserva el derecho de cada país a determinar lo que considera necesario para lograr un objetivo legítimo de política pública. Aunque otra parte pueda alegar que una medida es arbitraria, injustificadamente discriminatoria o una restricción encubierta al comercio, no podrá reclamar que no persiga un objetivo legítimo de política pública y que no sea necesaria. En segundo lugar, las medidas consideradas necesarias para proteger los intereses esenciales de seguridad están plenamente protegidas del escrutinio de otras partes. Por último, actualmente la RCEP no prevé mecanismos de solución de controversias entre Estados en relación con los compromisos relativos a la gobernanza de los datos (aunque sí contempla que esto podría reconsiderarse con la revisión del acuerdo), sino que más bien promueve las consultas de buena fe entre las partes (Streinz, 2021).

Las negociaciones del Acuerdo sobre el Comercio de Servicios son otro foro en el que se han debatido cuestiones relacionadas con los flujos de datos transfronterizos (entre 23 países, incluidos los Estados Unidos y la Unión Europea). Para el Acuerdo se habían planteado las mismas propuestas en relación con los flujos de datos que se incluían en el TPP, en particular el compromiso relativo a la libre circulación de los datos y la prohibición de su localización. Sin embargo, las negociaciones del Acuerdo sobre el Comercio de Servicios se han estancado en los últimos años, en parte debido a los desacuerdos entre los Estados Unidos y la Unión Europea en relación con los flujos de datos transfronterizos (Malcolm, 2016).

Además de los mencionados, existen otros acuerdos comerciales que incluyen cláusulas relacionadas con los flujos de datos transfronterizos, aunque son muy pocos los que prevén compromisos vinculantes respecto de la libre circulación de los datos. Una de esas excepciones es el acuerdo de libre comercio entre México y Panamá, que incluye un compromiso vinculante sobre el flujo transfronterizo de información. Otros acuerdos prevén la cooperación de los órganos reguladores sobre los flujos de datos transfronterizos, aunque no contienen compromisos vinculantes. Algunos ejemplos son el acuerdo de libre comercio entre Costa Rica y Colombia, el acuerdo de libre comercio entre Chile y Colombia, el acuerdo de libre comercio entre Panamá y Singapur y el acuerdo de libre comercio entre el Perú y la República de Corea (Wu, 2017). Otro ejemplo es el acuerdo de libre comercio entre el Canadá y Colombia, Honduras, el Perú y la República de Corea, que compromete a las partes a colaborar para "mantener los flujos transfronterizos de información como elemento esencial para fomentar un entorno dinámico para el comercio electrónico".

En la región de América Latina y el Caribe, los procesos de cooperación e integración se han caracterizado históricamente por su alcance subregional y su naturaleza fluctuante. La agenda digital no es una excepción, aunque su carácter incipiente debe considerarse fruto de los esfuerzos de aprendizaje necesarios para abordar un tema nuevo, cada vez más central para el desarrollo económico y sostenible. Hay pocas pruebas de los efectos de los flujos de datos transfronterizos en el comercio de la región, así como muy pocas referencias a su impacto en el valor económico (Meltzer, 2018).

La Alianza del Pacífico es el bloque más dinámico de América Latina en lo que respecta a las disposiciones relacionadas con el comercio digital y los flujos de datos transfronterizos. Esta ha adoptado disposiciones específicas de carácter puramente normativo en sus acuerdos fundacionales, como reflejo de los acuerdos comerciales concluidos en el marco del TIPAT. El grupo de países que conforman la Alianza del Pacífico (Chile, México, Colombia y Perú) ha tendido a concertar acuerdos con este tipo de contenidos, tanto de forma conjunta como unilateral. De hecho, los textos fundacionales de la Alianza del Pacífico incluyen más de 50 disposiciones específicas con un alcance considerable, en la medida en que regulan aspectos como la transferencia transfronteriza de información y la ubicación de las instalaciones informáticas. Aunque "las Partes reconocen que pueden tener sus propios requisitos regulatorios para la transferencia de información por medios electrónicos" (artículo 13.11 del Primer Protocolo Modificatorio del Protocolo Adicional al Acuerdo Marco), se aclara que "ninguna Parte podrá exigir a una persona cubierta usar o localizar instalaciones informáticas en el territorio de esa Parte, como condición para el ejercicio de su actividad de negocios" (artículo 13.11 *bis*). En junio de 2019, los países de la Alianza del Pacífico presentaron una comunicación en el contexto de la Iniciativa de Declaración Conjunta, en la que proponían un proyecto de texto para una disposición sobre cooperación que decía lo siguiente: "Reconociendo la naturaleza global del comercio electrónico, las Partes afirman la importancia de: … c) colaborar para mantener los flujos transfronterizos de información como un elemento esencial en el fomento de un entorno dinámico para el comercio electrónico"[14].

Los países del Cono Sur de América Latina, a excepción de Chile, participan desde finales de los años ochenta en el Mercado Común del Sur (MERCOSUR). Hasta hace poco, este foro apenas había realizado avances en la adopción de una normativa específica sobre el comercio digital, en particular sobre los flujos de datos transfronterizos. Sin embargo, en enero de 2021 los países del MERCOSUR aprobaron el Acuerdo sobre Comercio Electrónico, canalizado institucionalmente a través de una Decisión del Consejo del Mercado Común (Decisión CMC 15/20). Este acuerdo cumple la misma función que un capítulo sobre comercio electrónico de un acuerdo comercial (como en el caso de la Alianza del Pacífico o el Tratado de Libre Comercio de Centroamérica (CAFTA)), y se basa en las disposiciones propuestas por la Alianza del Pacífico en 2018. En este sentido, incorpora algunos elementos de interés en lo que respecta a los flujos de datos transfronterizos: el reconocimiento de la importancia de evitar obstáculos que constituyan una restricción encubierta al comercio realizado por medios electrónicos, la exigencia de disponer de mecanismos de protección de los datos personales, la prohibición de los derechos de aduana sobre los productos digitales procedentes de sus países miembros y la prohibición de los requisitos relativos a la ubicación de las instalaciones informáticas. Por otro lado, las partes en el MERCOSUR, con la excepción del Paraguay, han comenzado a incluir en sus acuerdos bilaterales disposiciones específicas sobre los flujos de datos transfronterizos.

El CAFTA engloba un conjunto de acuerdos comerciales y puede clasificarse como un acuerdo plurilateral subregional, entre cuyos miembros están Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y la República Dominicana, además de los Estados Unidos. Como en el caso de la Alianza del Pacífico, se trata de un acuerdo generado fundamentalmente por alianzas bilaterales y subregionales en torno a los Estados Unidos. El CAFTA ha servido de plataforma para asentar los principios comerciales de sus países miembros, e incluye disposiciones sobre el comercio digital. El acuerdo fundacional con los Estados Unidos, firmado en 2004, incluye un capítulo sobre el comercio electrónico. Los acuerdos celebrados con México, en 2011, y la Unión Europea, en 2012 (título III), también contienen un capítulo similar. Aunque el capítulo sobre las telecomunicaciones del segundo de ellos es más completo y detallado, su capítulo dedicado al comercio electrónico es mucho más limitado, si bien se dispone en él también que "el desarrollo del comercio electrónico deberá ser compatible con los estándares internacionales de protección de datos, con miras a asegurar la confianza de los usuarios del comercio electrónico".

Algunos hitos logrados en la región del Caribe —como el Tratado de Chaguaramas Revisado, la Visión y Hoja de Ruta para la creación de un Espacio Único de las TIC en la Comunidad del Caribe (CARICOM), las iniciativas regionales de intercambio de información, el proyecto de armonización de las políticas y la legislación de las TIC en todo el Caribe (HIPCAR) y el Foro de Gobernanza de Internet del Caribe—

[14] Comunicación de Chile, Colombia, México y el Perú, Declaración Conjunta sobre Comercio Electrónico (INF/ECOM/35), 20 de junio de 2019.

abordan o facilitan los flujos de datos transfronterizos. Aunque se está avanzando en la armonización de los marcos legislativos y normativos en materia de protección de datos y privacidad a nivel regional, hasta el momento ha habido muy pocas medidas efectivas que se hayan materializado en enfoques regionales de la regulación de los flujos de datos transfronterizos, aparte de algunas recomendaciones y directrices generales (Brathwaite y Remy, 2020).

Sin embargo, no hay pruebas de que alguna de las iniciativas de cooperación latinoamericanas mencionadas haya ido más allá de su impulso inicial. Asimismo, la primera generación de disposiciones sobre el comercio digital, que situó a la Alianza del Pacífico entre los acuerdos más avanzados en ese ámbito, no ha dado lugar a una segunda oleada de políticas conjuntas. En rigor, existe una gran diversidad de enfoques en lo que respecta a los asociados externos y las estrategias de inserción internacional, cuya evolución será clave para el futuro de la Alianza del Pacífico. Por ejemplo, Chile está profundizando en el enfoque adoptado por primera vez con el TIPAT a través del Acuerdo de Asociación de Economía Digital (DEPA) (véase la sección D), el primer acuerdo comercial enteramente dedicado a la economía digital (con Singapur y Nueva Zelandia), al tiempo que concierta acuerdos bilaterales con los países miembros del MERCOSUR; Colombia y el Perú han concertado un acuerdo con la Unión Europea, el Japón y la República de Corea; y México ha firmado el T-MEC y el Acuerdo Comercial entre la Unión Europea y México, así como las nuevas versiones de sus acuerdos respectivos con los Estados Unidos y el Canadá, por un lado, y con la Unión Europea, por otro. Todos ellos incluyen cuestiones relacionadas con el comercio electrónico o el comercio digital.

En lo que respecta a África, la Decisión sobre la Zona de Libre Comercio Continental Africana (AfCFTA) (Assembly/AU/4(XXXIII)), adoptada en el 33er período ordinario de sesiones de la Asamblea de la Unión Africana, los días 9 y 10 de febrero de 2020, en principio disponía que las negociaciones de la fase III, dedicadas a la elaboración de un protocolo de la AfCFTA sobre el comercio electrónico, comenzaran inmediatamente después de la conclusión de las negociaciones de la fase II (inversión, propiedad intelectual y política de competencia). En la decisión se "insta a los Estados miembros a que revisen de forma crítica las ofertas que les están haciendo sus asociados bilaterales para que suscriban con ellos instrumentos jurídicos bilaterales sobre el comercio electrónico, a fin de garantizar que África pueda negociar y aplicar un protocolo de la AfCFTA sobre el comercio electrónico que le otorgue plena autoridad sobre todos los aspectos relacionados con esta esfera, por ejemplo los datos". Desde entonces, la Asamblea de la Unión Africana ha decidido adelantar las negociaciones sobre el comercio electrónico y ha fijado como fecha límite para las negociaciones de las fases II y III el 31 de diciembre de 2021.

La Estrategia de Transformación Digital de la Unión Africana (2020-2030) —que debe actualizarse mediante la aplicación de estrategias a nivel nacional— puede dar algunas pistas sobre la posición de los países africanos respecto de determinadas cuestiones relativas a los flujos de datos. Entre los objetivos específicos de la estrategia están la entrada en vigor de la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo), y la promoción de normas abiertas y de sistemas de interoperabilidad para establecer marcos de confianza transfronterizos y garantizar la protección de los datos personales y la privacidad. En la estrategia se constata la falta de marcos de supervisión de la protección de datos y se señala el almacenamiento/tratamiento/manejo de datos como punto débil del continente. Además, se señala que la realización de los objetivos de transformación digital para África requiere políticas adecuadas y un entorno propicio que, según se explica, incluye "una regulación destinada a permitir la libre circulación de los datos no personales". En otra parte de la estrategia se trata la infraestructura digital y se indica que África necesita una infraestructura de centros de datos a fin de ahorrar costos, pero también por motivos de soberanía sobre los datos, para garantizar la localización de todos los datos personales de la ciudadanía africana.

3. Resultados de la regulación de los flujos de datos transfronterizos mediante acuerdos comerciales

A pesar de que cada vez son más los países que se esfuerzan por regular la cuestión de los flujos de datos transfronterizos en el marco de acuerdos comerciales, ha resultado difícil lograr un consenso a nivel multilateral y se han producido mayores avances a través de determinados acuerdos bilaterales y

regionales. No obstante, incluso en estos casos no hay una participación suficiente de los países con economías menos avanzadas digitalmente. En el momento en que se redactó el presente informe, por ejemplo, ningún país africano había concertado acuerdos comerciales que contuvieran compromisos relacionados con los flujos de datos.

Muchos países en desarrollo siguen mostrándose reticentes a ceder el control de sus datos mediante cláusulas vinculantes de acuerdos comerciales sin conocer bien todas las implicaciones que puede tener esa medida. Dada la concentración mundial de las plataformas, la facilitación de la "libre circulación de los datos" —tal como se aborda en los acuerdos comerciales— puede dar lugar en la práctica, en las circunstancias actuales, a una "circulación unidireccional" de los datos desde las economías menos avanzadas digitalmente.

Como se ha comentado en este capítulo, puede ser difícil que las negociaciones comerciales obtengan un resultado que permita garantizar el funcionamiento eficaz de una Internet global y, al mismo tiempo, tenga en cuenta las oportunidades y los desafíos de desarrollo multidimensionales asociados a los flujos de datos. En primer lugar, aunque el resultado de los acuerdos comerciales puede tener implicaciones significativas para la gobernanza de Internet, los agentes no gubernamentales no suelen tener el mismo acceso al proceso de negociación comercial que a los debates multilaterales sobre la gobernanza de Internet.

En segundo lugar, el tratamiento de los flujos de datos transfronterizos como una cuestión esencialmente comercial pone a los países en desarrollo en una posición difícil, ya que la mayoría de ellos carece de las capacidades necesarias para abordar esta cuestión en el ámbito comercial. En consecuencia, pueden verse presionados a aceptar ciertas normas sobre los flujos de datos como parte de acuerdos que les proporcionen beneficios en otras esferas del comercio. La negociación en torno a diversas esferas temáticas y sectores económicos puede ser una forma válida de avanzar en las negociaciones y llegar a un acuerdo, pero resulta menos propicia para ofrecer soluciones integrales a problemas multidimensionales complejos como los flujos de datos (Burri, 2017).

En tercer lugar, al incluir compromisos vinculantes sobre los flujos de datos en los acuerdos comerciales, se deja en manos de los mecanismos de resolución de diferencias comerciales la determinación de si las medidas nacionales sobre los datos —utilizando la formulación del TIPAT— se aplican "de forma que constituya[n] un medio de discriminación arbitraria o injustificable, o una restricción encubierta al comercio", y no imponen "restricciones a las transferencias de información mayores a las que se requieren para alcanzar el objetivo". En última instancia, la medida en que las partes se comprometan a la libre circulación de los datos en los acuerdos comerciales determinará si, por ejemplo, la privacidad de los datos debe ser protegida por los países soberanos y la Unión Europea, o si se incorpora a un ordenamiento jurídico supranacional en la esfera del comercio (Yakovleva e Irion, 2020).

Partiendo de este contexto, en la siguiente sección se examinan algunos procesos internacionales que abordan la regulación de los flujos de datos transfronterizos más allá del ámbito comercial.

D. INICIATIVAS INTERNACIONALES Y REGIONALES QUE ABORDAN LOS FLUJOS DE DATOS TRANSFRONTERIZOS MÁS ALLÁ DE LA ESFERA COMERCIAL

Además del sistema de comercio, existen otros foros internacionales y regionales que acogen debates sobre los flujos de datos transfronterizos. A nivel regional, algunos países en desarrollo se apoyan ahora en bloques regionales como la Unión Africana y la ASEAN para establecer mecanismos coordinados de interoperabilidad y confianza digital transfronteriza, así como marcos regionales comunes para los flujos de datos[15]. En el mundo desarrollado, la Unión Europea es otro ejemplo de bloque que intenta aumentar

[15] Véase Unión Africana, 2020; y "1st ASEAN Digital Ministers' Meeting (ADGMIN) 2020 Implementing Guidelines for ASEAN Data Management Framework and ASEAN Cross Border Data Flows Mechanism" (disponible en https://asean.org/storage/1-Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows_Final.pdf).

su competitividad digital a través de iniciativas regionales como GAIA-X (analizada en el capítulo IV). Uno de los objetivos comunes de estos mecanismos de cooperación es facilitar el desarrollo del sector digital en la región y crear oportunidades de mercado más adaptadas a los agentes regionales a fin de reducir la dependencia respecto de las empresas de los Estados Unidos y China. Una cooperación regional significativa en materia de gobernanza de los datos podría aumentar la competitividad digital de las economías en desarrollo y otorgarles ciertas ventajas frente a las empresas tecnológicas dominantes (Foster y Azmeh, 2020), pero, en última instancia, es necesario y deseable adoptar un enfoque coordinado a nivel internacional en relación con los flujos de datos. En esta sección se ofrece un panorama general de algunos de estos foros internacionales, así como de diversas iniciativas regionales, que guardan relación con los flujos de datos transfronterizos. En primer lugar se tratan los foros relacionados con la esfera económica en sentido amplio y, a continuación, se examinan los foros e iniciativas más allá de esa esfera.

1. Iniciativas sobre los flujos de datos transfronterizos en el ámbito económico más amplio

a) El G20 y la "circulación de datos libre y de confianza"

En un discurso pronunciado en Davos en 2019, el Primer Ministro del Japón destacó la necesidad de una gobernanza mundial de los datos y pidió a los líderes mundiales que iniciaran conversaciones sobre lo que dio en llamar la "circulación de datos libre y de confianza". Propuso abordar esta cuestión solicitando a la reunión del G20 en Osaka que se "pusiese en marcha una nueva vía para estudiar la gobernanza de los datos, denominada 'Vía de Osaka', en el marco de la Organización Mundial del Comercio" (Hurst, 2019). En la declaración de los líderes se destacó la importancia de los flujos de datos, al tiempo que se reconocieron los desafíos relacionados con la privacidad, la seguridad y la protección de datos. En la declaración se pedía además que se facilitara la libre circulación de los datos, reforzando al mismo tiempo la confianza de los consumidores y las empresas, con el fin de crear una circulación de datos libre y de confianza. Asimismo, se reafirmaba la importancia de la interrelación entre el comercio y la economía digital, se tomaba nota de los debates en curso en el marco de la Iniciativa de Declaración Conjunta sobre el comercio electrónico y se insistía en la importancia del programa de trabajo sobre el comercio electrónico de la OMC[16].

Algunas de las ideas sobre cómo abordar esta cuestión se discutieron en el grupo de trabajo sobre comercio, inversiones y globalización, integrado en Think-20 (T20), uno de los grupos de contacto de los que se sirve el G20 para comunicarse con los grupos de reflexión internacionales. En un informe de políticas sobre "la economía digital para el desarrollo económico: libre circulación de los datos y políticas de apoyo" (Chen y otros, 2019) se proponían una serie de políticas relacionadas con la economía digital. En lo que respecta a los flujos de datos transfronterizos, se pedía que por defecto se permitiese la libre circulación de los datos y que la intervención de los poderes públicos solo se permitiera en determinadas circunstancias, por ejemplo por los posibles efectos en importantes valores o preocupaciones sociales distintos de la eficiencia económica, como la protección de la privacidad, la moral pública, la salud humana o la seguridad nacional. En el informe de políticas se pedía que el objetivo último fuera un acuerdo comercial multilateral en el marco de la OMC, pero se reconocía que la dificultad que ello entrañaba podía llevar a los países a buscar otras vías.

La iniciativa, sin embargo, carece de consenso en el marco del G20, ya que Indonesia, la India y Sudáfrica se han negado a suscribirla, argumentando que socava los procesos de negociación multilaterales basados en la adopción de decisiones por consenso propios de las negociaciones mundiales sobre comercio, y priva a los países en desarrollo de margen de actuación en lo que respecta a la economía digital (Kanth, 2019).

[16] Véase el discurso del Primer Ministro Abe en la Reunión Anual del Foro Económico Mundial, "Toward a New Era of 'Hope-Driven Economy'", 23 de enero de 2019 (disponible en https://www.mofa.go.jp/ecm/ec/ page4e_000973.html); véase también la Declaración de Osaka de los Líderes del G20 (disponible en https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html; y la Declaración de Osaka sobre la Economía Digital (disponible en https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf).

Aunque esta iniciativa todavía no se ha materializado, su posible impacto dependerá en gran medida de la definición de confianza. No se han observado muchos avances en el contexto del G20. En la Cumbre de Riad, celebrada los días 21 y 22 de noviembre de 2020, los dirigentes declararon: "Reconocemos la importancia de la circulación de datos libre y de confianza y de los flujos de datos transfronterizos. Reafirmamos el papel de los datos en el desarrollo. Apoyamos que se fomente un entorno abierto, justo y no discriminatorio y se proteja y empodere a los consumidores, abordando al tiempo los desafíos relacionados con la privacidad, la protección de datos, los derechos de propiedad intelectual y la seguridad. Si seguimos afrontando estos desafíos, con arreglo a los marcos jurídicos aplicables, podremos facilitar aún más la libre circulación de los datos y reforzar la confianza de los consumidores y las empresas"[17]. El G20 cuenta con el apoyo de la OCDE, que al parecer está trabajando en la puesta en práctica del concepto de "circulación de datos libre y de confianza"[18].

No obstante, en la reunión de ministros de tecnología y asuntos digitales del G7, celebrada el 28 de abril de 2021, estos declararon: "Tomando como base la Declaración de Osaka de los Líderes del G20, de 2019, la Declaración Ministerial sobre comercio y economía digital del G20, de 2019, y la Declaración de Riad de los Líderes del G20, de 2020, recurriremos a nuestros valores compartidos como naciones con ideas afines, democráticas, abiertas y orientadas al exterior para apoyar un plan de trabajo que permita aprovechar los beneficios de la circulación de datos libre y de confianza. Para lograr este objetivo, aprobamos una Hoja de Ruta para la Cooperación en relación con la Circulación de Datos Libre y de Confianza (anexo 2) en la que se establece nuestro plan para lograr avances tangibles en esta cuestión, generar confianza para que las empresas y los particulares utilicen la tecnología y promover la creación de valor económico y social"[19].

b) Acuerdo de Asociación de Economía Digital

El Acuerdo de Asociación de Economía Digital (DEPA) fue suscrito por Nueva Zelandia, Chile y Singapur en junio de 2020, y entró en vigor en enero de 2021. El acuerdo aborda una serie de cuestiones relacionadas con la economía digital. En concreto, los artículos 4.2, 4.3 y 4.4 tratan cuestiones relacionadas con los flujos de datos transfronterizos y la localización de los datos. Reconociendo la importancia de la protección de la información personal, el artículo 4.2 compromete a cada parte a adoptar un marco jurídico para la protección de la información personal, y enumera varios criterios para dicho marco. El acuerdo también exige a los países que promuevan la compatibilidad y la interoperabilidad entre sus diferentes regímenes de protección de la información personal, y presenta algunos posibles mecanismos para lograr esa comparabilidad. El artículo 4.2 también contiene compromisos de transparencia y no discriminación en la adopción de un marco jurídico para la protección de los datos personales.

El artículo 4.3 se centra en los flujos de datos transfronterizos, y compromete a cada parte a permitir la transferencia transfronteriza de datos, incluida la información personal, cuando esta actividad sea para la realización de un negocio de una persona cubierta, pero establece excepciones en las que los Estados miembros pueden restringir estos flujos. El artículo 4.4 compromete a los miembros a no imponer el uso de instalaciones informáticas locales para el almacenamiento de datos como condición para la realización de negocios, pero permite a los miembros adoptar medidas incompatibles con este principio para alcanzar un objetivo legítimo de política pública, siempre que dichas medidas no sean discriminatorias ni representen restricciones encubiertas al comercio y no impongan restricciones al uso o la ubicación de las instalaciones informáticas mayores que las necesarias para lograr el objetivo. En apoyo a estos compromisos, el DEPA ofrece acceso a un mecanismo de solución de controversias en caso de infracción.

[17] Véase la Declaración de los Lideres del G20 de la Cumbre de Riad, 21 y 22 de noviembre de 2020 (disponible en https://www.consilium.europa.eu/media/46883/g20-riyadh-summit-leaders-declaration_en.pdf); y la Declaración Ministerial de la Reunión de Ministros de Economía Digital del G20, 22 de julio de 2020 (disponible en http://www.g20.utoronto.ca/2020/G20SS_Declaration_G20_Digital_Economy_Ministers_Meeting_EN.pdf).

[18] Véase, por ejemplo, OECD (2020) y Casalini y otros (2021). Este tema también ha sido abordado por el Foro Económico Mundial (WEF, 2020d y 2021).

[19] Véase la Declaración de los Ministros de Tecnología y Asuntos Digitales del G7, 28 de abril de 2021 (disponible en http://www.g8.utoronto.ca/ict/2021-digital-tech-declaration.html).

La adhesión de Singapur al DEPA se inscribe en los esfuerzos más amplios realizados por este país para suscribir acuerdos similares. Además del DEPA, Singapur y Australia firmaron el Acuerdo de Economía Digital entre Singapur y Australia, y están negociando un acuerdo similar con la República de Corea. Singapur, como reflejo de su economía pequeña y muy abierta, ve importantes ventajas en posicionarse como centro de referencia para la libre circulación de los datos a través de las fronteras.

c) Foro de Cooperación Económica de Asia y el Pacífico

En el Foro de Cooperación Económica de Asia y el Pacífico (APEC), que abarca 21 economías de la región de Asia y el Pacífico, se han venido celebrando debates en torno a la gobernanza de la economía digital y los flujos de datos transfronterizos[20]. Uno de los primeros resultados fue la adopción del Plan de Acción sobre el Comercio Electrónico del APEC, en 1998, y la posterior creación del Grupo Directivo sobre el Comercio Electrónico del APEC, en 1999. Otros hitos importantes fueron la adopción del Programa de Acción para la Nueva Economía y la creación del Grupo Directivo Especial sobre la Economía de Internet.

En lo que respecta a los flujos de datos transfronterizos, varias iniciativas del APEC pretenden facilitar la circulación de los datos, manteniendo al mismo tiempo medidas estrictas de protección de la privacidad. La Hoja de Ruta sobre Internet y la Economía Digital del APEC, adoptada en 2017, hacía hincapié en la facilitación de la libre circulación de los datos dentro del APEC y en la importancia de promover la interoperabilidad y la cooperación en materia de regulación en esferas relacionadas con la economía digital.

Una de las iniciativas importantes del APEC es el Sistema de Normas Transfronterizas de Privacidad (CBPR). El sistema se adoptó en 2011 sobre la base del Marco de Privacidad del APEC, de 2005. El CBPR es un sistema de certificación de la privacidad al que las empresas pueden acogerse para demostrar que cumplen los requisitos relativos a la protección de la privacidad de los datos. Impone requisitos específicos tanto a los Estados miembros como a las empresas que deseen obtener la certificación. A nivel nacional, exige a los Estados miembros que demuestren la aplicabilidad de las medidas destinadas a combatir las infracciones de las empresas certificadas, e incluye un mecanismo de cooperación transfronteriza. Si desean obtener la certificación, las empresas deben implantar medidas para garantizar la seguridad de los datos personales, un mecanismo para recibir e investigar reclamaciones y un sistema para que los consumidores puedan acceder a sus datos personales y corregirlos, entre otros requisitos. El sistema CBPR fue reconocido en el T-MEC, y en 2017 también fue adoptado por el Japón como mecanismo de transferencia válido (Harris, 2018). El APEC ha desarrollado también el sistema de Reconocimiento de la Privacidad para los Encargados del Tratamiento, con el que se certifica a los responsables del tratamiento de los datos.

Para dar aplicación a esas medidas, el APEC elaboró el Acuerdo de Aplicación Transfronteriza de la Privacidad. Este aporta un marco de cooperación regional para la aplicación de la legislación sobre la privacidad mediante el establecimiento de vínculos entre las autoridades responsables de cada miembro, y ofrece un mecanismo para que estas puedan intercambiar información.

Con esos diferentes protocolos y programas, el APEC está desempeñando un papel importante en la creación de un marco regulador de los flujos de datos transfronterizos. Sin embargo, es importante señalar que la participación en estos programas es voluntaria y que los Estados miembros pueden decidir si se adhieren o no a un acuerdo o programa específico. Por ejemplo, en la actualidad solo nueve miembros del APEC han adoptado el sistema CBPR[21].

d) Asociación de Naciones de Asia Sudoriental

La ASEAN es otro foro asiático en el que se desarrollan actividades de cooperación regional en materia de flujos de datos transfronterizos. En el Plan de la Comunidad Económica de la ASEAN para 2025 se destaca la importancia del comercio electrónico como cauce para el comercio transfronterizo y las inversiones extranjeras. Este enfoque se plasmó en el Acuerdo sobre Comercio Electrónico de la ASEAN, firmado en 2019. En él, los Estados miembros reconocen la importancia de permitir que la información

[20] Para consultar la lista de los miembros del APEC, véase https://www.apec.org/about-us/about-apec.

[21] Véase “Participation in the APEC Cross-Border Privacy Rules (CBPR) System affords Asia-Pacific Economic Cooperation members a unique opportunity to work” (disponible en http://cbprs.org/government/).

traspase las fronteras, "siempre y cuando esta información se utilice con fines comerciales, y con arreglo a las leyes y reglamentos respectivos"[22]. Sobre la base de este reconocimiento, los Estados miembros acordaron facilitar el comercio electrónico transfronterizo esforzándose por eliminar o reducir al mínimo los obstáculos a la circulación de la información a través de las fronteras, aunque establecieron salvaguardias para garantizar la seguridad y la confidencialidad de la información y el cumplimiento de otros objetivos legítimos de política pública.

El acuerdo también incluye una restricción que impide a los miembros exigir a las empresas y personas de otros Estados miembros que ubiquen sus instalaciones informáticas en su jurisdicción como condición para operar (con la excepción de los servicios financieros). Además, compromete a los Estados miembros a adoptar medidas para proteger la información personal. En cuanto a la protección de datos, en 2016 la ASEAN adoptó el Marco de Protección de los Datos Personales, cuyo objetivo es "reforzar la protección de los datos personales en el marco de la ASEAN y facilitar la cooperación entre los Participantes, con el fin de contribuir a la promoción y el crecimiento del comercio regional y mundial y la circulación de la información".

El marco se plantea como una declaración de intenciones de los participantes y no comporta obligaciones legales exigibles. Comprende algunos principios que los Estados miembros reconocen y se proponen tener en cuenta al elaborar sus leyes nacionales[23]. En relación con las transferencias transfronterizas de datos, el marco dispone que "antes de transferir datos personales a otro país o territorio, la organización deberá obtener el consentimiento del titular para que sus datos se transfieran al extranjero o adoptar medidas razonables para garantizar que la organización receptora proteja los datos personales con arreglo a estos principios". Sobre esta base, la ASEAN adoptó el Marco de Gobernanza de los Datos Digitales, aprobado en 2018, "como iniciativa encaminada a mejorar la gestión de los datos, facilitar la armonización de las normativas en materia de datos entre los Estados miembros de la ASEAN y promover los flujos de datos dentro del territorio de la ASEAN"[24]. En enero de 2021, la primera reunión de ministros encargados de asuntos digitales de la ASEAN aprobó el Marco de Gestión de Datos de la ASEAN y las Cláusulas Contractuales Modelo para los Flujos de Datos Transfronterizos. También aprobó el Plan Maestro Digital de la ASEAN para 2025[25].

2. Iniciativas relativas a los flujos de datos transfronterizos más allá de la esfera económica y comercial

En tanto que las iniciativas anteriormente expuestas están vinculadas a la agenda económica y comercial en sentido amplio, en esta sección se examinan algunas otras iniciativas sobre la gobernanza de los datos que se están desarrollando más allá de la esfera económica a nivel internacional y regional.

a) Directrices sobre privacidad de la OCDE

Además de la labor relativa a los flujos de datos transfronterizos en el contexto de su proyecto "Going Digital" y su apoyo al G20, la OCDE lleva muchos decenios ocupándose de los flujos de datos transfronterizos, centrándose especialmente en la privacidad. En 2007, el Consejo de la organización

[22] Véase el Acuerdo sobre Comercio Electrónico de la ASEAN (disponible en http://agreement.asean.org/media/download/20190306035048.pdf).

[23] Estos principios incluyen el consentimiento, la notificación y la finalidad de la recopilación de datos personales; la exactitud y seguridad de esos datos; el derecho del titular a acceder a los datos y corregirlos; la conservación de los datos; y la rendición de cuentas.

[24] Véase ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Personal Data (disponible en https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf), y ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Digital Data Governance (disponible en https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf).

[25] Véase "1st ASEAN Digital Ministers' Meeting approves Singapore-led initiatives on ASEAN Data Management Framework, ASEAN Model Contractual Clauses for Cross Border Data Flows and ASEAN CERT Information Exchange Mechanism" (disponible en https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meeting); y "ASEAN Digital Masterplan 2025" (disponible en https://asean.org/storage/ASEAN-Digital-Masterplan-2025.pdf).

adoptó un conjunto de recomendaciones relativas a la cooperación transfronteriza para la aplicación de las leyes que protegen la privacidad (OECD, 2007). En las recomendaciones se reconocían el aumento y los beneficios de los flujos transfronterizos de datos, incluidos los datos personales, y los desafíos y preocupaciones que este aumento había planteado en relación con la privacidad y la protección de datos. A fin de evitar en lo posible la perturbación de estos flujos, el Consejo de la OCDE destacó la necesidad de adoptar un enfoque más global e integral que promoviese una cooperación más estrecha en relación con las cuestiones de privacidad y protección de datos. El Consejo de la OCDE recomendó a los Estados miembros que adoptaran medidas para:

- Mejorar sus marcos nacionales de aplicación de la legislación sobre privacidad a fin de facilitar la cooperación de sus autoridades con las autoridades extranjeras.
- Desarrollar mecanismos internacionales eficaces que facilitasen la cooperación en la aplicación transfronteriza de la legislación sobre privacidad.
- Prestarse asistencia mutua en la aplicación de las leyes de protección de la privacidad, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en la investigación y el intercambio de información, con sujeción a las garantías adecuadas.
- Incluir a las partes interesadas pertinentes en los debates y las actividades destinadas a fomentar la cooperación en la aplicación de las leyes que protegen la privacidad.

En 2013, la OCDE actualizó sus directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, de 1980 (OECD, 2013b). Estas directrices incluyen medidas de protección y establecen límites para la recopilación de datos personales, y reconocen los derechos de los titulares a acceder a sus datos. Tomando como base esas medidas de protección, en las directrices se pide a los países miembros que se abstengan de imponer cualquier restricción a los flujos transfronterizos de datos personales con otros Estados miembros, siempre y cuando los otros países observen las directrices y dispongan de mecanismos efectivos para garantizar su aplicación. En este contexto, en las directrices se señala que las restricciones a los flujos transfronterizos de datos personales deben ser proporcionadas. Se pide a los Estados miembros que: desarrollen estrategias nacionales de privacidad; adopten legislación sobre protección de la privacidad; designen autoridades que se encarguen de velar por la privacidad; fomenten y apoyen la autorregulación mediante, por ejemplo, códigos de conducta; y proporcionen medios razonables para que los titulares de los datos ejerzan sus derechos, entre otras medidas. En las directrices se pide a los Estados miembros que desarrollen medidas para facilitar la aplicación transfronteriza de las medidas de privacidad y que apoyen la elaboración de acuerdos internacionales que promuevan la interoperabilidad entre los marcos de privacidad.

En 2014, la OCDE adoptó los “Principios relativos a la formulación de políticas de Internet”, un conjunto de recomendaciones que hacían hincapié en el apoyo a la libre circulación de los datos transfronterizos y la necesidad de garantizar la compatibilidad entre los distintos regímenes nacionales, para evitar en lo posible la perturbación de estos flujos. El primer principio es “promover y proteger la libre circulación mundial de la información” (OECD, 2014).

b) Convenio 108 y Convenio 108+ del Consejo de Europa

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa (comúnmente conocido como “Convenio 108”)[26] es el único instrumento multilateral jurídicamente vinculante en materia de protección de la privacidad y los datos personales abierto a cualquier país del mundo. El Convenio 108 se abrió a la firma en 1981 y, desde entonces, ha influido en diversas normativas internacionales, regionales y nacionales sobre privacidad. Actualmente consta de 55 Estados partes, de los cuales 8 no son europeos. Además, el Comité del Convenio cuenta con más de 25 observadores, y constituye un foro mundial de más de 70 países que colaboran en la protección de datos.

[26] Véase Details of Treaty No.108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

El Convenio 108 se actualizó recientemente para adaptar este instrumento histórico a las nuevas realidades de un mundo cada vez más conectado, así como para reforzar su aplicación efectiva. El Protocolo (STCE núm. 223) que modifica el Convenio 108 se abrió a la firma en octubre de 2018, y desde entonces ha sido firmado y ratificado por un gran número de países. Una vez que entre en vigor, el protocolo de enmienda cumplirá dos objetivos esenciales: facilitar los flujos de datos y promover el respeto por la dignidad humana en la era digital[27].

El Convenio 108+ es el único tratado internacional multilateral abierto y jurídicamente vinculante sobre el derecho a la protección de datos. Reconociendo su potencial único para convertirse en el instrumento mundial de protección de datos, el Relator Especial de las Naciones Unidas sobre el derecho a la privacidad recomendó que se alentara "a todos los Estados Miembros de las Naciones Unidas a ratificar el Convenio 108+"[28].

El Convenio crea un espacio jurídico común para todo el mundo en materia de privacidad y protección de datos. Garantiza a las personas la posibilidad de ejercer plenamente su derecho a la vida privada y la protección de sus datos personales y, en particular, a saber qué datos se recopilan, almacenan y tratan, cómo y por quién; rectificar sus datos y solicitar su supresión; y beneficiarse de mecanismos de reparación sumamente sólidos en caso de que se vulneren sus derechos.

Con sus normas equilibradas, establece el nivel convenido de protección del que deben gozar los particulares en la era digital para salvaguardar su dignidad y disfrutar plenamente de su derecho a la libre determinación informativa. El Convenio 108+ representa una herramienta viable para facilitar las transferencias internacionales de datos, y garantiza al mismo tiempo un nivel adecuado de protección a las personas de todo el mundo.

c) Convención de Malabo

En 2014, la Unión Africana adoptó la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, generalmente conocida como la Convención de Malabo (Abass, 2017). Su objetivo es proporcionar un marco normativo que regule la recopilación y el tratamiento de datos personales en todos los Estados miembros de la Unión Africana. Los firmantes de la Convención se comprometen a establecer un marco jurídico para reforzar la protección de los datos personales y a publicar las infracciones en materia de privacidad "sin perjuicio del principio de libre circulación de los datos personales" (African Union, 2014). A nivel nacional, exige que cada país designe una autoridad independiente encargada de la protección de los datos personales. La Convención también establece normas específicas sobre una serie de cuestiones relacionadas con la recopilación y el tratamiento de datos personales, como el consentimiento del titular de los datos, la legitimidad de la finalidad y el proceso y la transparencia. También otorga al titular importantes derechos en relación con el proceso, como los derechos de información, acceso, oposición y supresión. Sin embargo, a diferencia de lo que sucede en otras normativas, como el RGPD de la Unión Europea, los miembros de la Unión Africana pueden decidir adherirse o no a la Convención. La Convención todavía no ha entrado en vigor, ya que se requiere que la hayan ratificado 15 Estados signatarios. A junio de 2020, solo 8 países (Angola, Ghana, Guinea, Mauricio, Mozambique, Namibia, Rwanda y Senegal) habían ratificado la Convención[29].

d) Foros regionales de América Latina

La Organización de Estados Americanos (OEA) ha sido una referencia constante para los países de la región en materia de gobernanza del ecosistema digital. Esta influencia se ha ejercido fundamentalmente a través de tres órganos internos de esta organización: la Comisión Interamericana de Derechos

[27] Véase Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data Consolidated text, disponible en https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[28] Informe anual sobre el derecho a la privacidad a la Asamblea General de 2018 (A/73/45712) e Informe anual al Consejo de Derechos Humanos de las Naciones Unidas, del 1 de marzo de 2019 (A/HRC/40/63).

[29] Véase "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection", disponible en https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf.

Humanos, el Comité Jurídico Interamericano y el Comité Interamericano contra el Terrorismo. La Comisión Interamericana de Derechos Humanos ha ejercido una poderosa influencia en cuestiones relacionadas con la defensa de la libertad de expresión en el entorno digital y, más recientemente, a través de sus directrices sobre la moderación de los contenidos digitales. El Comité Jurídico Interamericano lleva trabajando desde 1996 en la protección de los datos personales, lo que en el año 2000 dio lugar a un documento sobre el "Derecho de la información: acceso y protección de la información y datos personales en formato electrónico". En 2012 aprobó una "Propuesta de Declaración de Principios sobre Privacidad y Protección de Datos Personales en las Américas", que contiene 12 principios en relación con este tema. Y en 2015 publicó la "Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas"[30].

No obstante, la Red Iberoamericana de Datos Personales (RIDP) representa el foro más pertinente en lo que respecta a la protección de datos[31]. Su enfoque se basa en la perspectiva integral promovida por la Unión Europea, mientras que el enfoque promovido por el Comité Jurídico Interamericano se acerca más a la perspectiva sectorial predominante en los Estados Unidos. El principal objetivo de la RIDP es promover entre los países de la región la adopción de un marco normativo que reconozca la protección de datos como derecho fundamental desde una perspectiva integral, así como un diseño institucional dotado principalmente de autoridades que se encarguen de garantizar el cumplimiento efectivo de este marco y sean independientes de los poderes ejecutivos. La Red ha crecido en número de miembros, complejidad institucional y tendencia política.

Desde su tercera reunión de 2004, la RIDP ha promovido la adopción de un régimen de garantías para la transferencia internacional de datos personales conforme con las normas europeas. Esto implicaba lograr el reconocimiento de un grado de protección adecuado o, en su defecto, apelar a las cláusulas contractuales tipo aprobadas por la Comisión Europea. En 2007 se aprobaron las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana"[32] y se recomendó la adhesión al Convenio 108 del Consejo de Europa.

En 2013 se adoptó una normativa por la que se establecía una nueva estructura institucional. También se crearon grupos de trabajo y un Foro de la Sociedad Civil. Por último, se instó a la cooperación con la OEA para lograr un consenso sobre un proyecto de ley modelo de protección de datos. Esto llevó en 2015 a la aprobación de los Principios sobre la Privacidad y la Protección de Datos Personales de la OEA, que se actualizaron en abril de 2021. No obstante, la cooperación entre la RIDP y la OEA se resintió a raíz de la sentencia del Tribunal de Justicia de la Unión Europea de octubre de 2015 por la que se invalidó el acuerdo de puerto seguro. En 2019, los miembros de la RIDP propusieron que la organización se posicionara ante los nuevos desafíos que plantea la agenda digital, teniendo en cuenta sus posibles efectos en el ámbito de la privacidad. En este sentido, aprobaron un documento sobre Principios y Recomendaciones para el Tratamiento de Datos Personales en la Inteligencia Artificial[33]. En resumen, la RIDP ha conseguido posicionarse como un foro cada vez más influyente entre las partes interesadas de la región.

La Agenda Digital para América Latina y el Caribe (eLAC) es una estrategia que propone el uso de las tecnologías digitales como instrumentos de desarrollo sostenible. Esta es la agenda digital promovida

30 Los documentos de la OEA mencionados en esta sección pueden consultarse en el Departamento de Derecho Internacional, Protección de Datos Personales (disponible en http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp).

31 La RIDP (Red Interamericana de Datos Personales) se creó en 2003; en 2020 constaba de 33 entidades públicas especializadas en la protección de datos, la mayoría de ellas latinoamericanas. Entre sus miembros se encuentran las autoridades de la Argentina, Colombia, Costa Rica, Chile, México, el Perú y el Uruguay, así como las autoridades de España y Portugal. Entre sus observadores hay organismos del Ecuador, el Brasil, El Salvador, Guatemala, Honduras, el Paraguay y la República Dominicana, además de la propia OEA, el Supervisor Europeo de Protección de Datos y el Comité del Convenio 108 del Consejo de Europa.

32 Véase "Directrices para la Armonización de la Regulación de la Protección de Datos en la Comunidad Iberoamericana", disponible en https://www.redipd.org/sites/default/files/2020-01/directrices_armonizacion_iberoamerica_seminario_2007.pdf.

33 Véase "La RIPD aprueba sendos documentos sobre Inteligencia Artificial y Protección de Datos Personales", disponible en https://www.redipd.org/es/noticias/la-ripd-aprueba-sendos-documentos-sobre-inteligencia-artificial-y-proteccion-de-datos".

por la Comisión Económica para América Latina y el Caribe de las Naciones Unidas, en cooperación con el Banco de Desarrollo de América Latina. La Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, celebrada en noviembre de 2020, estableció la eLAC2022. Esta incluye ocho esferas de acción e identifica 39 objetivos específicos, y contiene además un capítulo dedicado a la lucha contra la pandemia y la recuperación económica. El objetivo 11 se centra en la promoción de normas abiertas y el fomento de un entorno regional interoperable mediante el intercambio de datos que permita garantizar la transformación digital. Más concretamente, el objetivo 27 alienta a la elaboración de una estrategia de mercado digital regional, iniciativa que se ha debatido en los últimos cinco años y que ahora vuelve a plantearse. Incluye disposiciones específicas sobre el comercio electrónico y digital transfronterizo mediante la integración de la infraestructura digital, la armonización normativa y el libre flujo de datos con confianza, entre otras cosas. El objetivo 31 también persigue promover una mayor coherencia y armonización normativa digital, especialmente en materia de protección de datos, flujo de datos transfronterizo, ciberseguridad, comercio electrónico y digital, y defensa de los derechos del consumidor en las plataformas en línea (ECLAC, 2020).

E. CONCLUSIONES

En este capítulo se ha examinado el sistema de gobernanza de los flujos de datos transfronterizos en diversos acuerdos y foros internacionales y regionales. En los últimos años, una de las tendencias más importantes ha sido el constante esfuerzo por trasladar la cuestión de la gobernanza de los datos al ámbito comercial mediante la inclusión de cuestiones como la libre circulación de los datos a través de las fronteras y la localización de los datos en diferentes negociaciones comerciales. Esta tendencia comenzó con la adopción de la "agenda de comercio digital" por los Estados Unidos, y con la iniciativa de este país de promover, junto con otros países desarrollados, la inclusión de estas cuestiones en los acuerdos comerciales en los planos multilateral, regional y bilateral. A nivel multilateral, varias economías avanzadas han promovido la ampliación de las negociaciones sobre el comercio digital y los flujos de datos transfronterizos en el marco de la OMC. Sin embargo, estas demandas han encontrado una fuerte oposición de algunos países en desarrollo y coaliciones de países en desarrollo, lo que ha hecho que los avances sean escasos. El resultado ha sido que las negociaciones se han trasladado al marco de la Iniciativa de Declaración Conjunta sobre el comercio electrónico.

Sin embargo, el hecho de que algunos países en desarrollo hayan logrado limitar las negociaciones multilaterales sobre esta cuestión no ha puesto freno a los esfuerzos por promover normas sobre los flujos de datos transfronterizos en el ámbito comercial. Los primeros compromisos vinculantes en relación con la libre circulación de los datos y la prohibición de su localización se adoptaron en el marco del TIPAT y el T-MEC. En general, la mayoría de estos acuerdos tienen como objetivo promover los flujos de datos transfronterizos y restringir el uso de políticas de localización de datos. Sin embargo, difieren en algunos aspectos importantes, sobre todo en el modo en que abordan cuestiones como la privacidad y la protección de los datos personales, y en las condiciones en que los países pueden desviarse del principio de la libre circulación de los datos. En estas cuestiones existen importantes diferencias entre los enfoques adoptados por algunas de las principales economías.

> Los enfoques internacionales y regionales de la regulación de los flujos de datos transfronterizos son o bien demasiado restringidos, al centrarse solo en aspectos como el comercio o la privacidad, o bien demasiado limitados geográficamente, como en el caso de los enfoques regionales.

La expansión progresiva de las cláusulas sobre los datos en los acuerdos comerciales bilaterales y regionales deja a los países en desarrollo "entre la espada y la pared" en lo que respecta a la gobernanza digital y de los datos en el sistema de comercio. Aunque algunos de ellos siguen resistiéndose a adoptar estas normas en el sistema multilateral, existe el riesgo de que la inclusión creciente de este tipo de

disposiciones en los acuerdos bilaterales y regionales debilite aún más la capacidad de negociación de estos países en la esfera comercial.

No obstante, en esencia existen serias dudas sobre la adecuación del sistema de comercio para regular la cuestión de los datos. Los flujos de datos pueden estar estrechamente relacionados con el comercio de bienes y servicios en una economía digital en evolución, pero los datos son muy diferentes de los bienes y servicios, y los flujos de datos transfronterizos constituyen un tipo de flujo económico diferente. Conciliar las cuestiones que surgen de esta distinción reviste una gran dificultad, como se manifiesta en los esfuerzos por casar las cuestiones relativas a la privacidad con la libre circulación de los datos. Las disposiciones de los acuerdos comerciales tienen consecuencias para las políticas nacionales —como las relacionadas con la privacidad, la seguridad nacional y el desarrollo industrial—, pero estas implicaciones no se tienen suficientemente en cuenta (Fay, 2020).

Además, la vinculación de los datos y el comercio se traduce en decisiones más difíciles para los países en desarrollo en particular. El sistema de comercio permite a las grandes potencias económicas aprovechar su tamaño de mercado para obtener concesiones en otras esferas. Esto podría llevar a los países en desarrollo a tener que "ceder su derecho (margen de actuación) a regular los flujos de datos" para proteger otros intereses comerciales. Esto es especialmente cierto si se tiene en cuenta la capacidad de las economías avanzadas para aprovechar su poder de mercado a nivel multilateral, pero también regional y bilateral. Además, los países en desarrollo sufren deficiencias estructurales en la esfera comercial, en particular en lo que respecta a la resolución de controversias y a la capacidad de negociación, lo que a menudo los sitúa en una posición relativamente vulnerable.

> El panorama mundial de la gobernanza de los flujos de datos transfronterizos es un mosaico de políticas nacionales, regionales e internacionales diferentes.

A pesar del creciente número de acuerdos comerciales que abordan los flujos de datos, entre los principales agentes de la economía digital sigue habiendo importantes desacuerdos. En el seno del G20 existen opiniones contrapuestas, no solo en relación con el fondo (por ejemplo, sobre las medidas de localización de los datos), sino también con la forma (como acerca de si la OMC es un lugar de negociación adecuado, dada la abundancia de regímenes paralelos en materia de privacidad de los datos, fiscalidad, aplicación de la ley y regulación de las plataformas) (De La Chapelle y Porciuncula, 2021).

El presente capítulo pone de manifiesto que los enfoques internacionales y regionales de la regulación de los flujos de datos transfronterizos son o bien demasiado restringidos, al centrarse solo en aspectos como el comercio o la privacidad, o bien demasiado limitados geográficamente, como en el caso de los enfoques regionales. En los países en desarrollo, la cooperación regional en materia de gobernanza de los datos ha experimentado avances significativos en Asia, ligeramente inferiores en América Latina y escasos en África. Los enfoques regionales pueden ser útiles como paso previo a la gobernanza mundial de los datos, que debería ser el objetivo final, dado que el tratamiento de los flujos de datos transfronterizos representa un desafío a nivel mundial. Además, es probable que los enfoques regionales que incluyen a miembros con niveles similares de desarrollo digital tengan más posibilidades de prosperar que los enfoques en los que se plantean importantes desequilibrios de poder. Por último, tal y como se ha comentado en los capítulos anteriores, la gobernanza mundial de los datos debería tener en cuenta el carácter multidimensional de dichos datos y, por lo tanto, abordarse desde una perspectiva global e integrada.

> Los flujos de datos transfronterizos siguen sin contar con un sistema de regulación internacional que pueda contribuir a la prosperidad general.

En conjunto, este capítulo y los capítulos IV y V muestran que el panorama mundial de la gobernanza de los flujos de datos transfronterizos es un mosaico de diferentes políticas nacionales, regionales e internacionales. Esto se resume en el cuadro del anexo en línea de este capítulo[34], que proporciona información sobre estas normativas en los Estados miembros de la UNCTAD[35].

Los flujos de datos transfronterizos siguen sin contar con un sistema de regulación internacional que pueda contribuir a la prosperidad general, lo cual tiene varias consecuencias. En primer lugar, aumenta el riesgo de una proliferación de diferentes enfoques reguladores nacionales que conduzca a la fragmentación de Internet y limite su contribución al desarrollo sostenible. En segundo lugar, aquellos que estén mejor posicionados para captar los beneficios potenciales de los datos y los flujos de datos podrán reforzar aún más sus posiciones ya dominantes. En tercer lugar, aumenta el riesgo de que se produzca una mayor polarización entre los países en lo que respecta a los flujos de datos.

La armonización mundial de la política de datos deberá tener en cuenta que los países en desarrollo necesitan margen de actuación para adoptar medidas encaminadas a fomentar su desarrollo tecnológico e industrial. Los problemas y dificultades para lograr un consenso multilateral sobre esta cuestión en el marco de la OMC apuntan a la necesidad de examinar otras opciones con mayores perspectivas de obtener un resultado que facilite los flujos de datos transfronterizos y aborde, al mismo tiempo, las múltiples implicaciones asociadas a estos flujos. Dichas opciones deben permitir una distribución equitativa de los beneficios resultantes de estos flujos y abordar adecuadamente los riesgos que conllevan. Estas cuestiones se examinan con más detalle en el capítulo VII, en el que se estudia el camino hacia un enfoque equilibrado de la gobernanza mundial de los datos y los flujos de datos.

[34] El anexo en línea del capítulo VI está disponible en https://unctad.org/system/files/official-document/der2021_annex3_en.xlsx.

[35] Este análisis puede complementarse con otros exámenes útiles de las normativas sobre los flujos de datos transfronterizos a diferentes niveles, como: OECD (2020) y Casalini y otros (2021); World Bank (2021); "Global Data Governance Mapping Project of the Digital Trade and Data Governance Hub" (disponible en https://datagovhub.elliott.gwu.edu/); *Foreign Policy*, 6 de octubre de 2020, "Global Data Governance Database of Policies" (disponible en https://foreignpolicy.com/2020/10/06/global-dataprivacy-collection-laws-database-surveillance-cybersecurity-governance/); CSIS, "Data Governance" (disponible en https://datagovernance.csis.org/); y Universidad de Lucerna, "TAPED A New Dataset on Data-related Trade Provisions" (disponible en https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/ research/taped/).

El mundo apenas está empezando a comprender las implicaciones de la economía digital impulsada por los datos. Desde el punto de vista regulador, los responsables políticos y otros actores todavía están poco preparados para afrontar los nuevos retos, muchos de los cuales son de alcance mundial. A pesar de las muchas formas en que los datos pueden contribuir al desarrollo sostenible, hace falta adoptar un enfoque global de la gobernanza de los datos y de los flujos de datos transfronterizos para que estos generen beneficios para la mayoría, y no solo para unos pocos, y para abordar sus posibles efectos negativos.

En este capítulo se analizan posibles vías que podrían estudiarse con el objetivo de encontrar un enfoque internacional más holístico para regular los datos y sus flujos transfronterizos, de manera que se beneficie a las personas y al planeta. Se señala la posible necesidad de contar con un marco institucional global que incluya una combinación adecuada de participación multilateral, multipartita y multidisciplinar, posiblemente dirigida por un nuevo organismo de coordinación internacional. El enfoque debería reflejar las divisiones y desequilibrios existentes, garantizar la plena participación de todos los países, ser suficientemente flexible para contribuir al desarrollo de países con diferentes niveles de preparación digital, y destinar recursos significativos a ayudar a los países que se están quedando atrás a fortalecer su capacidad de aprovechar los datos.

EL CAMINO HACIA UN ENFOQUE EQUILIBRADO

VII

CAPÍTULO VII HACIA UNA GOBERNANZA GLOBAL DE LOS DATOS EQUILIBRADA QUE ESTÉ AL SERVICIO DE LAS PERSONAS Y EL PLANETA

¿Por qué es necesaria la gobernanza global de los datos?

Para evitar una mayor fragmentación en el espacio digital

Para aumentar la confianza en la economía digital y reducir la incertidumbre

Para permitir el intercambio de datos a nivel mundial y desarrollar bienes públicos digitales globales

Para abordar los retos políticos que crean las posiciones dominantes de las plataformas digitales globales

Para evitar que las desigualdades se amplíen

Para tener en cuenta los efectos indirectos de las políticas nacionales en otros países

Con el fin de permitir que los datos circulen a través de las fronteras tan libremente como sea necesario y posible, sin dejar de atender los diversos objetivos de desarrollo

Cómo

Áreas políticas clave relacionadas con los datos

- Acordar definiciones y taxonomías
- Establecer las condiciones de acceso a los datos
- Reforzar la medición
- Tratar los datos como un bien público global
- Explorar las nuevas formas de gobernanza de los datos
- Acordar derechos y principios
- Desarrollar normas
- Aumentar la cooperación internacional en materia de gobernanza de las plataformas

Un nuevo marco institucional global

Multilateral
Multipartito
Multidisciplinar

Un nuevo órgano de coordinación de las Naciones Unidas

Lo que hay que hacer

- **Poner fin a la infrarrepresentación** de los países en desarrollo en las actuales iniciativas mundiales y regionales, garantizando que se reflejen adecuadamente los conocimientos, las necesidades y las opiniones locales
- Funcionar como **complemento de las políticas nacionales y en coherencia con estas** para hacer que la economía digital impulsada por los datos contribuya al desarrollo inclusivo
- **Proporcionar un margen de actuación suficiente** para que países con diferentes niveles de preparación y capacidades puedan beneficiarse de la economía digital impulsada por los datos

A fin de mejorar la capacidad de los países en desarrollo de crear y obtener valor de los datos a nivel nacional, el apoyo internacional puede servir para:

Concienciar sobre los datos y sus implicaciones para el desarrollo

Crear estrategias nacionales de datos

Formular los marcos jurídicos y normativos pertinentes

Garantizar su participación efectiva en los procesos internacionales

A. REPLANTEAMIENTO DE LA REGULACIÓN DE LOS FLUJOS DE DATOS TRANSFRONTERIZOS

La rápida expansión de la digitalización afecta todos los aspectos de la vida, incluida la forma en que las personas se relacionan, trabajan, compran y reciben servicios, así como las formas de crear e intercambiar valor. Ese proceso ha puesto de manifiesto la creciente importancia de los datos y de sus flujos, incluidos los transfronterizos, en la economía mundial. Los datos se han convertido en un recurso económico clave a partir del cual se puede crear y obtener valor, y pueden influir en las perspectivas de desarrollo de diversas maneras. Por ello, los datos pueden contribuir de manera decisiva a la labor para alcanzar los Objetivos de Desarrollo Sostenible.

Aunque la economía digital impulsada por los datos aporta importantes beneficios, también plantea grandes retos. Por lo tanto, corresponde a los responsables políticos adaptarla de manera que contribuya al desarrollo (UNCTAD, 2019a). Pero los responsables políticos tienen grandes dificultades para seguir el ritmo de los avances tecnológicos en un contexto incierto, en rápida evolución y plagado de numerosas incógnitas. Para complicar aún más este panorama, la pandemia de COVID-19 ha provocado una significativa aceleración de las tendencias de digitalización, ya que se ha incrementado el número de personas que dependen de Internet para continuar con sus actividades y hacer frente a los efectos de la pandemia. En consecuencia, resulta aún más urgente regular y gobernar adecuadamente la economía digital impulsada por los datos para que esté al servicio de las personas y el planeta.

Aunque la economía digital impulsada por los datos aporta importantes beneficios, también plantea grandes retos. Corresponde a los responsables políticos adaptarla de manera que contribuya al desarrollo.

La pandemia ha puesto de manifiesto los desfases de desarrollo derivados de las enormes brechas digitales que aún existen dentro de los países y entre ellos. Y, a medida que aumenta la importancia de los datos, una brecha relacionada con los datos se suma a la brecha digital convencional, relacionada con la conectividad. Los países con capacidades limitadas para convertir los datos en inteligencia digital y oportunidades comerciales, y para ponerlos al servicio del desarrollo, están en clara desventaja. Reducir estas brechas resulta esencial para lograr los objetivos de desarrollo. A nivel internacional, las crecientes interconexiones derivadas del progreso de las tecnologías digitales han dado lugar a una nueva forma de interdependencia económica internacional, a través de los flujos de datos transfronterizos. Pero esta interdependencia es asimétrica, lo cual podría aumentar las desigualdades existentes a menos que se trate de corregir adecuadamente las asimetrías. No hay duda de que la pandemia ha acentuado los desequilibrios de poder de mercado relacionados con los datos, ya que las corporaciones digitales globales se han beneficiado enormemente de las necesidades urgentes de digitalización, mientras que el resto del mundo lucha por recuperarse de la crisis económica resultante.

Los capítulos anteriores han ilustrado la complejidad de las numerosas cuestiones que están en juego, así como las concesiones que los diferentes actores de los flujos de datos transfronterizos se ven obligados a realizar en relación con sus perspectivas de desarrollo. Los datos tienen características particulares que los diferencian de los bienes y servicios. Son intangibles y no rivales, pero parcialmente excluibles; y su valor es enormemente contextual, surge cuando se utilizan y aumenta mediante la agregación y la combinación. En ese sentido, los datos pueden generar no solo beneficios privados, sino también valor social. Dado que las fuerzas del mercado no pueden garantizar por sí solas la necesaria creación de valor social, se deben adoptar políticas públicas. El posible valor social de los datos implica que el hecho de compartirlos supone un beneficio para la sociedad. Esto, a su vez, haría deseable que los datos circularan libremente a través de las fronteras (cuando son de carácter público).

Sin embargo, no todos los datos pueden ser compartidos. Cuando los datos se mantienen privados, son quienes los extraen o recopilan los que tienen la capacidad de procesarlos y pueden apropiarse de la mayor

parte de su valor. Hablamos principalmente de las corporaciones digitales globales de los Estados Unidos y China. En cambio, quienes podemos considerar los productores de los datos brutos —los usuarios de las plataformas—, que también contribuyen a ese valor, no participan de esos beneficios. Dado que la mayoría de los países en desarrollo son proveedores de datos brutos, no suelen obtener los beneficios de los datos generados a nivel nacional. Por lo tanto, desde este punto de vista, es necesario regular las plataformas y los flujos de datos transfronterizos para que los beneficios se distribuyan equitativamente, dentro de los países y entre ellos.

Para regular los flujos de datos transfronterizos hay otros factores no económicos que se deben tener en cuenta. Los datos son multidimensionales, ya que también guardan relación con la privacidad, otros derechos humanos y la seguridad nacional. Esto entraña la necesidad de regular los flujos para evitar los abusos y el uso indebido de los datos por los Estados o el sector privado. En ese sentido, no es de extrañar que la regulación internacional de los flujos de datos transfronterizos se haya convertido en uno de los principales retos mundiales en el contexto de la economía digital.

Las normativas varían de un país a otro, y hay pocos avances a nivel regional e internacional. A escala mundial, la gobernanza de la economía digital impulsada por los datos, incluidos los flujos de datos transfronterizos, se enfoca principalmente desde tres puntos de vista que se están convirtiendo en importantes áreas de influencia: a) los Estados Unidos, donde el control de los datos es ejercido primordialmente por el sector privado; b) China, donde el control de los datos corresponde al Estado; y c) la Unión Europea, donde se favorece el control de los datos por el propio individuo sobre la base de los derechos y valores fundamentales. El contexto actual se caracteriza por las tensiones existentes entre estas áreas, especialmente entre los Estados Unidos y China. Asistimos a una carrera por colocarse a la vanguardia de las tecnologías digitales, ya que se piensa que controlando los datos y las tecnologías conexas, en particular la inteligencia artificial, se logrará el poder económico y estratégico.

En este contexto, existe un riesgo de fragmentación en el espacio digital, también llamado a menudo "splinternet". Además, las plataformas globales, que en algunos casos son tan grandes y tienen tanto poder e influencia como los Estados-nación, presionan para crear sus propios ecosistemas de datos. Estas plataformas tienden a autorregularse, lo que también puede tener una influencia significativa a nivel mundial. En general, existe el riesgo de que la economía digital impulsada por los datos se compartimentalice, lo cual va en contra del espíritu original de Internet, que pretendía ser una red libre, descentralizada y abierta. Tampoco sería una situación óptima en términos económicos, ya que la interoperabilidad ofrece mayores beneficios a nivel internacional.

> La regulación internacional de los flujos de datos transfronterizos se ha convertido en uno de los principales retos mundiales en el contexto de la economía digital.

Los países pueden tener una variedad de legítimas razones políticas para regular los flujos de datos transfronterizos, como la protección de la privacidad y otros derechos humanos, la seguridad nacional y los objetivos de desarrollo económico. Mientras no exista un sistema internacional adecuado para regular esos flujos, los países no tienen más remedio que restringir la circulación de los datos como consideren necesario. También deben adoptar diferentes estrategias nacionales para desarrollar la economía de los datos. Sin embargo, no es probable que la localización de los datos se traduzca en una adición de valor nacional a los datos, porque el vínculo entre el lugar donde se almacenan los datos y la creación de valor no está tan claro, y hay que tener en cuenta la relación costo-beneficio. No existe una política única para regular los flujos de datos transfronterizos. Las políticas varían en función de las condiciones tecnológicas, económicas, sociales, políticas, institucionales y culturales de los distintos países.

Dada la gran divergencia de opiniones y posiciones sobre la regulación de los flujos de datos transfronterizos, el debate internacional se encuentra en un punto muerto. Sin embargo, como los datos

y los flujos de datos transfronterizos están adquiriendo mayor protagonismo en la economía mundial, urge regularlos adecuadamente a nivel internacional. Para ello es necesario considerar los datos en todas sus dimensiones, tanto económicas como no económicas. Sin embargo, esto no debe entrañar que los factores no económicos se utilicen como excusa para cumplir los objetivos económicos. Además, si bien los datos están fuertemente vinculados al comercio y pueden proporcionar enormes ventajas competitivas a quienes sean capaces de beneficiarse de ellos, los flujos de datos esencialmente transfronterizos no son ni comercio electrónico ni comercio, y no deberían regularse como tales.

El hincapié que se hace en la privacidad varía de un país a otro. Sin embargo, teniendo en cuenta que la privacidad es un derecho humano y que el respeto de los derechos humanos es un deber fundamental, el fin de las políticas relacionadas con los datos debería ser tanto respetar los derechos humanos como promover los objetivos de desarrollo económico. Así pues, al estudiar la forma de regular los flujos de datos transfronterizos, la comunidad internacional tendrá que ir más allá del comercio y considerarlos de forma holística; el debate político internacional sobre los datos debería tener en cuenta las diferentes cuestiones en juego, como los derechos humanos, la seguridad, la competencia, la fiscalidad internacional y la gobernanza general de Internet. En ese sentido, cabe preguntarse cuál es el foro internacional apropiado para deliberar sobre las políticas relacionadas con los datos favorables al desarrollo.

> En lugar de las posiciones extremas sobre los flujos de datos transfronterizos, que no son óptimas y no pueden sostenerse, debería favorecerse un enfoque de cooperación mundial para encontrar criterios comunes de avance global en la economía digital impulsada por los datos y para fomentar el desarrollo inclusivo y sostenible.

Las posiciones extremas sobre los flujos de datos transfronterizos no son óptimas y no pueden sostenerse. Por lo tanto, es necesario replantear la regulación de los flujos de datos transfronterizos a nivel internacional para encontrar la base de un término medio y soluciones intermedias. Este capítulo pretende aportar una contribución en esa dirección. No es probable que un enfoque de confrontación aporte resultados positivos para la humanidad. Debería favorecerse un enfoque de cooperación mundial para encontrar criterios comunes de avance global en la economía digital impulsada por los datos y para fomentar el desarrollo inclusivo y sostenible. En lugar de centrarse en las diferencias, habría que esforzarse por encontrar principios y objetivos comunes. Debería encontrarse un equilibrio entre los intereses de soberanía nacional y la necesidad de que la red sea abierta, y entre la diversidad que favorece la innovación y la necesidad de armonización, para permitir que los datos circulen a través de las fronteras. Además, distribuyéndose de manera equilibrada los beneficios de los flujos de datos transfronterizos se podrían reducir las asimetrías y desigualdades en la economía digital impulsada por los datos.

Para que un sistema internacional de regulación de los flujos de datos transfronterizos esté al servicio de las personas y el planeta, debe garantizar que los datos puedan circular tan libremente como sea posible y necesario y asegurar al mismo tiempo una distribución más equitativa de los beneficios dentro de los países y entre ellos, sin desatender los riesgos relacionados con los derechos humanos y la seguridad nacional. Un sistema así contribuiría a garantizar el buen funcionamiento de Internet y aumentaría la confianza en la economía digital impulsada por los datos.

Se debe prestar especial atención a la situación de los países en desarrollo, que actualmente se encuentran entre la espada y la pared en lo que respecta a la gobernanza de los flujos de datos transfronterizos. Las autoridades de los países más pequeños o menos adelantados son objeto de una presión considerable para que elijan entre las áreas dominantes de gobernanza de los datos. Para encontrar respuestas adecuadas al reto de regular los flujos de datos transfronterizos hace falta más colaboración internacional

y diálogo político, con la plena participación de los países en desarrollo. Todo consenso deberá incorporar importantes flexibilidades y tener en cuenta las condiciones particulares de los distintos países para que todos ellos puedan participar de forma beneficiosa.

> Al concebir la normativa correspondiente, debe tenerse en cuenta que los riesgos relacionados con los datos pueden surgir del uso de estos que hagan tanto el sector privado como los Estados.

Además, al concebir la normativa correspondiente, debe tenerse también en cuenta que los riesgos relacionados con los datos pueden surgir del uso de estos que hagan tanto el sector privado como los Estados. Los datos pueden utilizarse para controlar o manipular preferencias, elecciones y decisiones. Con ellos se puede acabar llegando a resultados preconcebidos para dirigir a la sociedad en una dirección particular, restringiéndose las libertades humanas. Esto puede ocurrir en los ámbitos económico o político, e incluso amenazar la democracia. Por ello es necesario lograr un nuevo equilibrio entre los intereses de la ciudadanía y los de los Estados para que se respeten los derechos individuales. Para lograrlo podría hacer falta un sistema adecuado de equilibrio de poderes con el que pedir cuentas a quienes controlan los datos.

Con este telón de fondo, en este capítulo se analizan posibles vías que podrían estudiarse con el objetivo de encontrar un enfoque internacional más holístico para regular los datos y sus flujos transfronterizos. En la sección B se destaca la necesidad absoluta de establecer un sistema global de gobernanza de los datos. Las posibles opciones políticas para la gobernanza de los datos se presentan en la sección C. En la sección D se exploran las cuestiones relacionadas con el marco institucional que podría precisarse; se señala la posible necesidad de un nuevo órgano de coordinación internacional que se concentre en los asuntos relacionados con los datos, y se indican algunas formas en que podría funcionar dicho marco institucional. Para que un enfoque internacional funcione a nivel nacional, es necesario disponer de margen de actuación para crearlo, como se expone en la sección E. En la sección F se analiza la cuestión del fomento de la capacidad para la digitalización y la elaboración de políticas impulsadas por los datos. Por último, en la sección G se presentan las conclusiones.

B. LA NECESIDAD DE UNA GOBERNANZA GLOBAL DE LOS DATOS

Por gobernanza de los datos se entiende la forma en que los datos son gestionados y regulados para cumplir diferentes objetivos. Puede tener lugar en diferentes niveles interrelacionados, a saber:

- Los *particulares* deben manejar sus datos con responsabilidad. Es importante ser consciente de los riesgos de la digitalización. Esta conciencia puede mejorarse mediante la educación y el aprendizaje. Además, toda persona puede adoptar un papel activo y reivindicar sus derechos. Un ejemplo de ello es Max Schrems, que ha luchado por defender los derechos de privacidad en la Unión Europea.
- Las *comunidades* también pueden desempeñar un importante papel en cuanto a la gobernanza colectiva de los datos de sus miembros. En las organizaciones de la sociedad civil, las personas y las comunidades pueden reclamar que se hagan avances en la gobernanza de los datos mediante el activismo social[1].
- El *sector privado* debe gobernar los datos de forma que no solo se defiendan los beneficios privados, sino también el interés público. Una buena gobernanza de los datos también ayuda a las empresas a aumentar su competitividad, al mejorar la confianza. Sin embargo, la autorregulación

[1] Véase UNCTAD, "Social activism needed to rein in tech's destructive elements", 13 de abril de 2021, disponible en https://unctad.org/news/social-activism-needed-rein-techs-destructive-elements.

en el sector privado tiene límites, y ante la creciente evidencia de la influencia de este sector y de los desequilibrios de poder en la economía digital impulsada por los datos, se hace más necesario reforzar la regulación pública, tanto a nivel nacional como internacional.

- Los *gobiernos nacionales y subnacionales*, incluidas las ciudades, en estrecho diálogo con otros actores, son responsables de establecer normativas que garanticen que los datos benefician a todos y de contrarrestar sus impactos negativos.
- A *nivel internacional* (o a nivel regional para empezar), la gobernanza global o la cooperación internacional deben tener como objetivo llegar a acuerdos sobre la forma de facilitar el intercambio global de datos de valor social, al servicio de las personas y el planeta, así como permitir los flujos de datos transfronterizos, siempre que los beneficios se distribuyan equitativamente y los riesgos se aborden adecuadamente.

Los diferentes niveles de la gobernanza de los datos están interrelacionados. De hecho, debe entenderse que la gobernanza global de los datos está compuesta por todos estos subniveles interrelacionados. Por lo tanto, debe ser una gobernanza de varios niveles en cuanto a los actores implicados. La relación entre estos niveles de gobernanza es tanto descendente como ascendente. El interés principal de este Informe es el nivel internacional, aunque sin perder de vista los demás niveles. Los responsables políticos, en estrecha consulta con otros actores, deben evaluar cuáles son los aspectos reguladores relacionados con los datos que pueden ser nacionales (sin perder de vista la perspectiva global) y cuáles requieren un enfoque coordinado a nivel mundial, dado el alcance global de la economía digital. Para que los datos estén al servicio de las personas y el planeta, todos los niveles de la gobernanza de los datos deben fundamentarse en los valores universales globales vinculados al respeto de los derechos humanos y la dignidad humana, como la igualdad, la equidad, el desarrollo, la diversidad, la libertad, la transparencia y la rendición de cuentas.

La justificación de un marco global de gobernanza de datos, que complemente los demás subniveles, radica en diferentes factores, por ejemplo[2]:

- Los datos pueden aportar un valor social —no solo a nivel nacional, sino también internacional— y contribuir al desarrollo en todo el mundo. El intercambio de datos a nivel mundial puede ayudar a superar los principales desafíos del desarrollo en todo el planeta, como la pobreza, la salud, el hambre y el cambio climático. La pandemia de COVID-19 ha puesto de manifiesto la necesidad y las ventajas de compartir datos e información a nivel mundial; sin la cooperación mundial en materia de datos e información, la investigación para desarrollar una vacuna y las medidas para hacer frente al impacto de la pandemia habrían sido una tarea mucho más difícil. Del mismo modo que algunos datos pueden ser bienes públicos, hay motivos para que algunos datos sean considerados bienes públicos mundiales, que se aborden y proporcionen a través de la gobernanza global.
- El aumento de los flujos de datos transfronterizos y la inminente implantación de la tecnología 5G, la Internet de las cosas y la IA, así como la aceleración de la digitalización a raíz de la pandemia de COVID-19, crean las condiciones para una ingente recopilación y monetización de los datos a nivel mundial. Sin embargo, sin un marco de gobernanza global coherente que genere confianza, esa situación podría conducir a un retroceso en el intercambio de datos y amplificar las preocupaciones ya existentes por la falta de transparencia en la cadena de valor de los datos, en particular respecto de la privacidad de los datos personales, el uso ético de las tecnologías de IA y la monetización de los datos por las plataformas de medios sociales.
- Es necesaria una coordinación técnica transfronteriza para que no se acabe fragmentando la infraestructura de Internet y el espacio digital. Esto está relacionado con las cuestiones de interoperabilidad de las redes y de portabilidad de los datos, con el fin de facilitar los flujos de datos.
- La proliferación de normativas nacionales sobre los flujos de datos transfronterizos genera confusión en cuanto a las reglas que deben seguirse, así como una falta de consistencia, coherencia y aplicación. Con ello se suscita incertidumbre y se elevan los costos de cumplimiento, lo que puede ser especialmente pernicioso para las microempresas y las pequeñas empresas, y por lo tanto para los países en desarrollo en particular.

[2] Basado parcialmente en Fay (2021).

- Dada la naturaleza interconectada de la economía digital impulsada por los datos, así como el alto grado de interdependencia global, las políticas nacionales relacionadas con los datos tienen efectos indirectos en otros países.
- La extraterritorialidad de algunas medidas puede no ser adecuada para otras jurisdicciones, que tal vez no sean capaces de influir en ellas, lo que se traduciría en una falta de rendición de cuentas democrática en esas jurisdicciones.
- La autorregulación ha dado lugar a estructuras de mercado que las plataformas han definido para beneficiarse. Esta situación, combinada con unas reglas diseñadas para la era industrial, tiene profundas repercusiones en áreas como la política de competencia y la innovación, la distribución del valor de las tecnologías entre los países y dentro de ellos, y la cohesión social, tanto a nivel nacional como internacional.
- Los enormes desequilibrios en el poder de mercado, generados por el hecho de que las corporaciones digitales globales refuerzan su dominio gracias a su acceso privilegiado a los datos, conducen a una mayor desigualdad mundial. Estas plataformas tienen un alcance y una influencia globales. Cada vez es más difícil que los países —incluso los desarrollados— puedan hacer frente por sí solos a los retos que generan estos desequilibrios.
- Las desigualdades históricas sistémicas en contra de los países en desarrollo se están trasladando e incluso amplificando en el espacio digital impulsado por los datos. Sus conocimientos y puntos de vista locales están infrarrepresentados en los debates internacionales, mientras que sus datos son explotados al no ejercerse una regulación adecuada y sus economías de gran intensidad de mano de obra son probablemente las más afectadas por la creciente implantación de las tecnologías digitales impulsadas por los datos.
- No se ha hecho una evaluación exhaustiva y coherente de los riesgos, vulnerabilidades y resultados de los modelos de negocio de las plataformas digitales, en particular de las plataformas de medios sociales, en un contexto de aumento de los daños causados en línea a nivel mundial. El uso indebido de los datos privados puede provocar —y ha provocado— daños sociales generalizados, para los que actualmente existe poca gobernanza. Esto se debe, en parte, a la falta de acceso a los datos que recopilan las plataformas, que podrían utilizarse para evaluar dichos riesgos. También se debe a la falta de acceso a los algoritmos utilizados para amplificar la información.
- Dadas las interdependencias y el carácter interconectado de la arquitectura global de Internet, el debate sobre el futuro de los flujos de datos transfronterizos no puede limitarse a unos pocos países.

Por lo tanto, la gobernanza global de los datos, así como de la economía y las tecnologías digitales, es claramente necesaria debido a su alcance mundial y a sus implicaciones para el desarrollo en todo el planeta. La digitalización impulsada por los datos crea oportunidades globales, pero también desafíos globales que requieren soluciones globales para aprovechar los impactos positivos y mitigar los negativos. Contar con una gobernanza global eficaz de los datos es un requisito fundamental para que estos favorezcan la consecución de los objetivos económicos, sociales y ambientales de la Agenda 2030 para el Desarrollo Sostenible centrando la atención en las personas.

También existe una creciente demanda de cooperación global en materia de datos entre las diferentes partes interesadas de todo el mundo[3]. Los Estados Miembros de las Naciones Unidas han reconocido firmemente la necesidad de mejorar el manejo de los datos y las tecnologías digitales. En la declaración de los Jefes y Jefas de Estado y de Gobierno que representaban a los pueblos del mundo en la conmemoración del 75º aniversario de las Naciones Unidas se destacó la cooperación digital como un área fundamental[4]: “Mejoraremos la cooperación digital. Las tecnologías digitales han transformado

[3] Por ejemplo, el Comité de Coordinación de las Actividades Estadísticas ha hecho un llamado a la acción sobre la necesidad de un nuevo consenso mundial sobre los datos (World Bank, 2021:297). Véase también MacFeely (2020b); Pisa y otros (2020); Hill (2020); Ichilevici de Oliveira y otros (2020); Sacks y Sherman (2019); y Carter y Yayboke (2019).

[4] Declaration on the Commemoration of the Seventy-Fifth Anniversary of the United Nations, disponible en www.un.org/pga/74/wp-content/uploads/sites/99/2020/06/200625-UN75-highlight.pdf.

profundamente la sociedad y generan oportunidades sin precedentes y nuevos desafíos. Cuando se utilizan de manera impropia o maliciosa, pueden fomentar las divisiones dentro de los países y entre ellos, aumentar la inseguridad, socavar los derechos humanos y exacerbar la desigualdad. Forjar una concepción común de la cooperación digital y un futuro digital que muestre todas las posibilidades que ofrece el uso beneficioso de la tecnología, y abordar las cuestiones de confianza y seguridad digitales, debe seguir siendo una prioridad, pues nuestro mundo depende hoy más que nunca de las herramientas digitales para mantener la conectividad y la prosperidad socioeconómica. Las tecnologías digitales tienen el potencial de acelerar la realización de la Agenda 2030 y debemos garantizar un acceso digital seguro y asequible para todos. Las Naciones Unidas pueden brindar una plataforma para que todos los interesados participen en esas deliberaciones".

C. ESFERAS Y PRIORIDADES CLAVE

Una vez analizada la interdependencia en la economía digital impulsada por los datos y las cuestiones intersectoriales que están en juego, parece claro que —dadas las complejas interconexiones de las disciplinas, los actores, las políticas y los países implicados (que se influyen mutuamente)— es necesario adoptar un enfoque sistémico de la formulación de políticas. Ese enfoque debe ser interdisciplinario e incluir aspectos relacionados con la tecnología, la ética, la economía y el desarrollo, la política, la geografía (geopolítica), el derecho, etc. También debe ser multipartito e incluir a todos los actores implicados. A nivel de los Gobiernos nacionales, debe abarcar todas sus dependencias, ya que las políticas adoptadas por un ministerio pueden afectar a los objetivos de las políticas de otro. En general, la gobernanza mundial de los datos requerirá una combinación de políticas nacionales, regionales e internacionales, con la plena participación de los países en desarrollo.

En las siguientes subsecciones se analizan una serie de esferas y prioridades clave que deben considerarse de forma holística y adoptando un enfoque multidimensional, multipartito y pangubernamental. Se trata de: elaborar definiciones básicas y clasificaciones de datos; intensificar los esfuerzos para medir el valor de los datos y de sus flujos transfronterizos; establecer las condiciones de acceso a los datos; desarrollar los datos como bienes públicos mundiales; explorar nuevas formas de gobernanza de los datos; definir los derechos, los principios y las normas de los datos; y coordinarse con las iniciativas de cooperación internacional en otros ámbitos de política económica relacionados con los datos.

1. Convenir en definiciones comunes de los conceptos relacionados con los datos

Para que los debates políticos internacionales alcancen resultados productivos, es importante que los asuntos discutidos estén bien definidos y que las definiciones sean consensuadas entre los participantes. La existencia de diferentes definiciones o interpretaciones complica sobremanera la posibilidad de encontrar un terreno de entendimiento. Sin embargo, tal y como se ha comentado en el capítulo II, hay conceptos básicos relacionados con los datos y los flujos de datos que aún no se han definido. El conocimiento y la comprensión de las características de los datos, su recopilación, tratamiento y uso "necesitan ser socializados para fomentar la transparencia en las conversaciones que la sociedad mantiene sobre este asunto, así como en las decisiones que toma" (De La Chapelle y Porciuncula, 2021:51).

Desde la perspectiva del desarrollo económico, es fundamental distinguir entre datos (en el sentido de datos brutos) y productos de datos (en el sentido de inteligencia digital, resultante del tratamiento de los datos). El valor añadido tiene lugar en la cadena de valor de los datos, que comienza con su recopilación y pasa por las diferentes fases de organización, análisis y tratamiento para convertirlos en inteligencia digital. Dado que las cadenas de valor de los datos se expanden por todo el mundo, las diferentes etapas de la cadena de valor de los datos pueden tener lugar en distintos países. Por lo tanto, es importante saber dónde se produce la adición de valor.

También hay que aclarar el significado de la soberanía nacional en el contexto de la economía digital impulsada por los datos. En el espacio descentralizado, libre y abierto que pretendía ser Internet, es difícil aplicar la asociación tradicional de soberanía nacional a los territorios de los países. No está claro dónde está la frontera

cuando hablamos de flujos de datos transfronterizos. Los diferentes puntos de vista e interpretaciones sobre lo que significa la soberanía sobre los datos o soberanía digital pueden provocar confusión sobre los derechos relativos a los datos y plantear conflictos con respecto a quién puede reivindicarlos. De hecho, también es necesario definir qué son los derechos digitales y los derechos relacionados con los datos. Asimismo, no hay duda de que se debe llegar a algún tipo de interpretación común sobre lo que significa la gobernanza de los datos y lo que implica en los diferentes niveles y para los distintos actores.

Los problemas con las definiciones son habituales en un contexto tan complejo y evolutivo, a causa de la rapidez con que avanzan las tecnologías digitales. El mundo se está adentrando en el desconocido territorio de la economía digital impulsada por los datos, y muchos conceptos de la economía convencional pueden transponerse directamente con solo añadirles el adjetivo "digital", pero esto no siempre es así. La digitalización añade nuevos parámetros que cambian significativamente la dinámica económica, y es necesario comprenderlos cabalmente. Por ello es necesario redoblar los esfuerzos para encontrar definiciones comunes que faciliten la labor de los poderes públicos en un contexto difícil.

Las distintas taxonomías utilizadas para clasificar el tipo de datos se basan en criterios diferentes. Sin embargo, aún no se ha explorado suficientemente la interfaz existente entre las distintas taxonomías y los flujos de datos transfronterizos. Aunque establecer clasificaciones de datos no es una tarea fácil, sería aconsejable dedicarse a acordar una taxonomía común de los tipos de datos que sea la más pertinente para la regulación de los flujos de datos transfronterizos. Ello permitiría establecer las condiciones de acceso a los datos, como se explica en la siguiente subsección, y también determinaría qué datos deben considerarse bienes públicos.

2. Establecer las condiciones de acceso a los datos

Una vez que se haya acordado una taxonomía relevante de los tipos de datos, convenir en las condiciones de acceso a cada tipo de datos podría despejar el camino hacia la facilitación de los flujos de datos transfronterizos. Cada tipo de datos circularía según esas condiciones establecidas. Estas podrían determinar qué datos deben permanecer dentro de las fronteras nacionales y cuáles pueden traspasarlas. También determinarían quién tiene acceso a los datos, en qué condiciones y para qué uso. Así, diferentes organizaciones o individuos tendrían diferentes derechos de acceso a los distintos tipos de datos. Ello requeriría un marco institucional fiable para gestionar, supervisar y hacer cumplir las condiciones de acceso (Coyle y otros, 2020). Estas condiciones incluirían:

- Quién puede recopilar los diferentes tipos de datos, cómo pueden recopilarse y con qué fines.
- Quién puede acceder a los datos (derechos de acceso) y en qué condiciones (si se pueden compartir los datos, ya sea a nivel nacional o internacional).
- Quién es responsable, y cómo, en caso de que no se cumplan las condiciones de recopilación, compartición, uso o control de los datos.

3. Intensificar los esfuerzos para medir el valor de los datos y de sus flujos transfronterizos

Para formular políticas con conocimiento de causa se debe partir de datos. Como muestra este Informe, encontrar datos sobre los datos es una tarea muy complicada. Las estadísticas existentes sobre el tráfico de datos son difíciles de interpretar. En lo que respecta al valor de los datos y de sus flujos transfronterizos, existen importantes lagunas que impiden comprender bien lo que realmente ocurre. Cuando se habla de los flujos de datos transfronterizos se suele hacer referencia a las estadísticas sobre el ancho de banda internacional. Sin embargo, estas no son un buen indicador, ni siquiera como aproximación. Solo reflejan el volumen de los datos que circulan, sin saber en que dirección y sin distinguir entre datos y productos de datos. Por tanto, no hay posibilidad de descubrir cuál es el flujo del valor relacionado con los datos a través de las fronteras. De hecho, lo importante no es el flujo de datos, sino el flujo del valor asociado a los datos. Sin esa información no es posible evaluar los efectos de las diferentes normativas en los flujos de datos transfronterizos, ni su relación con el desarrollo.

Además, la mayor parte de los datos sobre datos son manejados por el sector privado[5], que mantiene la información en propiedad. Dado que los datos se han convertido cada vez más en un recurso económico clave para la creación y obtención de valor, determinando el curso de las relaciones económicas internacionales mediante los flujos de datos transfronterizos, resulta cada vez más urgente reforzar la labor estadística para producir más indicadores oficiales en este ámbito que se pongan a disposición de las sociedades. También es necesario estudiar la forma de exigir a las principales plataformas digitales que divulguen más información sobre sus datos que pueda ser valiosa para los poderes públicos. De lo contrario, estos carecen de la brújula de información necesaria para sus decisiones.

4. Los datos como bienes públicos (globales)

Como se ha comentado en el capítulo III, los bienes públicos digitales, incluidos los datos cuando tienen carácter de bien público, son esenciales para aprovechar todo el potencial de las tecnologías digitales. Las posibilidades de crear y obtener valor a partir de los datos se amplían cuando las organizaciones disponen de un conjunto de datos amplio y diverso. La disponibilidad de estos datos a nivel mundial ha sido a menudo limitada, debido al control firme de los datos o a que estos datos incluyen detalles personales que no pueden ser divulgados. Sin embargo, cuando se ponen a disposición del público grandes conjuntos de datos, se puede generar un significativo valor social y un gran impacto en el desarrollo. Dos ejemplos recientes de ello son el valor de los datos durante las crisis sanitarias del ébola y la COVID-19 (Moorthy y otros, 2020; Wesolowski y otros, 2014), y los casos de ciudades que han podido apoyarse en empresas privadas para divulgar datos urbanos.

Estos ejemplos positivos han dado lugar a peticiones de iniciativas más amplias de apoyo a la cooperación internacional en materia de bienes públicos digitales globales, con mecanismos y plataformas que amplíen estas ideas. Según el Panel de Alto Nivel sobre la Cooperación Digital de las Naciones Unidas, “muchos tipos de tecnologías y contenidos digitales —datos, aplicaciones, herramientas de visualización de datos o planes de estudio— podrían acelerar la consecución de los ODS. Cuando se puede acceder a ellos de manera libre y abierta, con restricciones mínimas sobre la manera en que pueden ser distribuidos, adaptados y reutilizados, podemos pensar en ellos como ‘bienes públicos digitales’”. El Panel recomendó que “una amplia alianza de múltiples partes interesadas, con la participación de las Naciones Unidas, cree una plataforma para intercambiar bienes públicos digitales, atraer talentos y poner en común conjuntos de datos, respetando la privacidad, en las esferas relacionadas con el logro de los ODS” (Naciones Unidas, 2019)[6].

En lo que a los datos se refiere, por “bienes públicos digitales” podría entenderse grandes conjuntos de datos públicos que se comparten bajo licencias abiertas y que han sido cuidadosamente anonimizados para reducir los riesgos de identificación personal. El término también podría incluir las herramientas y plataformas de código abierto que permitan el acceso y el tratamiento de dichos datos para proporcionar inteligencia digital (Gurumurthy y Chami, 2019). La Alianza de Bienes Públicos Digitales fue creada en relación con esas demandas. La Alianza ha definido seis áreas clave relevantes para los Objetivos de Desarrollo Sostenible con el fin de construir una colección de bienes públicos digitales: lectura en los primeros grados, inclusión financiera, adaptación al cambio climático, salud digital, habilidades digitales y laborales, y aprendizaje a distancia[7].

La noción de datos “como bien público” también puede proporcionar un enfoque importante para que las alianzas de países y organizaciones orientadas al desarrollo se unan para apoyar la compartición transfronteriza de datos. Como han demostrado los éxitos anteriores de los Estados que han abierto el acceso a sus datos, los Gobiernos suelen disponer de datos útiles, así como las empresas. Sin embargo, para compartirlos hacen falta actividades y apoyos adicionales, así como herramientas adecuadas, de manera que se contribuya al desarrollo. Aprender de estas alianzas de datos puede ser importante para fomentar los “bienes públicos digitales” como pieza clave para conseguir los objetivos de desarrollo.

[5] Por ejemplo, por empresas como Cisco, International Data Corporation (IDC) y TeleGeography.

[6] Véase la Oficina del Enviado del Secretario General de las Naciones Unidas para la Tecnología (disponible en www.un.org/techenvoy/es/content/digital-public-goods).

[7] Véase la Alianza de Bienes Públicos Digitales (disponible en https://digitalpublicgoods.net).

5. Explorar nuevas formas de gobernanza de los datos

Están surgiendo nuevas formas de gobernanza de los datos que permiten compartirlos como cuestión de interés público. En el contexto actual, son las corporaciones digitales que extraen los datos las que controlan lo que se hace con ellos y, por tanto, se apropian de la mayor parte de los beneficios. Sin embargo, dada la multiplicidad de actores que intervienen como fuentes de datos o que se ven afectados por su uso, la administración de los datos debe ser vista de manera que pueda contribuir al desarrollo. Es necesario replantear la gobernanza de los datos para que esté al servicio de las personas y el planeta. En ese sentido, están surgiendo nuevos modelos de gobernanza de los datos que permiten a diferentes actores asociarse y compartir sus datos, lo que permite potenciar el valor social de los mismos. Esos modelos incluyen las cooperativas de datos, el patrimonio común de datos, las colaboraciones de datos, los fideicomisos de datos, los fiduciarios de datos, la soberanía indígena sobre los datos y los mercados de datos (UNCTAD, 2019a; Micheli y otros, 2020; Mozilla Insights y otros, 2020). Las colaboraciones sobre los datos, como nueva forma de asociación en la que los participantes comparten datos para el bien público, tienen un enorme potencial de beneficio a la sociedad y mejora de la IA. Pueden crear valor al mejorar el análisis situacional y causal; potenciar la capacidad de predicción de los responsables de la toma de decisiones; y hacer que la IA sea mejor, más precisa y más receptiva (Verhulst, 2019).

Estas asociaciones de datos digitales —que reúnen a diferentes organizaciones, organismos públicos incluidos, para unir fuerzas con el fin de recopilar, intercambiar, combinar y compartir sus datos— se están multiplicando en todo el mundo (GagnonTurcotte, Sculthorp y Coutts, 2021). Ya existen muchos ejemplos concretos en diversos ámbitos relacionados con la salud, el medio ambiente, la investigación, la agricultura y la alimentación, y el desarrollo económico. Y pueden abarcar diferentes territorios: pueden ser locales, pero también cruzar las fronteras. Los proyectos Data Collaboratives Explorer, de GovLab, y Data for Empowerment, del Data Futures Lab de Mozilla, son ejemplos de inventarios de estas nuevas prácticas de gobernanza de los datos[8]. Aunque estas iniciativas se encuentran aún en ciernes y no son numerosas, pueden aportar ideas útiles sobre el camino para mejorar la compartición y el uso de los datos en interés público. En este sentido, ha surgido un movimiento de "datos responsables" o "datos para el bien" que pide a las empresas que compartan sus datos con fines filantrópicos en lo que se denomina "filantropía de datos" (PNUD, 2020). Además, la Comisión Europea ha explorado el potencial de la compartición de datos en toda la Unión Europea para ayudar a las administraciones públicas a utilizar los datos del sector privado para el bien público (Comisión Europea, 2020b).

6. Derechos y principios digitales y relacionados con los datos

Como ya se ha dicho, es necesario definir adecuadamente los derechos digitales y los derechos relacionados con los datos. La siguiente etapa es reconocerlos. En los últimos años han proliferado las declaraciones, cartas o manifiestos sobre la ética y los derechos digitales y relacionados con los datos a diversos niveles (Digital Future Society, 2019). Uno de los primeros ejemplos de ello es la Carta de Derechos Humanos y Principios para Internet de 2011, del Foro para la Gobernanza de Internet (FGI). También cabe citar estos otros ejemplos[9]:

- Manifiesto por la Justicia Digital.
- Datos para las emergencias sanitarias internacionales: gobernanza, operaciones y competencias.

[8] Véase https://datacollaboratives.org/explorer.html?#data-pooling y https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/. Véase también Data Collaboratives, Leveraging Private Data for Public Good. A Descriptive Analysis and Typology of Existing Practices, disponible en https://datacollaboratives.org/static/files/existing-practices-report.pdf.

[9] Para más información a este respecto, véase www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf, https://justnetcoalition.org/digital-justice-manifesto.pdf, https://rsc-src.ca/sites/default/files/DES7289_3_S7%20Statement_Data_EN_FINAL.pdf, https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf, www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html, https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/SEDIA_Carta_Derechos_Digitales.aspx, https://ec.europa.eu/isa2/sites/default/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_pdf, https://citiesfordigitalrights.org/declaration y https://digitaldeclaration.com/img/uploads/EN_DigitalDeclaration_2-Pager_R3_WEB_2020-compressed_200225_115932.pdf.

- Declaración Africana sobre Derechos y Libertades en Internet.
- Carta Digital del Canadá.
- Carta de Derechos Digitales de España.
- Declaración de Berlín sobre la Sociedad Digital y el Gobierno Digital Basado en Valores.
- Declaración de la Coalición de Ciudades por los Derechos Digitales.
- Declaración digital (compromiso con la empresa responsable en la era digital).

Estos y otros ejemplos muestran la necesidad de definir y reconocer los derechos en el nuevo contexto de la economía digital impulsada por los datos. Estas declaraciones de derechos y principios son muy ambiciosas y no implican ninguna obligación. Sin embargo, en su mayoría están centradas en el ser humano y pueden constituir una guía útil para avanzar en la búsqueda de un terreno de entendimiento sobre los derechos relacionados con los datos a nivel mundial.

Los problemas referentes a los derechos relacionados con los datos también están presentes en el derecho mercantil. Como ha señalado la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI, 2020:5), “en el contexto de las operaciones de datos, parece haber incertidumbre no solo entre las partes en cuanto a los derechos y obligaciones que deben establecerse en sus contratos, sino también entre los abogados y los jueces en cuanto a la aplicación de las normas y principios vigentes del derecho de los contratos”.

Podría incluso resultar que sea necesario revisar los marcos generales de derechos y actualizarlos a las nuevas realidades que no existían cuando se diseñaron. La necesidad de regulación en la economía digital tiende a considerarse como la necesidad de hacer encajar los nuevos fenómenos en la normativa existente. Por ejemplo, se ha considerado que los flujos de datos transfronterizos se inscriben en el sistema de comercio internacional, que es donde se debate sobre su regulación internacional. Sin embargo, como se señala en este Informe, los datos son muy diferentes de los bienes y servicios, y la regulación de sus flujos transfronterizos requiere un enfoque diferente al del comercio internacional.

Del mismo modo, no hay duda de que los derechos humanos en el mundo analógico deben respetarse en el espacio digital. El Secretario General de las Naciones Unidas, en su llamamiento a la acción en favor de los derechos humanos en medio de la pandemia, destacó que “seguimos manteniendo que los derechos humanos también se aplican en el mundo virtual” (Naciones Unidas, 2020c). No hay duda de que así es, pero podría ser que hayan surgido nuevas violaciones de los derechos humanos en el espacio digital que no existían cuando se aprobó la Declaración Universal de Derechos Humanos. Por ejemplo, en 1948 nadie podría haber previsto que el derecho al olvido sería importante, pero hoy en día la información antigua publicada en los medios sociales sobre una persona podría impedir a esta ser seleccionada para un puesto de trabajo. Por lo tanto, podría ser necesario pensar de forma innovadora.

7. Normas relacionadas con los datos

Otra forma de avanzar en la facilitación de los flujos de datos transfronterizos para el desarrollo inclusivo con las salvaguardias necesarias es la normalización. Estableciendo normas se facilita que los datos circulen entre diferentes países y sistemas, al determinar características necesarias para la interconexión como la interoperabilidad y la portabilidad de los datos. Con las normas también se fomenta la confianza en los procesos de digitalización y se establecen puntos de referencia adecuados en relación con la gobernanza de los datos (Girard, 2019, 2020). Las normas pueden referirse a diferentes ámbitos, como los aspectos técnicos o la privacidad. También es fundamental elaborar “normas comunes sobre datos abiertos que orienten a los sectores público y privado sobre cómo proporcionar acceso abierto a los conjuntos de datos, a fin de garantizar que más datos pasen a ser bienes públicos digitales, respetando al mismo tiempo la privacidad y la confidencialidad” (Naciones Unidas, 2020a).

Como se ha comentado en el capítulo IV, las principales áreas de influencia a nivel mundial en materia de gobernanza de los datos son los Estados Unidos, China y la Unión Europea. Las tres están tratando de establecer normas globales para la economía digital impulsada por los datos. Sin embargo, es evidente

que no existe un único enfoque de la gobernanza de los datos, ya que las condiciones tecnológicas, económicas, políticas, institucionales y culturales varían de un país a otro. Por ello, las normas deben ser suficientemente flexibles para adaptarse a las condiciones particulares de cada país. Las normas no deben imponerse, sino que deben acordarse de forma colectiva, inclusiva y global.

8. Iniciativas de cooperación internacional sobre la gobernanza de las plataformas

Los intercambios desiguales en la economía digital impulsada por los datos están estrechamente relacionados con los desequilibrios de poder de mercado resultantes del dominio de las corporaciones digitales globales y de su capacidad de utilizar prácticas de optimización fiscal para eludir el pago de los impuestos que les corresponden (UNCTAD, 2019a). Por lo tanto, la gobernanza de las plataformas en lo que atañe a las políticas de competencia y fiscalidad es clave para corregir esos desequilibrios. Aunque dichas políticas tienden a aplicarse a nivel nacional, hay un margen importante para la cooperación internacional. Y esta cooperación es muy necesaria, teniendo en cuenta el alcance mundial de las corporaciones implicadas. Ninguna autoridad nacional en materia de competencia o fiscalidad puede hacer frente por sí sola a los retos que plantean las corporaciones digitales. Incluso los países y grupos de países desarrollados, como los Estados Unidos y la Unión Europea, tienen dificultades en estas esferas.

La necesidad de adaptar la política de competencia a la nueva realidad de la economía digital impulsada por los datos está suscitando un consenso cada vez mayor (UNCTAD, 2019a; Gökçe Dessemond, 2020). Sin embargo, los avances en materia de cooperación internacional son lentos. Se han celebrado diálogos internacionales, por ejemplo, en el Grupo Intergubernamental de Expertos en Derecho y Política de la Competencia de la UNCTAD. Otro ejemplo es la declaración de "entendimiento común" emitida por las autoridades encargadas de la competencia de los países del G7 en 2019[10].

La cooperación internacional ha adoptado un papel más activo en relación con la fiscalidad en el contexto de la economía digital en los últimos años. En la OCDE se han llevado a cabo complejas negociaciones sobre la erosión de la base imponible y el traslado de beneficios. Se esperaba una solución internacional y consensuada para mediados de 2021 (OECD, 2021); en julio de 2021, 130 países y jurisdicciones del Marco Inclusivo del G20/OCDE sobre la BEPS (erosión de la base imponible y traslado de beneficios) se sumaron a un nuevo plan de dos pilares para reformar las normas fiscales internacionales y garantizar que las empresas multinacionales paguen los impuestos que les corresponden dondequiera que operen. El plan incluye también un impuesto de sociedades mínimo del 15 % en todo el mundo[11]. Aunque el Marco Inclusivo del G20/OCDE sobre la BEPS cuenta con 139 países, carece de inclusividad en cuanto a la voz y la participación de los países en desarrollo. Un mes antes, en junio de 2021, los ministros de finanzas del G7 alcanzaron un acuerdo sobre la reforma fiscal mundial que podría obligar a los principales gigantes tecnológicos multinacionales a pagar los impuestos que les corresponden en los países en que operan. Los ministros del G7 también convinieron en el principio de un tipo mínimo a nivel mundial que obligue a las multinacionales a pagar un impuesto de sociedades de al menos el 15 % en cada país en que operan[12].

Aunque estas medidas constituyen pasos en la buena dirección, no se debe olvidar que se trata de un acuerdo entre unos pocos países desarrollados. Como se analiza en UNCTAD (2019a), el Comité de Expertos sobre Cooperación Internacional en Cuestiones de Tributación de las Naciones Unidas es

[10] Véase G7, "Common Understanding of G7 Competition Authorities on 'Competition and the Digital Economy'", disponible en www.ftc.gov/system/files/attachments/press-releases/ftc-chairman-supports-common-understanding-g7competition-authorities-competition-digital-economy/g7_common_understanding_7-5-19.pdf.

[11] Véase OECD/G20 Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address the Tax Challenges Arising From the Digitalisation of the Economy, 1 de julio de 2021, disponible en https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economyjuly-2021.pdf.

[12] Véase "G7 Finance Ministers Agree Historic Global Tax Agreement", disponible en www.g7uk.org/g7-finance-ministersagree-historic-global-tax-agreement/; y "G7 Finance Ministers and Central Bank Governors' Communiqué", disponible en www.g7uk.org/g7-finance-ministers-and-central-bank-governors-communique/.

un órgano más inclusivo para tratar las cuestiones fiscales desde una perspectiva de desarrollo, por lo que debería reforzarse. El Comité ha continuado su labor sobre la fiscalidad en la economía digital, con especial atención a los impactos en los países en desarrollo (Naciones Unidas, 2021).

En resumidas cuentas, todas estas opciones normativas ponen de manifiesto la necesidad de aumentar el diálogo internacional al más alto nivel para lograr una gobernanza global de los datos más eficaz. Los principios éticos de los datos o las declaraciones sobre los derechos relativos a los datos, así como las normas, pueden considerarse pasos iniciales en la dirección correcta. Sin embargo, suelen aplicarse de forma voluntaria. Para regular eficazmente (garantizando el cumplimiento) los flujos de datos transfronterizos podría ser necesario ir más allá de los enfoques voluntarios. Además, para responder a las necesidades de cooperación internacional, algunos aspectos de la gobernanza de los datos requerirán que se acuerden nuevos marcos normativos a nivel internacional y se adopten a nivel nacional.

Esto plantea la cuestión de cuál podría ser el marco institucional más adecuado a nivel mundial para desarrollar la gobernanza global de los datos. Al acordar las normativas que se aplicarán a nivel nacional, no cabe duda de que el enfoque intergubernamental debe desempeñar un papel importante. Sin embargo, es posible que los organismos intergubernamentales existentes no estén bien preparados para tratar de forma holística los asuntos relacionados con la gobernanza de los datos. Habida cuenta del particular carácter multidimensional de los datos, su amplia y cada vez más crítica relevancia, las numerosas cuestiones e intereses que están en juego, así como la rápida evolución de un contexto lleno de incógnitas, es necesario estudiar soluciones innovadoras. El marco debería ser verdaderamente multilateral, multipartito y multidisciplinar, para incluir todas las complejas interrelaciones que implican los datos. En la siguiente sección se exploran distintas posibilidades para el marco institucional encargado de la gobernanza global de los datos.

D. MARCO INSTITUCIONAL

En diferentes foros de responsables políticos a nivel regional o mundial se han celebrado debates sobre los datos de diversas formas. Surgidas del nacimiento de Internet, las organizaciones de “gobernanza de Internet” fueron diseñadas para regular las cuestiones técnicas a medida que Internet se expandía en todo el mundo (como el sistema de nombres de dominio y los protocolos de Internet). Además, el FGI ha tratado de fomentar un diálogo entre las distintas partes interesadas sobre cuestiones económicas y sociales más generales. Sin embargo, la falta de atribuciones normativas formales ha limitado su capacidad para establecer orientaciones para los poderes públicos. Por lo tanto, sigue sin definirse cuáles son los foros apropiados para una gobernanza global de los datos más amplia.

El Panel de Alto Nivel de las Naciones Unidas sobre la Cooperación Digital, creado por el Secretario General, consultó a muy diversas partes interesadas sobre, entre otros temas, la manera en que debería tener lugar la cooperación digital. En su informe (Naciones Unidas, 2019:22), señaló que “existe una gran insatisfacción con los mecanismos de cooperación digital existentes: un deseo de resultados más tangibles, una participación más activa de los Gobiernos y el sector privado, procesos más inclusivos y un mejor seguimiento. En general, los sistemas deben ser más holísticos, multidisciplinarios, multipartitos, ágiles y capaces de convertir las palabras en hechos”. En el informe se señalaron seis lagunas principales:

- La escasa prioridad asignada a la cooperación tecnológica digital a nivel nacional, regional y mundial.
- La falta de inclusividad en los trabajos que realizan los organismos técnicos y normativos, e incluso la falta de capacidad de muchos para participar de forma efectiva y significativa.
- La superposición y complejidad de las estructuras de cooperación digital, que podrían afectar a su eficacia.
- La insuficiencia de la comunicación y la creación de sinergias entre los organismos para responder a las tecnologías digitales que cada vez afectan a más esferas en que las políticas son elaboradas por instituciones distintas.
- La falta de datos fiables, criterios mensurables y pruebas en los que basar las políticas.

- La falta de confianza entre los Gobiernos, la sociedad civil y el sector privado, que puede dificultar el establecimiento del enfoque de colaboración multipartita necesario para crear mecanismos de cooperación eficaces.

En el informe también se recomendaba emprender un proceso de consulta para elaborar mecanismos mejores y actualizados de cooperación digital mundial. Las consultas mencionadas no habían concluido cuando se preparó el presente Informe[13].

En efecto, los marcos institucionales existentes a nivel internacional no son adecuados para abordar las características y necesidades específicas de la gobernanza mundial de los datos. Para que esta sea eficaz, lo más probable es que se necesite un nuevo marco institucional mundial. En esta sección se analiza por qué dicho marco tendría que ser multilateral, multipartito y multidisciplinar. La gobernanza mundial de los datos también podría requerir la creación de un nuevo organismo internacional que desempeñe un papel de coordinación mundial.

1. Marco multilateral, multipartito y multidisciplinar

El análisis que se ofrece en el presente Informe confirma que para abordar las complicaciones derivadas de las múltiples interconexiones e interdependencias entre las distintas dimensiones de los datos, los diversos actores implicados y las concesiones emergentes, es necesario combinar un enfoque multilateral, multipartito y multidisciplinar de la gobernanza mundial de los datos. Si se hace un inventario de las cuestiones e interrelaciones clave en la gobernanza digital mundial, los datos desempeñan un papel fundamental en todos los ámbitos considerados: tecnológico, jurídico, sociocultural, económico, de desarrollo, de derechos humanos y de seguridad (Kurbalija y Höne, 2021).

Hasta ahora, la gobernanza mundial de los datos y las tecnologías digitales se ha desarrollado por diferentes vías. La mayoría de las cuestiones relacionadas con la gobernanza de Internet, como red de comunicaciones, se han tratado en foros multilaterales. La comunidad de Internet, bien organizada y globalizada, se dedica de lleno a estudiar enfoques para coordinar los recursos de Internet y hacer que la red de redes funcione de forma eficiente. Esta tarea reviste un carácter muy técnico, y tiene lugar en diversos entornos institucionales, como la Corporación para la Asignación de Nombres y Números en Internet (ICANN), el Grupo de Tareas sobre Ingeniería de Internet (IETF) y el Consorcio World Wide Web (W3C). Estos procesos suelen tener lugar con la participación de los pares en igualdad de condiciones (UNCTAD, 2017).

En los foros actuales, el grado de contribución de todas las partes interesadas varía considerablemente. Con el creciente papel de los datos en la sociedad, otras organizaciones relacionadas con los datos han dado pasos para mejorar el componente multilateral. Por ejemplo, el Convenio 108 del Consejo de Europa incluye un foro en el que los Gobiernos nacionales, los reguladores, las partes interesadas del sector privado y los representantes de la sociedad civil pueden recibir información e intercambiar opiniones sobre la promoción y la mejora del Convenio (UNCTAD, 2016). En el caso del FGI, el Secretario General de las Naciones Unidas ha creado un Grupo Asesor Multilateral para asesorar sobre el programa y preparar sus futuras reuniones.

Además, la Comisión de Ciencia y Tecnología para el Desarrollo de las Naciones Unidas proporciona un valioso marco para que todas las partes interesadas articulen el papel de las tecnologías digitales y los datos, como facilitadores de los Objetivos de Desarrollo Sostenible, y para informar y asesorar a los órganos ejecutivos de las Naciones Unidas. Con su mandato de proporcionar a la Asamblea General y al Consejo Económico y Social asesoramiento de alto nivel sobre las cuestiones relacionadas con la ciencia y la tecnología para el desarrollo, podría aprovecharse aún más para explorar la conexión entre los datos, la gobernanza de Internet y el desarrollo (recuadro VII.1).

[13] Véase "Recommendation5A/B. Options for the Future of Global Digital Cooperation", disponible en www.globalcooperation.digital/GCD/Redaktion/EN/Downloads/options-for-the-future-of-global-digital-cooperation.pdf?__blob=publicationFile&v=2; y "Follow-up on Digital Cooperation Architecture", disponible en www.global-cooperation.digital/GCD/Navigation/EN/Follow-up/follow-up.html.

Recuadro VII.1. La Comisión de Ciencia y Tecnología para el Desarrollo y la cooperación internacional para abordar las cuestiones relacionadas con Internet que competen a los poderes públicos

La Comisión de Ciencia y Tecnología para el Desarrollo, órgano subsidiario del Consejo Económico y Social, es el principal foro de las Naciones Unidas para tratar las implicaciones de la ciencia y la tecnología para el desarrollo. Como tal, proporciona una plataforma mundial para el debate y la creación de consenso sobre las tecnologías digitales. Uno de los principales componentes de su mandato es su función de punto focal de todo el sistema para el seguimiento de la Cumbre Mundial sobre la Sociedad de la Información. Sus principios básicos y sus líneas de acción en materia de cooperación digital son acordados por la comunidad internacional. Los informes de la Comisión de Ciencia y Tecnología para el Desarrollo relativos a la Cumbre Mundial sobre la Sociedad de la Información constituyen uno de los mayores depósitos internacionales de conocimientos, experiencias y debates internacionales sobre las dimensiones de desarrollo de las cuestiones digitales[a].

La Comisión ha avanzado en aspectos críticos de la digitalización de la economía y la sociedad, tanto en términos políticos como prácticos. Prestó apoyo al exitoso Grupo de Trabajo sobre Mejoras del Foro para la Gobernanza de Internet (2011-2012)[b] y a dos grupos de trabajo sobre la cooperación reforzada en cuestiones de política pública relacionadas con Internet (2013-2014 y 2016-2018)[c]. Esa labor permitió definir características de alto nivel, así como principios rectores, para reforzar la cooperación al elaborar políticas públicas internacionales relacionadas con Internet. Sin embargo, a pesar de la significativa convergencia de puntos de vista en importantes esferas políticas relacionadas con la digitalización, también puso de manifiesto la existencia de diferentes sensibilidades y enfoques con respecto a otras.

Los conocimientos y la experiencia acumulados por la Comisión en estos procesos de una gran complejidad y con una importante carga política podrían, si los Estados miembros así lo deciden, servir como valiosos aportes a ulteriores deliberaciones en el seno de las Naciones Unidas sobre las conexiones entre la gobernanza de Internet, la gobernanza de los datos y el desarrollo.

Fuente: UNCTAD.

[a] Véase "ECOSOC Document - WSIS Follow-up", disponible en https://unctad.org/publications-search?f[0]=product%3A667.

[b] Véase "Improvements of the Internet Governance Forum (2011–2012)", disponible en https://unctad.org/topic/commission-on-science-and-technology-for-development/igf-2011-2012.

[c] Véase "Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (2013–2014)", disponible en https://unctad.org/topic/commission-on-science-and-technology-for-development/wgec-2013-2014; y "Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (2016–2018)", disponible en https://unctad.org/topic/commission-on-science-and-technology-for-development/wgec-2016-2018.

Los actores de la comunidad de Internet podrían beneficiarse de los puntos de vista de otros ámbitos de la política socioeconómica o de los derechos humanos, y así entender mejor lo que se necesita en términos de desarrollo. A la inversa, los poderes públicos podrían beneficiarse de su colaboración con otros actores, adquiriendo un conocimiento técnico más especializado de la evolución del contexto digital y, de ese modo, garantizando que cualquier acuerdo relevante para los problemas relacionados con los datos sea viable desde el punto de vista operacional y sostenible desde el político, así como menos propenso a tener consecuencias imprevistas o indeseables (UNCTAD, 2017). También podría resultar que para solucionar algunos de los problemas relacionados con las tecnologías de datos deban aplicarse soluciones técnicas. Además, en los procesos de gobernanza de los datos no solo hay que tener en cuenta las disciplinas económicas o técnicas, sino también otras ciencias sociales y humanidades relacionadas con la ética y los derechos humanos.

Para dar con la combinación adecuada en ese marco multilateral, multipartito y multidisciplinar harán falta ideas innovadoras. Deberá adoptarse un enfoque tanto descendente como ascendente; en el mecanismo de gobernanza deberían combinarse de alguna manera estos enfoques. Por razones prácticas, esto podría conllevar que no todos los aspectos de la gobernanza tengan que ser tratados

por todos los grupos o niveles implicados al mismo tiempo. Podría preverse una especie de gobernanza de varios niveles. Sin embargo, sería fundamental contar con un sistema de coordinación de alto nivel a escala mundial. Podrían explorarse nuevas formas de gobernanza para los datos, como los modelos de gobernanza de datos distribuidos y policéntricos (Verhulst, 2017; Singh, 2019). Además, dada la creciente influencia de las tecnologías digitales en nuestra vida y en la sociedad, así como en la economía mundial y las relaciones internacionales, se considera que la diplomacia tecnológica será cada vez más importante (Kurbalija y Höne, 2021; Feijóo y otros, 2020).

2. ¿Se necesita crear un organismo internacional de coordinación que se ocupe de las cuestiones relacionadas con los datos?

A pesar de que se reconoce la necesidad de una mayor colaboración mundial en materia de gobernanza digital, apenas se han producido avances sustanciales en cuanto a la manera de lograrla. En el mencionado informe del Panel de Alto Nivel de las Naciones Unidas sobre la Cooperación Digital se proponen tres posibles modelos: un "Foro para la Gobernanza de Internet Plus", basado en el actual FGI, una "arquitectura de cogobernanza distribuida" y una "arquitectura basada en el concepto del patrimonio común digital". El modelo elegido sería dirigido por las Naciones Unidas.

En lugar de basarse en organizaciones existentes que ya tienen las manos llenas, y a las que se intenta atraer desde demasiadas direcciones, otra opción sería reconocer que la era digital requiere una institución dedicada a evaluar y desarrollar una gobernanza global digital y de los datos y capacitada para ello. Con ella se reconocería que nuestras instituciones mundiales actuales se construyeron para un mundo diferente, que ahora estamos en un nuevo mundo digital dominado por cuestiones intangibles, y que se necesitan nuevas estructuras de gobernanza. En palabras de Medhora y Owen (2020), "necesitamos un modelo tipo Bretton Woods que mitigue las implicaciones negativas de la revolución digital y dé paso a una nueva era de prosperidad compartida".

Una posible opción que se ha propuesto consiste en inspirarse en el Consejo de Estabilidad Financiera, que fue creado por el G20 para controlar y volver a regular los bancos y las aseguradoras a nivel mundial a raíz de la falta de regulación suficiente y los fallos reguladores que condujeron a la crisis financiera mundial de 2008. Basándose en ese modelo, podría crearse un Consejo de Estabilidad Digital para que se ocupe de las complejas cuestiones políticas y reguladoras derivadas de las tecnologías digitales a nivel mundial[14]. Sus funciones podrían incluir:

- Coordinar la elaboración de normas, reglamentos y políticas en las numerosas áreas relevantes para las plataformas. Esas áreas incluirían —de manera no exhaustiva— la gobernanza a lo largo de la cadena de valor de los datos y la IA (en esferas como la privacidad, la ética, la calidad y la portabilidad de los datos, la rendición de cuentas algorítmica, etc.); el contenido de los medios sociales; la política de competencia; y la integridad electoral. El objetivo de la coordinación sería elaborar un conjunto de principios y normas que pudieran aplicarse en todo el mundo, permitiendo al mismo tiempo variaciones nacionales para reflejar las condiciones de cada país.
- Evaluar las vulnerabilidades derivadas de estas tecnologías, incluido su impacto en la sociedad civil, y las medidas reguladoras y estratégicas necesarias para tratarlas oportunamente.
- Controlar la evolución de la situación, asesorar sobre las mejores prácticas y estudiar las medidas reguladoras y estratégicas necesarias para hacer frente a las vulnerabilidades en el momento oportuno.
- Garantizar que esta labor beneficie a otras organizaciones que necesitan modernizar las normas para reflejar la inteligencia de datos y la IA, pero también elaborar un marco con el que evaluar las implicaciones.

Este Consejo ofrecería claramente una oportunidad para que los países en desarrollo y los desarrollados trabajaran juntos. Su creación sería toda una declaración de intenciones y un reconocimiento de que el mundo digital necesita su propia institución y una gobernanza internacional integrada. Se centraría

[14] Para más información sobre la propuesta del Consejo de Estabilidad Digital, véase Fay (2019).

explícitamente en los resultados —por ejemplo, en la elaboración de normas voluntarias y en la aplicación, estudio y evaluación de los cambios— en un entorno multilateral, para evitar la captura de intereses creados. No se basaría en un tratado, al menos inicialmente, dado que los requisitos para crear una institución de este tipo serían elevados y podrían, de hecho, disuadir de su creación. Se trataría más bien de un foro de debate.

Esta propuesta contiene algunos elementos útiles para avanzar en la dirección de la creación de un organismo de coordinación internacional que se centre en las cuestiones relacionadas con los datos. Sin embargo, la estabilidad no sería uno de los principales problemas de la economía digital; de hecho, captar las numerosas complejidades que entraña la economía digital impulsada por los datos en un único objetivo no parece factible. Además, y sobre todo, se trata de una propuesta centrada únicamente en el G20.

Para abarcar todas las cuestiones analizadas en este Informe se necesita mucho más. Los debates mundiales sobre la gobernanza de los datos y la IA —así como la posible creación de un organismo internacional o de eventuales marcos normativos resultantes de esos debates— deben ser plenamente inclusivos, por lo que deberían tener lugar bajo los auspicios de las Naciones Unidas, que es el foro internacional más inclusivo en cuanto a la representación de los países. Actualmente, los países en desarrollo están poco representados en las iniciativas mundiales y regionales, lo que hace que se descuiden los conocimientos locales y el contexto cultural, así como sus intereses y necesidades, y contribuye a aumentar la desigualdad (recuadro VII.2).

Los debates estratégicos internacionales también deberían combinar procesos intergubernamentales con procesos verdaderamente multipartitos. Además, la inclusión debería empezar por el lenguaje utilizado. Como se ha señalado anteriormente, ha habido voces que han pedido un nuevo impulso digital similar a Bretton Woods o un *New Deal* digital. Los acuerdos de Bretton Woods y el *New Deal* fueron grandes logros en su momento; contribuyeron a una próspera recuperación tras la Segunda Guerra Mundial y a una cooperación multilateral muy necesaria. Aunque las circunstancias actuales pueden ser similares en varios aspectos, la situación no es la misma. Como muchos países en desarrollo aún no eran independientes en el momento en que se celebraron los acuerdos de Bretton Woods, no formaban parte de ellos. Y el *New Deal* fue la política de una sola gran potencia. Además, el contexto cambiante de la digitalización es muy diferente. Por lo tanto, sería aconsejable hacer uso de cierta creatividad para encontrar nuevos términos que reflejen más adecuadamente las realidades y necesidades actuales de todos los países y partes interesadas.

En las Naciones Unidas ya existen varias iniciativas que se centran en cuestiones relacionadas con la gobernanza de los datos. Algunas ya se han tratado en este capítulo, como el Panel de Alto Nivel de las Naciones Unidas sobre la Cooperación Digital, el FGI y la Comisión de Ciencia y Tecnología para el Desarrollo. En el recuadro VII.3 se muestran otros ejemplos, aunque no es una lista exhaustiva; muchos otros organismos, así como las comisiones económicas regionales, se dedican cada vez más a estas cuestiones. Esto sería ya suficiente para justificar la creación de un órgano fuerte de coordinación en el sistema de las Naciones Unidas. Los datos se han convertido en un recurso económico y estratégico clave —que afecta a todos los actores, sectores, actividades y países—, así como en un ingrediente fundamental para lograr los Objetivos de Desarrollo Sostenible. Por ello, su gobernanza debe abordarse de forma transversal. Sin embargo, el rápido aumento de la importancia de los datos y las tecnologías digitales en la economía mundial, así como las necesidades particulares de su gobernanza, podrían hacer necesario un órgano de coordinación internacional dedicado a la gobernanza y el desarrollo de los datos a nivel mundial, con la función de coordinar las actividades relacionadas con los datos en el sistema de las Naciones Unidas.

La labor de este organismo de coordinación debería complementar la de otras iniciativas y propuestas regionales y mundiales relacionadas con la gobernanza de los datos, incluidas las que se tratan en el capítulo VI. En el recuadro VII.4 se presentan otras iniciativas mundiales relacionadas con los datos.

Además, en los últimos tiempos han aumentado los llamados a la formación de coaliciones o alianzas de países afines sobre las cuestiones relacionadas con los datos y las tecnologías digitales[15]. Un ejemplo

[15] Véase, por ejemplo, Fogh Rasmussen (2021), Vestager y Borrell (2021) e Imbrie y otros (2020).

Recuadro VII.2. Participación de los países en desarrollo en la gobernanza mundial de los datos

Para que la gobernanza internacional de los datos responda a las necesidades de países con niveles de preparación muy diferentes, de modo que puedan participar en la economía digital impulsada por los datos y beneficiarse de ella, es necesario que estén representados y que sus voces se escuchen en los debates correspondientes. Los debates deben tener alcance mundial, con la plena participación de todas las regiones, incluidos los países en desarrollo con economías digitales incipientes. Actualmente, la representación de las economías menos avanzadas es limitada en los principales foros de debate sobre la gobernanza de los datos. Algunos ejemplos son:

- El Convenio 108 del Consejo de Europa —el acuerdo con más apoyo y mayor potencial para impulsar la compatibilidad— cuenta con 55 Estados partes, de los cuales solo 2 son PMA (Burkina Faso y Senegal).
- En las negociaciones de la Iniciativa de Declaración Conjunta sobre comercio electrónico en la Organización Mundial del Comercio (OMC), hasta mayo de 2021, solo cuatro PMA habían decidido participar (Benín, Burkina Faso, Myanmar y República Democrática Popular Lao).
- La Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo) solo ha sido ratificada por ocho países, entre ellos cinco PMA (Angola, Guinea, Mozambique, Rwanda y Senegal).
- Menos de la mitad de los PMA han aprobado una ley de protección de datos y privacidad.
- Un examen de las iniciativas de gobernanza de los datos permitió encontrar relativamente pocos ejemplos de iniciativas replicables a escala respecto de más de un puñado de enfoques de gobernanza de los datos que se repiten con frecuencia. La mayoría de ellas se emprendieron en unos pocos países europeos, el Canadá y los Estados Unidos, y principalmente en inglés (Mozilla Insights y otros, 2020).
- También hay una serie de iniciativas mundiales que establecen normas para el desarrollo y el uso de la IA. Sin embargo, los países en desarrollo están prácticamente ausentes o poco representados en la mayoría de ellas, aunque estas iniciativas podrían tener importantes repercusiones para su desarrollo económico y social.

Fuente: UNCTAD.

de alianza iniciada recientemente es el Consejo de Comercio y Tecnología entre la Unión Europea y los Estados Unidos para liderar la transformación digital global basada en valores[16]. En cuanto a países por separado, China ha propuesto la creación de una iniciativa mundial sobre la seguridad de los datos[17]. En lo relativo al desarrollo mundial, estas iniciativas pueden ser útiles solo en la medida en que se consideren la base, con el objetivo final de contribuir a una verdadera gobernanza mundial. Si se entienden como grupos cerrados de países que actúan de forma diferente al resto del mundo, su contribución a los objetivos de desarrollo mundial inclusivo y a no dejar a nadie atrás podría ser limitada. Tratar de lograr un consenso mundial en el contexto de las Naciones Unidas sería una mejor opción, preferiblemente con un nuevo organismo de coordinación internacional. Este debería adoptar la forma que decidan los Estados miembros. Por ejemplo, podría ser un mecanismo similar al Consejo Económico y Social para las cuestiones relacionadas con los datos.

[16] Véase Comisión Europea, "EU-US launch Trade and Technology Council to lead values-based global digital transformation", disponible en https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990; y Consejo Europeo, "EU-US summit statement: 'Towards a renewed Transatlantic partnership'", disponible en www.consilium.europa.eu/en/press/press-releases/2021/06/15/eu-us-summit-statement-towards-a-renewed-transatlantic-partnership/.

[17] Véase Ministerio de Relaciones Exteriores de la República Popular China, "Global Initiative on Data Security", 8 de septiembre de 2020, disponible en www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml.

Recuadro VII.3. La labor de las Naciones Unidas sobre las cuestiones relacionadas con la gobernanza de los datos

Además de prestar servicios a la Comisión de Ciencia y Tecnología para el Desarrollo, la *UNCTAD* también contribuye a los debates internacionales sobre la gobernanza digital y la gobernanza de los datos por conducto de sus tres pilares de trabajo. El *Informe sobre la economía digital* es un ejemplo del pilar de investigación y análisis. En materia de creación de consenso, el Grupo Intergubernamental de Expertos en Comercio Electrónico y Economía Digital ha contribuido con amplios debates sobre el papel de los datos y las políticas conexas. Por último, las actividades de cooperación técnica han examinado las normativas relacionadas con los datos, por ejemplo, con el Global Cyberlaw Tracker de la UNCTAD. Además, la UNCTAD forma parte de varias alianzas que se ocupan de la medición de la economía digital, también en relación con los datos.

La *Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH)* se ha mostrado cada vez más activa en relación con el respeto de los derechos humanos en el espacio digital, ya que cada vez se realizan más actividades humanas a través de Internet. Por ejemplo, el Relator o Relatora Especial sobre el derecho a la privacidad elabora múltiples informes sobre cuestiones relacionadas con los datos, como la protección de datos, la vigilancia y los datos abiertos. La Oficina también estudia la importancia de las nuevas tecnologías para la realización de los derechos económicos, sociales y culturales (OHCHR, 2020).

La *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)* desempeña un papel central y de coordinación dentro del sistema de las Naciones Unidas en cuanto a las cuestiones jurídicas relacionadas con la economía y el comercio digitales. En un principio, su labor en el ámbito del comercio electrónico se centraba en la eliminación de los obstáculos jurídicos al uso de los datos como medio para establecer relaciones jurídicas y satisfacer los requisitos legales. Con el tiempo ha pasado a establecer un entorno jurídico que permita los flujos de datos, incluido el uso de los datos como base de las herramientas de comercio. En las *Notas sobre las principales cuestiones relacionadas con los contratos de computación en la nube* se analizan las cuestiones de derecho contractual relacionadas con la prestación de servicios de computación en la nube y se abordan varias cuestiones jurídicas específicas de los flujos de datos transfronterizos, como la localización de los datos y los requisitos de privacidad de los datos en virtud de la legislación aplicable, así como las cuestiones relacionadas con el acceso y la portabilidad. En 2018, la CNUDMI se embarcó en un proyecto para explorar las cuestiones jurídicas relacionadas con la economía digital. Las transacciones transfronterizas de datos a lo largo de la "cadena de valor de los datos" se definieron desde el principio como tema de interés. Como "mapa para orientar la labor futura", la Comisión pidió a la Secretaría que preparara una taxonomía jurídica de las tecnologías emergentes y sus aplicaciones, que contiene una sección sobre las transacciones de datos (UNCITRAL, 2020). Uno de los temas generales que ha surgido de la labor exploratoria de la CNUDMI es la conveniencia de elaborar una respuesta armonizada a las cuestiones jurídicas relacionadas con la economía y el comercio digitales.

La *Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)* da prioridad a las soluciones abiertas y, por lo tanto, a la mejora de la transferencia transfronteriza de datos en ámbitos como el cambio climático, la gestión de los recursos hídricos, el desarrollo transfronterizo, los datos oceanográficos, la educación, la cultura y la biodiversidad, entre otros, facilitando los flujos de datos transfronterizos en las transacciones de conocimiento. Al fomentar el acceso universal de los Estados miembros a la información y el conocimiento disponible, la UNESCO aboga por el uso de las tecnologías de la información y la comunicación (TIC), los recursos educativos abiertos, el acceso abierto a la información científica, los datos abiertos y las TIC de banda ancha. La labor de la UNESCO en materia de datos transfronterizos se basa en los principios de datos FAIR (por sus siglas en inglés: encontrabilidad, accesibilidad, interoperabilidad y reutilización), y garantiza el pleno aprovechamiento del poder de los datos para aplicaciones innovadoras y socialmente beneficiosas. La UNESCO también ha liderado la labor interinstitucional de las Naciones Unidas para formular recomendaciones sobre la ética de la IA, en la que los datos desempeñan un papel fundamental (UNESCO, 2020).

La *Unión Internacional de Telecomunicaciones (UIT)* desempeña un papel fundamental en los aspectos tecnológicos y técnicos de la gobernanza mundial de la red. Ha codirigido con la UNESCO la labor mencionada sobre la ética de la IA. También ha realizado trabajos sobre los datos para realizar el bien. Su Iniciativa Muncial sobre la IA y el Patrimonio Común de Datos es un programa y una plataforma de colaboración que contribuye a la aplicación de soluciones beneficiosas basadas en la IA para avanzar en el logro de los Objetivos de Desarrollo Sostenible. Cuenta con una plataforma de regulación digital que abarca múltiples áreas de la gobernanza de las tecnologías emergentes (https://digitalregulation.org).

El *Pulso Mundial de las Naciones Unidas* es la iniciativa del Secretario General sobre la inteligencia de datos y la IA para el desarrollo, la labor humanitaria y la paz. Se apoya en una red de laboratorios para acelerar el descubrimiento, el desarrollo y el uso responsable de la inteligencia de datos y las innovaciones de IA. Su Marco Mundial de Acceso a Datos tiene como objetivo principal permitir el intercambio de datos entre los sectores público y privado de manera que se proteja la privacidad ayudando a desarrollar y ampliar los proyectos impulsados por la IA.

El *Grupo de Expertos Gubernamentales de las Naciones Unidas sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional* y el *Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional* son los que se ocupan de las cuestiones de seguridad.

El *Fondo de las Naciones Unidas para la Infancia (UNICEF)* creó la Alianza de Bienes Públicos Digitales (junto con el Gobierno de Noruega) y está estudiando la gobernanza de los datos de los niños y niñas.

La *Comisión de Estadística de las Naciones Unidas*, el órgano decisorio de más alto nivel respecto de las actividades estadísticas internacionales, establece normas estadísticas y crea conceptos y métodos, incluida su aplicación a nivel nacional e internacional. Decidió crear el Comité de Expertos de las Naciones Unidas sobre la Inteligencia de Datos y la Ciencia de Datos para las Estadísticas Oficiales. También organiza el Foro Mundial de Datos de las Naciones Unidas.

Fuente: UNCTAD.

Recuadro VII.4. Otras iniciativas relevantes para la gobernanza mundial de los datos

La *Red de Políticas de Internet y Jurisdicción* es la principal organización multilateral que aborda la tensión existente entre la naturaleza transfronteriza de Internet y las jurisdicciones nacionales. Su secretaría facilita un proceso mundial de formulación de políticas en el que participan más de 400 entidades clave de más de 70 países, como Gobiernos, las mayores empresas de Internet del mundo, operadores técnicos, grupos de la sociedad civil, universidades y organizaciones internacionales. Ha publicado un estudio que enmarca el debate en torno a la libre circulación de los datos y la soberanía sobre los mismos mediante una serie de consultas con actores de los Estados, las organizaciones internacionales, las empresas, la sociedad civil, la comunidad técnica y las universidades. Con dicho estudio se pretende desentrañar los conceptos de libre circulación de los datos y soberanía sobre los datos, y explorar sus implicaciones para los sistemas de gobernanza. En el estudio se llega a la conclusión de que para hacer frente a los retos relacionados con la gobernanza de la creciente "dataesfera" es necesario organizar un debate mundial entre las múltiples partes interesadas de todos los sectores, reorientar la labor conexa para lograr más matices y objetivos comunes, y explorar y fomentar enfoques innovadores en herramientas, marcos y conceptos (De La Chapelle y Porciuncula, 2021).

El *New Deal Digital* es un proyecto de colaboración de la Just Net Coalition y de IT for Change, con contribuciones de universitarios y activistas, para diseñar formas innovadoras de relacionarse con el mundo digital en el panorama posterior a la COVID-19, recuperando su promesa original y construyendo un mundo digitalmente justo. Defiende la gobernanza democrática y los mecanismos reguladores eficaces en todo el ámbito digital, situando en el foco el desarrollo centrado en las personas. Una de las propuestas incluidas es su Nueva Convención para los Datos y el Ciberespacio (Hill, 2020).

El proyecto *Justicia de Datos Mundial*, del Instituto de Derecho, Tecnología y Sociedad de Tilburg (Países Bajos), se centra en los diversos debates y procesos que se producen en torno a la gobernanza de los datos en diferentes regiones, con el fin de extraer principios generales y definir las necesidades que puedan impulsar la gobernanza de las tecnologías de datos en dirección a la justicia social.

La *Asamblea Global de Privacidad* reúne a autoridades de protección de datos y privacidad locales, nacionales e internacionales. Sus objetivos son servir de foro mundial para las autoridades de protección de datos y privacidad, difundir conocimientos y proporcionar asistencia práctica para ayudar a las autoridades a desempeñar mejor sus funciones, proporcionar liderazgo a nivel internacional en materia de protección de datos

y privacidad, y conectar y reforzar las iniciativas a nivel nacional y regional, y en otros foros internacionales, para que las autoridades puedan proteger y promover mejor la privacidad y la protección de datos.

La *OCDE* examina las cuestiones de gobernanza de los datos y de sus flujos transfronterizos en el marco de su proyecto integrado Going Digital. Este contribuye a la labor del G20 sobre la economía digital. En torno a un compromiso compartido con la Recomendación de la OCDE sobre Inteligencia Artificial, la Alianza Mundial sobre Inteligencia Artificial reúne a mentes comprometidas y expertas de la ciencia, la industria, la sociedad civil, los Estados, las organizaciones internacionales y las universidades para fomentar la cooperación internacional. Incluye un Grupo de Trabajo sobre la Gobernanza de los Datos.

El *Foro Económico Mundial* lleva a cabo una serie de actividades sobre cuestiones relacionadas con la gobernanza de los datos y de sus flujos de datos. Entre ellas se encuentran la plataforma Configuración del Futuro de la Gobernanza de la Tecnología: Política de Datos, el Consejo del Futuro Global sobre la Política de Datos y la Cumbre sobre la Gobernanza Global de la Tecnología 2021, que pretende ser la principal reunión mundial multilateral dedicada a garantizar el diseño y la implantación responsables de las nuevas tecnologías mediante la colaboración público-privada.

"Solid" (derivado en inglés de "social linked data", o "datos vinculados sociales") es un conjunto propuesto de convenciones y herramientas para construir aplicaciones sociales descentralizadas basadas en los principios de los datos vinculados. "Solid" es modular y extensible, y se basa, en la medida de lo posible, en los estándares y protocolos existentes del W3C. Se trata de un nuevo proyecto dirigido por Tim Berners-Lee, inventor de la World Wide Web, que tiene lugar en el MIT. El proyecto pretende cambiar radicalmente el funcionamiento actual de las aplicaciones web, dando lugar a una verdadera propiedad de los datos, así como a una mayor privacidad.

Fuente: UNCTAD.

E. MARGEN DE ACTUACIÓN PARA EL DESARROLLO

Aunque este Informe se ha centrado en el marco político internacional de los flujos de datos transfronterizos, es importante destacar que este debe complementarse con las políticas nacionales para lograr que la economía digital impulsada por los datos funcione para el desarrollo. Los países se encuentran en diferentes niveles de desarrollo y preparación para participar y beneficiarse de la economía digital impulsada por los datos. No existe un enfoque único de la regulación de los flujos de datos transfronterizos. Por lo tanto, las políticas internacionales en esta materia deben incluir cierta flexibilidad para garantizar que los países en desarrollo dispongan del margen de actuación necesario para desarrollarse en la economía digital impulsada por los datos; por ejemplo, deben permitir a los países en desarrollo implementar políticas industriales para añadir valor a los datos nacionales. Al mismo tiempo, los países en desarrollo deben seguir creando las capacidades necesarias para beneficiarse de la economía digital impulsada por los datos, como se analiza en la siguiente sección.

En el contexto de los debates sobre los flujos de datos transfronterizos en el sistema de comercio, varios países en desarrollo han pedido que se fomenten sus capacidades nacionales en la economía digital, así como sus capacidades institucionales para negociar, antes de regular los flujos de datos transfronterizos a nivel internacional. También se ha considerado prioritaria la necesidad de concluir el Programa de Doha para el Desarrollo antes de estudiar en la OMC la regulación de otras cuestiones, como los flujos de datos transfronterizos. Mientras que el segundo argumento es correcto, el primero podría ser arriesgado. En el contexto actual, las tecnologías digitales evolucionan rápidamente y es necesario llegar a algún tipo de acuerdo internacional para que los datos circulen adecuadamente. Es probable que centrar exclusivamente la atención en el desarrollo de la economía digital nacional impulsada por los datos dé lugar a algo que no se adapte a un eventual nuevo régimen internacional que tal vez no tenga en cuenta las particularidades de los diferentes países. Es probable que las políticas o estrategias nacionales destinadas a fomentar el desarrollo de la economía digital impulsada por los datos fracasen si no tiene en cuenta la perspectiva mundial; del mismo modo, todo régimen internacional de gobernanza de los datos

debería tener en cuenta las circunstancias especiales de los países con diferentes niveles de preparación y capacidades para beneficiarse de los datos.

F. CREACIÓN DE CAPACIDAD PARA LA DIGITALIZACIÓN Y LA FORMULACIÓN DE POLÍTICAS BASADAS EN LOS DATOS

1. Creación de capacidad para la digitalización

Los distintos países se encuentran en diferentes niveles de preparación para participar en la economía digital impulsada por los datos y beneficiarse de ella. La mayoría de ellos necesitan desarrollar su capacidad para digitalizar sus datos y convertirlos en inteligencia digital. Los PMA tienen dificultades particulares en este sentido. La creación de capacidad para la digitalización ayudará a colmar las brechas digitales y las relacionadas con los datos. Para ello será necesario aumentar la inversión en el desarrollo de la conectividad y la infraestructura de datos. El fomento de la iniciativa empresarial digital también es fundamental. Sin embargo, resulta interesante que incluso en los países desarrollados las empresas siguen teniendo notables dificultades para orientarse totalmente hacia los datos; en efecto, según los resultados de la novena encuesta anual a altas y altos dirigentes ejecutivos sobre los temas de la inteligencia de datos y la adopción de la IA, que abarca a 85 empresas de la lista Fortune 1000 o líderes de su sector: "Un decenio después de iniciarse estas iniciativas, las empresas todavía tienen un largo camino por recorrer: solo el 39,3 % de ellas están gestionando los datos como parte de su activo; solo el 24,4 % han forjado una cultura de datos dentro de su estructura empresarial; y solo el 24 % han convertido su empresa en una organización impulsada por los datos" (NewVantage Partners, 2021:7).

Las políticas educativas deben mejorar la alfabetización en el uso de los datos, las competencias digitales y los conocimientos especializados sobre los datos, ya que hay una importante escasez de estas competencias. Como se ha comentado en el capítulo III, la analítica y la transformación de los datos están asociadas a los profesionales de la ciencia de datos y de las TIC. Además, la analítica requiere cada vez más funciones relacionadas con los datos de cualificación media y baja, como la extracción, selección, corrección, filtrado y etiquetado de datos, que son esenciales para la eficacia de las grandes organizaciones basadas en datos. Por otro lado, es importante prestar atención a la innovación y a la política industrial para desarrollar la economía digital. Todo ello contribuirá a la capacidad de los países en desarrollo para añadir valor nacional a los datos y desarrollar su economía.

En el caso de muchos países en desarrollo de pequeño tamaño, podría ser mejor adoptar un enfoque regional de la creación de capacidad para alcanzar la escala y la masa crítica necesarias para la digitalización. Por ejemplo, en el ámbito de las competencias relacionadas con los datos, el APEC ha emprendido la iniciativa titulada Competencias Recomendadas en materia de Ciencia y Analítica de Datos[18].

2. Capacidad institucional de los Estados para regular la economía digital impulsada por los datos

Los recursos humanos e institucionales existentes de los Estados tienen una capacidad limitada para establecer procesos de regulación, por razones que incluyen, entre otras: a) la falta de competencias apropiadas en las administraciones públicas para estar al día de las novedades científicas y tecnológicas que surgen en este espacio; y b) los intereses divergentes y los procesos disfuncionales de transferencia de conocimientos entre las partes interesadas de los sectores universitario, público y privado.

La falta de competencias adecuadas en las administraciones públicas es consecuencia directa de la insuficiente representación de las comunidades técnica y analítica en los procesos de elaboración de marcos legislativos y reguladores, lo que limita la detección tanto de las oportunidades que podrían ofrecer estas tecnologías como de los posibles riesgos y amenazas que podrían surgir. El diseño y la

[18] Véase "Big Data Analytics in Critical Demand Across APEC", disponible en https://www.apec.org/press/features/2017/0620_ dsa; APEC (2017); y Quismorio (2019).

aplicación de buenas políticas podrían resultar gravemente perjudicados si los Estados pierden terreno respecto de los actores privados en cuanto a la comprensión de las propiedades de la tecnología, las características de su comportamiento y las amenazas que van surgiendo.

En cuanto a los intereses divergentes y los procesos disfuncionales de transferencia de conocimientos entre las partes interesadas de los sectores universitario, público y privado, los datos se están convirtiendo en una importante ventaja competitiva para el sector privado (sobre todo en los países avanzados y en China), y la investigación de vanguardia se lleva a cabo cada vez más con incentivos orientados a la obtención de beneficios en lugar de tener en cuenta el bien público o los derechos individuales. Este monopolio del sector privado y la falta de incentivos adecuados de los sectores público o universitario también provocan el flujo de los mejores especialistas hacia el sector privado (Abban, 2020). Un peligro claro a largo plazo es el aumento de la dependencia pública del sector privado con fines de lucro, poniendo seriamente en peligro los valores democráticos y los derechos humanos individuales. Los países menos desarrollados también sufren la huida de sus mejores especialistas a los países desarrollados y están menos representados en la articulación de los debates globales, lo que contribuye a la creciente desigualdad a nivel mundial.

3. Apoyo internacional

Los países en desarrollo tendrán que destinar más recursos internos al desarrollo de su capacidad para crear y captar el valor de los datos a nivel nacional, pero sus recursos financieros, técnicos y de otro tipo podrían ser insuficientes para atender esas necesidades. Esto es aún más evidente en el caso de los PMA. Si bien la pandemia de COVID-19 y su impacto en los ingresos de los Estados han reducido aún más los fondos públicos disponibles, también ha hecho que los Gobiernos y otras partes interesadas sean más conscientes de la necesidad de mejorar su preparación para participar en la economía digital impulsada por los datos y beneficiarse de ella. Ello pone de manifiesto la necesidad del apoyo internacional.

Para garantizar que la transformación digital contribuya a obtener resultados más inclusivos y a alcanzar los Objetivos de Desarrollo Sostenible, es necesario que los esfuerzos nacionales de los países en desarrollo reciban un mayor apoyo de la comunidad internacional. La asistencia oficial para el desarrollo (AOD) destinada a impulsar el desarrollo de la capacidad productiva en el contexto de la digitalización es fundamental. Dicha asistencia debería destinarse también a mejorar las capacidades tecnológicas de los países, incluidas las capacidades digitales, y sus conocimientos sobre el funcionamiento de la economía digital impulsada por los datos.

Las políticas de ayuda y las personas responsables de la toma de decisiones en todo el mundo reconocen cada vez más que la digitalización crea tanto oportunidades como riesgos, y que es necesario seguir explorando la contribución de la AOD a la digitalización para el desarrollo. Solo una pequeña parte de la AOD se destina explícitamente a las implicaciones de las transformaciones digitales para el desarrollo. El análisis realizado por la UNCTAD de los datos de la OCDE indica que la parte del total de la ayuda para el comercio correspondiente a la ayuda para las TIC aumentó del 1,2 % en 2017 al 2,7 % en 2019 (UNCTAD, 2021e). Aunque esa tendencia es positiva, la proporción sigue siendo inferior al 3 % registrado durante el período comprendido entre 2002 y 2005 (OECD y WTO, 2017).

En el contexto de los flujos de datos transfronterizos, el apoyo internacional podría centrarse en una serie de áreas. En primer lugar, podría ayudar a los países en desarrollo a formular los marcos jurídicos y normativos pertinentes. Por ejemplo, menos de la mitad de los PMA cuentan con leyes de protección de datos y privacidad. En segundo lugar, muchos países necesitan formular estrategias nacionales para tratar los datos y los flujos de datos de manera que puedan ayudar a obtener beneficios de desarrollo económico, respetando al mismo tiempo los derechos humanos y las diversas dimensiones de seguridad. En tercer lugar, se necesitan actividades de capacitación diversas, como cursos de formación y servicios de asesoramiento, para crear conciencia sobre los distintos aspectos de los datos y los flujos de datos, y sus implicaciones para el desarrollo. Por último, para lograr resultados inclusivos en los diálogos regionales y mundiales relacionados con la gobernanza de los datos y de las plataformas, los países en desarrollo deben poder participar de forma efectiva en los procesos y reuniones pertinentes. Para ello podría hacer falta un apoyo internacional adicional, de manera que los especialistas de esos países puedan estar sentados a la mesa cuando se celebren dichos diálogos.

G. CONCLUSIONES

Como se ha señalado, existe una clara necesidad de una gobernanza mundial de que pueda complementar las medidas adoptadas en otros niveles de gobernanza. El panorama actual es un mosaico de normativas nacionales basadas en objetivos de desarrollo económico, protección de la privacidad y otros intereses de derechos humanos y seguridad nacional. Esto supone un reto para el espíritu libre, descentralizado y abierto de Internet, y crea obstáculos para una circulación de los datos potencialmente beneficiosa a través de las fronteras. Además, aunque el reto de regular los flujos de datos transfronterizos es de naturaleza global, actualmente no existe una solución satisfactoria a nivel regional o internacional.

Es necesario un enfoque político global y amplio que refleje las múltiples dimensiones interrelacionadas de los datos. Dicho enfoque debe lograr un equilibrio que tenga debidamente en cuenta los diferentes intereses y necesidades, de manera que contribuya a un desarrollo inclusivo y sostenible. Para que funcione realmente en beneficio de las personas y del planeta, el marco internacional de gobernanza de los datos debe permitir que los beneficios de los flujos de datos se distribuyan equitativamente dentro de los países y entre ellos, garantizando al mismo tiempo que se aborden los riesgos y las preocupaciones que puedan surgir. Para lograrlo será necesario un mayor diálogo político que implique a todos los actores pertinentes y que pueda ayudar a diseñar el marco regulador necesario y la configuración institucional conexa, lo que posiblemente desemboque en la creación de un nuevo organismo internacional dedicado a la gobernanza de los datos.

Para que funcione realmente en beneficio de las personas y del planeta, el marco internacional de gobernanza de los datos debe permitir que los beneficios de los flujos de datos se distribuyan equitativamente dentro de los países y entre ellos, garantizando al mismo tiempo que se aborden los riesgos y las preocupaciones.

Las oportunidades que ofrecen las tecnologías digitales basadas en los datos son exhaustivas y omnipresentes; y los riesgos y amenazas que presentan son de tal magnitud que no pueden ser abordados por ninguna nación por separado. Los Gobiernos están relativamente acostumbrados a lidiar con nuevas tecnologías disruptivas que provocan grandes cambios en los procesos de la economía y la sociedad, pero la disrupción relacionada con los datos va más allá e introduce además cuestiones existenciales en torno a la capacidad cognitiva y el control del ser humano, la organización y la construcción de las sociedades, los valores democráticos y los derechos individuales.

La pandemia de COVID-19 ha enseñado al mundo importantes lecciones en relación con las interacciones entre las políticas y los datos y el papel que estos pueden desempeñar para superar las crisis globales. Nunca antes la vida de las personas ha dependido tanto de la ayuda de los datos y la tecnología en tiempo real: desde la vigilancia y el control de la propagación de la pandemia hasta la forma en que realizamos nuestras actividades cotidianas (trabajar, comprar, socializar, recibir educación, etc.), pasando por el tiempo récord en que el mundo científico creó nuevas vacunas. Las crisis de este tipo no obedecen a los límites y fronteras nacionales establecidos, por lo que las soluciones requieren flujos de datos transfronterizos y colaboraciones tecnológicas a una escala similar. Lo mismo ocurre con otros grandes problemas mundiales y amenazas dinámicas para las sociedades, como el cambio climático, el desarrollo sostenible, los prejuicios raciales y las desigualdades de género, las desigualdades digitales y los problemas de seguridad internacional. Los intereses nacionales, junto con los intereses existenciales de los seres humanos y del planeta, se atienden mejor con la colaboración internacional para desarrollar y regular los flujos de datos transfronterizos.

Este Informe proporciona algunas orientaciones, pero no pretende ofrecer soluciones. En el territorio desconocido de la economía digital impulsada por los datos, que evoluciona rápidamente, muchas preguntas no tienen aún respuesta. Las respuestas deben encontrarse mediante un debate político

global, multidisciplinar y multipartito. Es necesario replantear y ampliar el debate político internacional sobre esta cuestión, de manera que se tengan en cuenta las dimensiones económicas y no económicas de los datos. Para responder a los mayores retos de interconexión e interdependencia en la economía mundial de los datos hace falta abandonar los enfoques compartimentados y adoptar un enfoque global, coordinado y holístico. Ello podría requerir formas innovadoras de gobernanza mundial, ya que las antiguas tal vez no sean adecuadas para responder al nuevo contexto.

> Es necesario replantear y ampliar el debate político internacional sobre los flujos de datos transfronterizos, de manera que se tengan en cuenta las dimensiones económicas y no económicas de los datos.

Los retos son extremadamente complejos y multidimensionales, por lo que requieren nuevos modelos de relación entre las múltiples tradiciones disciplinarias y las diferentes partes interesadas de los sectores público y privado, así como de la ciudadanía. Las posibles soluciones deben respetar los derechos humanos universales básicos y ser suficientemente flexibles para reflejar los intereses y culturas locales. La gobernanza también tendrá que ser flexible en el tiempo y ágil, teniendo en cuenta la rápida evolución de las tecnologías digitales y el contexto tecnológico; los retos que hay que abordar hoy podrían ser diferentes de los que surjan dentro de unos años. Dado que muchos de los retos son globales, se necesitan soluciones globales. Las normas internacionales o regionales deben tener en cuenta el margen de actuación político necesario para la creación de capacidad y el desarrollo. Y al construir sus economías e instituciones digitales, así como al diseñar sus políticas de desarrollo, los países en desarrollo no deben perder de vista la dimensión internacional de los datos y su regulación, que influyen en el desarrollo económico nacional.

Sin embargo, no será fácil lograr un terreno de entendimiento ni soluciones globales. De hecho, en esta época de populismo, antiglobalización e intereses creados que compiten por la captura de rentas a partir del uso de las tecnologías y los datos digitales, proponer un nuevo organismo internacional puede parecer no solo sorprendente, sino también contraproducente. Sin embargo, todos estos factores hacen que sea más necesario que nunca tomar una nueva senda en la gobernanza del espacio digital y de los datos. Un refuerzo de los reinos de datos o una escisión en múltiples esferas convertiría una situación ya caótica en una aún más confusa. Esto disminuiría sustancialmente el valor que pueden generar estas tecnologías, además de crear posibilidades para que se produzcan daños sustanciales en la privacidad y la ciberseguridad, así como otros riesgos.

Para garantizar la plena participación de todos los países del mundo en la configuración de las formas de gobernar los flujos de datos a nivel mundial, las Naciones Unidas tendrán que desempeñar un papel central. Ya hay un gran número de entidades de las Naciones Unidas que realizan trabajos importantes en este sentido —respecto de todas las dimensiones de los datos—, muchas de ellas fuera de la Sede de las Naciones Unidas: en Ginebra (como la UIT, la UNCTAD, el ACNUDH, la Organización Mundial de la Salud, la Organización Mundial de la Propiedad Intelectual y la OMC); en París (la UNESCO); y en Viena (como la Oficina de las Naciones Unidas contra la Droga y el Delito y la CNUDMI)[19]. Pero para que las Naciones Unidas puedan desempeñar su papel en este contexto, tendrán que establecer vínculos eficaces con otros procesos e iniciativas en curso dirigidos por la sociedad civil, las universidades y el sector privado.

> Para garantizar la plena participación de todos los países en la configuración de las formas de gobernar los flujos de datos a nivel mundial, las Naciones Unidas tendrán que desempeñar un papel central.

[19] Para una descripción detallada del panorama de las organizaciones internacionales en Ginebra, véase el Geneva Digital Atlas, disponible en https://dig.watch/actors/geneva.

REFERENCIAS

Aaronson SA (2014). Why the US and EU are failing to set information free. VoxEU.org, 14 July. Available at: https://voxeu.org/article/why-us-and-eu-are-failing-set-information-free.

Aaronson SA (2015). Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review*, 14(4): 671–700.

Aaronson SA (2019a). Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows. *Digital Policy, Regulation and Governance*, 21(5): 441–460.

Aaronson SA (2019b). What are we talking about when we talk about digital protectionism? *World Trade Review*, 18(4): 541–577.

Aaronson SA and Leblond P (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, 21(2).

Aaronson SA and Maxim R (2013). Data Protection and Digital Trade in the Wake of the NSA Revelations. *Intereconomics*, 48(5): 281–286.

Abass A (2017). Historical and political background to the Malabo protocol. In: Werle G and Vormbaum M, eds., *The African Criminal Court*, TMC Asser Press, The Hague: 11–28.

Abban D (2020). The Battle for AI Talent, 4 June. Available at: https://becominghuman.ai/the-battle-for-ai-talent-e938f4082f94.

Abbott FM (2009). Cross-Retaliation in TRIPS: Options for Developing Countries. Issue Paper 8. ICTSD Programme on Dispute Settlement and Legal Aspects of International Trade, International Centre for Trade and Sustainable Development, Geneva.

Abramova A and Thorne E (2021). Digital Economy Developments Within the EAEU. In: Piskulova NA, ed., *The Economic Dimension of Eurasian Integration*, Palgrave Macmillan: 161–174.

Access Now (2021). *Shattered dreams and lost opportunities – a year in the fight to #KeepItOn*. The #KeepItOn report on Internet shutdowns 2020, March. Available at: https://www.accessnow.org/keepiton-report-a-year-in-the-fight/.

Ademuyiwa I and Adeniran A (2020). Assessing Digitalization and Data Governance Issues in Africa. CIGI Papers No. 244, Centre for International Governance Innovation, Waterloo, ON.

African Union (2014). African Union Convention on Cyber Security and Personal Data Protection. African Union, Addis Ababa. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

African Union (2020). The Digital Transformation Strategy for Africa 2020–2030. African Union, Addis Ababa, Ethiopia. Available at: https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

Aguerre C (2019). Digital Trade in Latin America: Mapping Issues and Approaches. *Digital Policy, Regulation and Governance*, 21(1): 2–18.

Ahmed N and Wahed M (2020). The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research. arXiv:2010.15581, Cornell University, Ithaca, NY, 22 October. Available at: https://arxiv.org/abs/2010.15581.

Aktoudianakis A (2020). Fostering Europe's Strategic Autonomy – Digital sovereignty for growth, rules and cooperation. European Policy Centre and Konrad-Adenauer-Stiftung, 18 December.

Anwar MA and Graham M (2020). Digital Labour at Economic Margins: African Workers and the Global Information Economy. *Review of African Political Economy*, 47(163): 95–105.

APEC (2017). Recommended APEC Data Science and Analytics (DSA) Competencies. Asia–Pacific Economic Cooperation, Singapore. Available at: https://apru.org/wp-content/uploads/2019/04/Recommended_APEC_DSA_Competencies_Endorsed-8.pdf.

Arcesati R (2020). The Digital Silk Road is a development issue. Mercator Institute for China Studies, Berlin. 28 April. Available at: https://merics.org/en/short-analysis/digital-silk-road-development-issue.

Arnold Z, Rahkovsky I and Huang T (2020). Tracking AI Investment. Initial Findings from the Private Markets. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service,

Washington, DC, September. Available at: https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf.

Arockia P, Varnekha S and Veneshia K (2017). The 17 V's Of Big Data. *International Research Journal of Engineering and Technology*, 4(9).

Arora P (2016). Bottom of the Data Pyramid: Big Data and the Global South. *International Journal of Communication*, 10: 1681–1699.

Arora P (2019). *The Next Billion Users. Digital Life Beyond the West*. Harvard University Press, Cambridge, MA.

Arrieta-Ibarra I et al. (2018). Should We Treat Data as Labor? Moving beyond "Free", *American Economic Association Papers and Proceedings*, 108: 38–42.

Avila R (2018). Digital Sovereignty or Digital Colonialism? *Sur International Journal on Human Rights*, 15(27): 15–27.

Avila R (2020). Against Data Colonialism. In: Muldoon J and Stronge W, eds., *Platforming Equality: Policy Challenges for the Digital Economy*, Autonomy Research Ltd, Crookham Village, September: 47–57.

Aydın A and Bensghir TK (2019). Digital Data Sovereignty: Towards a Conceptual Framework. 2019 1st International Informatics and Software Engineering Conference (UBMYK): 1–6. Available at: https://ieeexplore.ieee.org/document/8965469.

Azmeh S and Foster C (2016). The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements. *LSE Working Paper Series* 2016, No. 16–175, London School of Economics and Political Science, London.

Azmeh S and Foster C (2018). Bridging the Digital Divide and Supporting Increased Digital Trade: Country Case Studies. Discussion Paper, GEGAfrica, Global Economic Governance, Pretoria. Available at: http://www.gegafrica.org/item/862-bridging-the-digital-divide-and-supporting-increased-digital-trade-country-case-studies.

Azmeh S, Foster C and Abd Rabuh A (2021). The Rise of the Data Economy and Policy Strategies for Digital Development. Digital Pathways at Oxford Paper Series, No. 10. Oxford, United Kingdom.

Azmeh S, Foster C and Echavarri J (2020). The International Trade Regime and the Quest for Free Digital Trade. *International Studies Review*, 22(3): 671–692.

Back D, Kalenzi C and Yim M (2021). Digital contact tracing apps help slow COVID-19. Here's how to increase trust. Available at https://www.weforum.org/agenda/2021/05/could-the-governance-required-for-contact-tracing-apps-already-exist/.

Badran MF (2018). Economic Impact of Data Localization in Five Selected African Countries. *Digital Policy, Regulation and Governance*, 20(4): 337–357.

Bagchi K and Kapilavai S (2018). Political Economy of Data Nationalism. 22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, 24–27 June. Available at: http://hdl.handle.net/10419/190347.

Barnes J, Black A, Roberts S, Andreoni A, Mondliwa P and Sturgeon T (2019). Towards a Digital Industrial Policy for South Africa: A Review of the Issues. The Industrial Development Think Tank, Johannesburg. Available at: http://www.thedtic.gov.za/wp-content/uploads/DPIP.pdf.

Bauer M, Erixon F, Krol M and Lee-Makiyama H (2013). The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce. European Centre for International Political Economy, Brussels. Available at: https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

Bauer M, Ferracane MF and van der Marel E (2016). Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization. GCIG (Global Commission on Internet Governance) Paper Series No. 30. Centre for International Governance Innovation, Waterloo, ON and Chatham House, London.

Bauer M, Lee-Makiyama H, van der Marel E and Verschelde B (2014). The Costs of Data Localisation: Friendly Fire on Economic Recovery. ECIPE Occasional paper, No. 3, European Centre for International Political Economy, Brussels.

BDI (2017). Grenzüberschreitende Datenflüsse und EU-Handelsabkommen. Positionspapier, Bundesverband der Deutschen Industrie e.V. (BDI) – The Voice of German Industry, Berlin, 27 June. Available at: https://bdi.eu/publikation/news/grenzueberschreitende-datenfluesse-und-eu-handelsabkommen/.

Bennett CJ and Raab CD (2020). Revisiting the Governance of Privacy: Contemporary Policy Instruments in Global Perspective. *Regulation and Governance*, 14(3): 447–464.

Birch K, Chiappetta M and Artyushina A (2020). The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. *Policy Studies,* 41(5): 468–487.

Bird and Bird (2017). Guide to the General Data Protection Regulation. Bird and Bird, London.

Bleeker A (2020). Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: A review of data protection legislation for alignment with the General Data Protection Regulation. *Studies and Perspectives series - ECLAC Subregional Headquarters for the Caribbean*, No. 94, (LC/TS.2020/126-LC/CAR/TS.2020/4), Economic Commission of Latin America and the Caribbean (ECLAC), Santiago.

Bradford A (2020). The Brussels Effect Comes for Big Tech. Project Syndicate, 17 December. Available at: https://www.project-syndicate.org/commentary/eu-digital-services-and-markets-regulations-on-big-tech-by-anu-bradford-2020-12.

Brathwaite C and Remy JY (2020). E-commerce-related policies, initiatives & legislation across CARICOM: Diagnostic Review 2020. The Shridath Ramphal Centre for International Trade Law, Policy and Services, Barbados.

Brehmer HJ (2018). Data Localization: The Unintended Consequences of Privacy Litigation. *American University Law Review*, 67(3): 927–969.

Bria F (2020). Digital Sovereignty for the People in the post-pandemic World. Medium, 24 August. Available at: https://medium.com/@francescabria/digital-sovereignty-for-the-people-in-the-post-pandemic-world-109472dd736b.

BSA (2012). Lockout: How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets – and What to Do about it. Business Software Alliance, Washington, DC. Available at: https://www.bsa.org/files/reports/BSALockout2012.pdf.

BSA (2017). Cross-border Data Flows. Business Software Alliance, Washington, DC. Available at: https://www.bsa.org/policy-filings/cross-border-data-flows.

Budnitsky S and Jia L (2018). Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance. *European Journal of Cultural Studies*, 21(5): 594–613.

Bughin J and Lund S (2017). The ascendancy of international data flows. VoxEU.org, 9 January. Available at: https://voxeu.org/article/ascendancy-international-data-flows.

Burman A (2020). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? Working Paper, Carnegie India, New Delhi, March.

Burri M (2016). The World Trade Organization as an Actor in Global Internet Governance. SSRN Paper No. ID 2792219, Social Science Research Network, Rochester, NY. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792219.

Burri M (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law*, 48(1): 407–448.

Bygrave LA (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits*. Kluwer Law International, The Hague, London and New York.

Carter WA and Yayboke E (2019). Data Governance Principles for the Global Digital Economy. Center for Strategic & International Studies, Washington, DC, 4 June. Available at: https://www.csis.org/analysis/data-governance-principles-global-digital-economy.

Casalini F and López González J (2019). Trade and Cross-Border Data Flows. *OECD Trade Policy Paper*, No. 220, OECD Publishing, Paris.

Casalini F, López González J and Nemoto T (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. *OECD Trade Policy Paper,* No. 248, OECD Publishing, Paris. Available at: https://doi.org/10.1787/ca9f974e-en.

Casella B and Formenti L (2018). FDI in the Digital Economy: A Shift to Asset-Light International Footprints. *Transnational Corporations*, 25(1): 101–130.

Castro D and McLaughlin M (2021). Who is winning the AI race? China, the EU, or the United States? 2021 Update. Center for Data Innovation, Washington, DC, January. Available at: https://www2.datainnovation.org/2021-china-eu-us-ai.pdf.

Castro D and McQuinn A (2015). Cross-border data flows enable growth in all industries. Information Technology and Innovation Foundation, Washington, DC. Available at: http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=2.142131440.350197758.1621849794-1974323496.1621849794.

Cattaruzza A (2019). *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data.* Le Cavalier Bleu, Paris.

CBInsights (2021). Expert Collection database: Cybersecurity. Investment in cybersecurity companies. Period: 01 January 2016 – 28 January 2021, CBInsights. Dataset downloaded on 28 January 2021. Available at: https://www.cbinsights.com (document extracted on 28 January 2021).

Center for Responsive Politics (2021). Lobbying spending nears record high in 2020 amid pandemic. Center for Responsive Politics, Washington, DC, 27 January. Available at: https://www.opensecrets.org/news/2021/01/lobbying-spending-nears-record-high-in-2020-amid-pandemic/.

CFR (2020). Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms? Council on Foreign Relations, New York, NY. Available at: https://www.cfr.org/china-digital-silk-road/.

Chakravorti B (2018). Why the Rest of the World Can't Free Ride on Europe's GDPR Rules. *Harvard Business Review*, 30 April. Available at: https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules.

Chander A (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, Oxford University Press, 23(3): 771–84.

Chander A and Ferracane M (2019). Regulating Cross-border Data Flows – Domestic Good Practices. In: Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence, White Paper, World Economic Forum, Geneva, December: 7–17. Available at: http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.

Chander A and Lê UP (2014). Breaking the Web: Data Localization vs. the Global Internet. UC Davis Legal Studies Research Paper, No. 378, University of California, Davis.

Chander A and Lê UP (2015). Data nationalism. *Emory Law Journal,* 64(3):677–739.

Chen L, Cheng W, Ciuriak D, Kimura F, Nakagawa J, Pomfret R, Rigoni G and Schwarzer J (2019). The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies. T20 Japan Task Force 8: Trade, Investment and Globalization. Available at: https://t20japan.org/policy-brief-digital-economy-economic-development/.

Chetty M, Sundaresan S, Muckaden S, Feamster N and Calandro E (2013). Measuring Broadband Performance in South Africa. In: Proceedings of the 4th Annual Symposium on Computing for Development (ACM DEV-4 '13). Association for Computing Machinery, New York, NY, Article 1, 1–10. Available at: http://dl.acm.org/citation.cfm?doid=2537052.2537053.

Chin C (2018). AI Is the Future—But Where Are the Women? Available at www.wired.com/story/artificial-intelligence-researchers-gender-imbalance/.

Christakis T (2020). "European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence and Grenoble Alpes Data Institute, December. Available at: https://ssrn.com/abstract=3748098.

Cisco (2018). Cisco Visual Networking Index: Forecast and Trends, 2017–2022. White paper, Cisco. Available at: https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf.

Cisco (2020). Cisco Annual Internet Report (2018-2023). White Paper, Cisco. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.

Ciuriak D (2018). Rethinking Industrial Policy for the Data-driven Economy. CIGI Papers, No. 192, Centre for International Governance Innovation, Waterloo, ON.

Ciuriak D (2019). On the Cusp of Change: Trade and Development in the Age of Data. Presentation at the Egyptian Center for Economic Studies, 23 December. Available at: https://www.youtube.com/watch?v=vC7Qu2zs-KM.

Ciuriak D (2020). Economic Rents and the Contours of Conflict in the Data-driven Economy. CIGI Paper, No. 245, Centre for International Governance Innovation, Waterloo, ON.

Ciuriak D and Ptashkina M (2018). The Digital Transformation and the Transformation of International Trade. RTA Exchange Issues Paper, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB). Available at: https://e15initiative.org/publications/the-digital-transformation-and-the-transformation-of-international-trade/.

Clarke R (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, 34(1): 59–80.

Clinton HR (2010). Remarks on Internet Freedom. United States Department of State, Washington, DC, 21 January. Available at: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

CNNum (2014). Strengthening EU's Negotiation Strategy to Make TTIP a Sustainable Blueprint for the Digital Economy and Society: Opinion of the French Digital Council. Conseil National du Numérique (French Digital Council), Paris, April. Available at: https://cnnumerique.fr/files/uploads/2014/05/Version-web-ANGLAIS-19.05.pdf.

Cofone I (2020). Beyond Data Ownership. *ardozo Law Review* (2021, forthcoming). Available at: https://ssrn.com/abstract=3564480.

Correa CM (2020). Data in Legal Limbo: Ownership, Sovereignty, or a Digital Public Goods Regime? Research Paper, No. 117, South Centre, Geneva.

Cory N (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation, Washington, DC, 1 May. Available at: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

Cory N (2019). The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored. Information Technology and Innovation Foundation, Washington, DC, 1 April. Available at: https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where.

Cory N (2020). Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers. Information Technology and Innovation Foundation, Washington, DC, 27 January. Available at: https://itif.org/publications/2020/01/27/surveying-damage-why-we-must-accurately-measure-cross-border-data-flows-and.

Cory N and Castro D (2018). Crafting an Open and Innovative Digital Trade Agenda for Latin America. Information Technology and Innovation Foundation, Washington, DC, 26 November. Available at: https://itif.org/publications/2018/11/26/crafting-open-and-innovative-digital-trade-agenda-latin-america.

Couldry N and Mejias AU (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 20(4): 336–349.

Couldry N and Mejias AU (2021). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It For Capitalism*. Stanford University Press, Stanford, CA.

Couture S (2020). The Diverse Meanings of Digital Sovereignty. Global Media Technologies & Cultures Lab, Massachusetts Institute of Technology, Cambridge, MA, 5 August. Available at: https://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/.

Couture S and Toupin S (2019). What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *New Media and Society*, 21(10): 2305–2322.

Coyer K and Higgott R (2020). Sovereignty in a Digital Era: A Report Commissioned by The Dialogue of Civilizations Research Institute Berlin. Dialogue of Civilizations Research Institute, Berlin. Available at: https://doc-research.org/wp-content/uploads/2020/09/Sovereignty-in-a-digital-era_____.pdf.

Coyle D, Diepeveen S, Wdowin J, Kay L and Tennison J (2020). The value of data – Policy implications. The Bennett Institute for Public Policy, Cambridge and the Open Data Institute. Available at: https://www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/.

Coyle D and Li W (2021). The Data Economy: Market Size and Global Trade. Presentation at the Allied Social Science Associations (ASSA) Annual Meeting, 3 January, session on Big Data: Competition, Innovation, and Policy. Available at: https://www.aeaweb.org/conference/2021/preliminary/1993?q=eNqrVipOLS7OzM8LqSxIVbKqhnGVrJQMIXSUUstS80qAbCOlWh2IxOLi_GQgx9QYKFOSWpQLZANZKYmVEEZJZm4qhFWWmVoOMqyooFwwZJABCCjV1gJcMD7VH74.

Coyle D and Nguyen D (2019). Cloud Computing, Cross-Border Data Flows and New Challenges for Measurement in Economics. *National Institute Economic Review,* 249(1): R30–R38.

Creemers R (2020). China's Approach to Cyber Sovereignty. Konrad-Adenauer-Stiftung, Berlin.

CRS (2020a). Internet Regimes and WTO E-Commerce Negotiations. CRS Report, R46198, Congressional Research Service, Washington, DC, 28 January.

CRS (2020b). Digital Trade. In: Focus IF10770, Congressional Research Service, Washington, DC, 3 December.

CSET (2020). Tracking AI Investment. Initial Findings from the Private Markets. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, Washington, DC, September. Available at: https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf.

Daskal J (2017). Congress Needs to Fix Our Outdated Email Privacy Law. *Slate*, 26 January. Available at https://slate.com/technology/2017/01/the-confusing-court-case-over-microsoft-data-on-servers-in-ireland.html.

David-West O and Evans PC (2016). The Rise of African Platforms: A Regional Survey. The Emerging Platform Economy Series, No. 2, Center for Global Enterprise (CGE), New York, NY. Available at: https://www.researchgate.net/publication/306401003_The_Rise_of_African_Platforms_A_Regional_Survey.

Daza Jaller L, Gaillard S and Molinuevo M (2020). The Regulation of Digital Trade: Key Policies and International Trends. World Bank, Washington, DC.

De La Chapelle B and Porciuncula L (2021). We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty. Internet & Jurisdiction Policy Network (I&JPN), Paris. Available at: https://www.internetjurisdiction.net/news/aboutdata-report.

De Nardis L (2016). Introduction: One Internet: an evidentiary basis for policy making on Internet universality and fragmentation. In *A Universal Internet in a Bordered World. Research on Fragmentation, Openness and Interoperability*. Vol. I. Global Commission on Internet Governance and Chatham House, Ottawa.

Deardorff AV (2017). Comparative Advantage in Digital Trade. In: Evenett SJ, ed. *Cloth for Wine? The Relevance of Ricardo's Comparative Advantage in the 21st Century*. CEPR Press, London: 35–44.

Dekker B, Okano-Heijmans M and Zhang ES (2020). Unpacking China's Digital Silk Road. Clingendael Report. Clingendael Institute, The Hague. Available at: https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf.

Digital Future Society (2019). Toward better data governance for all: Data ethics and privacy in the digital era. Digital Future Society, Barcelona, July. Available at: https://digitalfuturesociety.com/app/uploads/2019/08/060819_Toward_better_data_governance_for_all_dfs_mwcapital_DIGITAL.pdf.

DigitalEurope, BusinessEurope, ERT and ACEA (2020). Schrems II: Impact Survey Report. DigitalEurope, Brussels, 26 November. Available at: https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2020-11-26_schrems_ii_impact_survey_report.pdf.

Donovan KP and Park E (2019). Perpetual Debt in the Silicon Savannah. *Boston Review*, 20 September. Available at: http://bostonreview.net/class-inequality-global-justice/kevin-p-donovan-emma-park-perpetual-debt-silicon-savannah.

Drake WJ, Cerf VG and Kleinwächter W (2016). Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, World Economic Forum, Geneva, January. Available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Duch-Brown N, Martens B and Mueller-Langer F (2017). The Economics of Ownership, Access and Trade in Digital Data. Digital Economy Working Paper, 2017–01, Joint Research Centre (JRC) Technical Reports, European Commission and JRC, Seville. Available at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.

Ebert I, Busch T and Wettstein F (2020). Business and Human Rights in the Data Economy: A Mapping and Research Study. German Institute for Human Rights, Berlin. Available at: https://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/Publikationen/ANALYSE/Analysis_Business_and_Human_Rights_in_the_Data_Economy.pdf.

ECLAC (2020). Digital Agenda for Latin America and the Caribbean (eLAC2022). LC/CMSI.7/4. Seventh Ministerial Conference on the Information Society in Latin America and the Caribbean, 23–26 November 2020, Economic Commission for Latin America and the Caribbean, Santiago. Available at: https://conferenciaelac.cepal.org/7/sites/elac2020-2/files/20-00902_cmsi.7_digital_agenda_elac2022.pdf.

ECLAC (2021). Datos y hechos sobre la transformación digital. Project Documents. LC/TS.2021/20. Economic Commission for Latin America and the Caribbean, Santiago.

ECLAC and I&JPN (2020). *Internet & Jurisdiction and ECLAC Regional Status Report 2020*. LC/TS.2020/141. Economic Commission for Latin America and the Caribbean and Internet & Jurisdiction Policy Network, Santiago. Available at: https://www.cepal.org/sites/default/files/publication/files/46421/S1901092_en.pdf.

Eder TS, Arcesati R and Mardell J (2020). Networking the "Belt and Road" – The future is digital. Mercator Institute for China Studies, Berlin. Available at: https://merics.org/en/tracker/networking-belt-and-road-future-digital.

EDRi (2015). Data protection and privacy must be excluded from TTIP. European Digital Rights, Brussels, 8 April. Available at: https://edri.org/our-work/data-protection-privacy-ttip/.

Eferin Y, Hohlov Y and Rossotto C (2019). Digital platforms in Russia: Competition between National and Foreign Multi-sided Platforms Stimulates Growth and Innovation. *Digital Policy, Regulation and Governance*, 21(2): 129–45.

Elmi N (2020). Is Big Tech Setting Africa Back? *Foreign Policy,* 11 November. Available at: https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/.

Engels B (2019). Data Governance as the Enabler of the Data Economy. *Intereconomics*, 54(4): 216–222.

Epifanova A (2020). Deciphering Russia's "Sovereign Internet Law". DGAP Analysis, No. 2, German Council on Foreign Relations, Berlin, January. Available at: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

Equinix (2020). Hyperscale vs. Colocation. Equinix, 27 August. Available at: https://blog.equinix.com/blog/2020/08/27/hyperscale-vs-colocation/.

Ericsson (2020). *Ericsson Mobility Report, November 2020*. Telefonaktiebolaget LM Ericsson, Stockholm, November. Available at: https://www.ericsson.com/en/mobility-report/reports/november-2020.

Erie MS and Streinz T (2021). The Beijing effect: China's "Digital Silk Road" as Transnational Data Governance. *New York University Journal of International Law and Politics* (forthcoming). Available at: https://cld.web.ox.ac.uk/article/beijing-effect-chinas-digital-silk-road-transnational-data-governance.

European Commission (2019). Questions and Answers on the Japan adequacy decision. MEMO/19/422. European Commission, Brussels, 23 January. Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_422.

European Commission (2020a). *The European Data Market Monitoring Tool: Key Facts and Figures, First Policy Conclusions, Data Landscape and Quantified stories, D2.9 Final Study Report.* European Commission, Brussels. Available at: https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update.

European Commission (2020b). Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. European Commission, Brussels. Available at: https://digital-strategy.ec.europa.eu/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more.

European Commission (2021). Trade Policy Review – An Open, Sustainable and Assertive Trade Policy. COM/2021/66 final. European Commission, Brussels, 18 February. Available at: https://trade.ec.europa.eu/doclib/docs/2021/february/tradoc_159438.pdf.

European Data Protection Board (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted 10 November 2020). European Data Protection Board, Brussels. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Parliament (2020). Digital sovereignty for Europe. European Parliamentary Research Service Ideas Paper Briefing, European Parliament, Brussels. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

Evans PC (2016). The Rise of Asian Platforms: A Regional Survey. The Emerging Platform Economy Series, No. 3, Center for Global Enterprise (CGE), New York, NY. Available at: https://www.thecge.net/app/uploads/2016/11/FINALAsianPlatformPaper.pdf.

Fanou R, Francois P, Aben E, Mwangi E, Goburdhan N and Valera F (2017). Four Years Tracking Unrevealed Topological Changes in the African Interdomain. *Computer Communications*, 106: 117–135.

Farrell H and Newman AL (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1): 42–79.

Fay R (2019). Digital Platforms Require a Global Governance Framework. A CIGI essay series on Models for Platform Governance, Centre for International Governance Innovation, Waterloo, ON, 28 October. Available at: https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework.

Fay R (2020). CUSMA's Data and Intellectual Property Commitments Could Inhibit Domestic Policy Flexibility. Presentation on 26 February 2020 at the Standing Committee on International Trade, the Canadian Parliament. Centre for International Governance Innovation, Waterloo, ON. Available at: https://www.cigionline.org/articles/cusmas-data-and-intellectual-property-commitments-could-inhibit-domestic-policy.

Fay R (2021). A Model for Global Governance of Platforms. In Moore M and Tambini D, eds., *Regulating Big Tech: Policy Responses to Digital Dominance* (forthcoming), New York: Oxford University Press.

Feijóo C, Kwon Y, Bauer JM, Bohlin E, Howell B, Jain R, Potgieter P, Vu K, Whalley J and Xia J (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, 44(6): 101988.

Feldstein S (2019). The Global Expansion of AI Surveillance. Working Paper, Carnegie Endowment for International Peace, Washington, DC, September.

Ferracane MF, Kren J and van der Marel E (2020). Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries? *Review of International Economics,* 28(3): 676–722.

Ferracane MF and van der Marel E (2020). Digital Innovation in East Asia: Do Restrictive Data Policies Matter? Policy Research Working Paper, No. 9124. World Bank, Washington, DC.

Floridi L (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*, 33(3): 369–378.

Flyverbom M, Madsen AK and Rasche A (2017). Big Data as Governmentality in International Development: Digital Traces, Algorithms, and Altered Visibilities. *The Information Society*, 33(1): 35–42.

Fogh Rasmussen A (2021). Building a Democratic High-Tech Alliance. Project Syndicate, 29 March. Available at: https://www.project-syndicate.org/commentary/democratic-technology-alliance-global-digital-rules-by-anders-fogh-rasmussen-2021-03.

Fortune Business Insights (2021). Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis, By Component (Platform, Solution & Services), By End Use Industry (BFSI, Retail, Government, Healthcare, Manufacturing, Agriculture, Sustainable Energy, Transportation, IT & Telecom, Others), and Regional Forecast, 2021–2028. Report ID: FBI100307, 21 May. Available at: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307.

Foster C (2020). Digital trade in the Kenya-US FTA? The Digital Trade Tracker, 28 September. Available at: https://digitaltradetracker.org/2020/09/28/digital-trade-in-the-kenya-us-fta/.

Foster C and Azmeh S (2020). Latecomer Economies and National Digital Policy: An Industrial Policy Perspective. *Journal of Development Studies*, 56(7): 1247–1262.

Foster C, Graham M, Mann L, Waema T and Friederici N (2018). Digital Control in Value Chains: Challenges of Connectivity for East African Firms. *Economic Geography*, 94(1): 68–86. Available at: https://doi.org/10.1080/00130095.2017.1350104.

Freedom House (2020). User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization. Freedom House, Washington, DC. Available at: https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.

Gagné JF, Hudson S and Mantha Y (2020). Global AI Talent Report 2020. Blog of JF Gagné. Available at: https://jfgagne.ai/global-ai-talent-report-2020/.

Gagné JF, Kiser G and Mantha Y (2019). Global AI Talent Report 2019. Blog of JF Gagné. Available at: https://jfgagne.ai/talent-2019/.

Gagnon-Turcotte S, Sculthorp M and Coutts S (2021). Digital data partnerships: building the foundations for collaborative data governance in the public interest. Open North, Montreal. Available at: https://assets.ctfassets.net/e4wa7sgik5wa/6mV2HLHbhKbU2sgtXSTMQX/da0ede46238b1809d60b5ba65732fb2b/Digital_Data_Partnerships_Report-EN.pdf.

Gao HS (2019). Data Regulation with Chinese Characteristics. SMU Centre for AI & Data Governance Research Paper, No. 2019/04. Singapore Management University (SMU), Singapore.

Gartner (2019). The Data Center is (Almost) Dead. Gartner, 5 August. Available at: https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead/.

Gawer A (2014). Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework. *Research Policy*, 43(7): 1239–1249.

Geist M (2018). Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. A CIGI Essay Series on Data Governance in the Digital Age, Centre for International Governance Innovation, Waterloo, ON, 4 April. Available at: https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security/.

Gheyle N and De Ville F (2017). How Much is Enough? Explaining the Continuous Transparency Conflict in TTIP. *Politics and Governance*, 5(3): 16–28.

Girard M (2019). Standards for the Digital Economy: Creating an Architecture for Data Collection, Access and Analytics. CIGI Policy Brief, No. 155, Centre for International Governance Innovation, Waterloo, ON, 4 September. Available at: https://www.cigionline.org/publications/standards-digital-economy-creating-architecture-data-collection-access-and-analytics/.

Girard M (2020). Standards for Digital Cooperation. CIGI Papers, No. 237, Centre for International Governance Innovation, Waterloo, ON,. Available at: https://www.cigionline.org/publications/standards-digital-cooperation/.

Global Data Alliance (2020). Cross-Border Data Transfers and Data Localization. Global Data Alliance, Washington, DC. Available at: https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf.

Gökçe Dessemond E (2020). Restoring competition in "winner-took-all" digital platform markets. UNCTAD Research Paper, No. 40. UNCTAD/SER.RP/2019/12. UNCTAD, Geneva.

Gong S, Gu J and Teng F (2019). The Impact of the Belt and Road Initiative Investment in Digital Connectivity and Information and Communication Technologies on Achieving the SDGs. K4D Emerging Issues Report. Institute of Development Studies, Brighton. Available at: https://assets.publishing.service.gov.uk/media/5c86628940f0b6369b76a372/K4D_Emerging_Issues_-_BRI_Investment_Part_A_-_final.pdf.

Gonzalez-Zapata F and Heeks R (2015). The Multiple Meanings of Open Government Data: Understanding Different Stakeholders and Their Perspectives. *Government Information Quarterly*, 32(4): 441–452.

Google (2010). Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information. White paper. Google, Mountain View, CA. Available at: https://static.googleusercontent.com/media/www.google.com/fr//googleblogs/pdfs/trade_free_flow_of_information.pdf.

Government Office for Science (2020). Evidence and Scenarios for Global Data Systems. The Future of Citizen Data Systems. Government of the United Kingdom of Great Britain and Northern Ireland. Available at: https://www.gov.uk/government/publications/the-future-of-citizen-data-systems.

Graham M, Hjorth I and Lehdonvirta V (2017). Digital Labour and Development: Impacts of Global Digital Labour Platforms and the Gig Economy on Worker Livelihoods. *Transfer: European Review of Labour and Research*, 23(2): 135–162.

Gray ML and Suri S (2019). *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. Houghton Mifflin Harcourt, Boston, MA.

Greze B (2019). The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives. *International Data Privacy Law*, 9(2): 109–128.

GSMA (2017). The Mobile Economy 2017. Global System for Mobile Communications Association, London, February.

GSMA (2018a). Cross-Border Data Flows: Realising benefits and removing barriers. Global System for Mobile Communications Association, London, September.

GSMA (2018b). Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation. Global System for Mobile Communications Association, London, September.

GSMA (2018c). The Data Value Chain. Global System for Mobile Communications Association, London, June.

GSMA (2019a). The GSMA Guide to the Internet of Things. Global System for Mobile Communications Association, London, July.

GSMA (2019b). The contribution of IoT to economic growth: Modelling the impact on business productivity. GSMA Intelligence, Global System for Mobile Communications Association, London, April.

GSMA (2019c). The Impact of Data Localisation Requirements on the Growth of Mobile Money-enabled Remittances. Global System for Mobile Communications Association, London, March.

GSMA (2020a). The Mobile Economy 2020. Global System for Mobile Communications Association, London, March.

GSMA (2020b). The State of Mobile Internet Connectivity Report 2020. Global System for Mobile Communications Association, London, September.

GSMA (2020c). Artificial Intelligence and Start-Ups in Low- and Middle-Income Countries: Progress, Promises and Perils. Global System for Mobile Communications Association, London, October.

GSMA (2021). Cross-Border Data Flows: The impact of data localisation on IoT. Global System for Mobile Communications Association, London, January.

Gupta S, Gupta K, Ghosh P and Paul SK (2020). Data Localisation: India's Double Edged Sword? Consumer Unity & Trust Society (CUTS) International, Jaipur. Available at: https://ssrn.com/abstract=3665197.

Gurumurthy A and Chami N (2019). Digital Public Goods. A Precondition for Realising the SDGs. *Global Governance Spotlight*: 4, the Development and Peace Foundation, Bonn. Available at: https://www.sef-bonn.org/fileadmin/SEF-Dateiliste/04_Publikationen/GG-Spotlight/2019/ggs_2019-04_en.pdf.

Gurumurthy A and Chami N (2020). The intelligent corporation. Data and the digital economy. In: Buxton N, ed., *State of Power 2020: The Corporation*, Transnational Institute: 10–20.

Gurumurthy A, Vasudevan A and Chami N (2017). The grand myth of cross-border data flows in trade deals. IT for Change, Bangalore, December. Available at: https://itforchange.net/sites/default/files/1470/dataflow-11am.pdf.

Haskel J and Westlake S (2017). *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton University Press, Princeton, NJ.

Heeks R and Renken J (2018). Data Justice for Development: What Would It Mean? *Information Development*, 34(1): 90–102.

Heeks R, Rakesh V, Sengupta R, Chattapadhyay S and Foster C (2021). Datafication, Value and Power in Developing Countries: Big Data in Two Indian Public Service Organizations. *Development Policy Review*, 39(1): 82–102.

Hesselman C et al. (2020). A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management*, 28(4): 882–992.

Heverly RA (2003). The Information Semicommons. *Berkeley Technology Law Journal*, 18(4): 1127–1190.

Hilbig S (2018). Handelsrecht – freie Fahrt auf der Datenautobahn. Brot für die Welt, 6 November. Available at: https://www.brot-fuer-die-welt.de/blog/2018-handelsrecht-freie-fahrt-auf-der-datenautobahn/.

Hill JF (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. *Lawfare Research Paper Series*, 2(3): 1–41.

Hill R (2018). Why should data flow freely? Association for Proper Internet Governance (APIG), March. Available at: http://www.apig.ch/Forum%202018%20Policy%20statement.pdf.

Hill R (2020). A New Convention for Data and Cyberspace. In: Sarkar S and Korjan A, eds., *A Digital New Deal: Visions of Justice in a Post-Covid World,* Just Net Coalition and IT for Change: 180–200.

Hinrich Foundation (2019). The Data Revolution: Capturing the Digital Trade Opportunity at Home and Abroad. Hinrich Foundation, 4 February. Available at: https://www.hinrichfoundation.com/research/project/digital-trade-research-project/.

Hoffmann S, Lazanski D and Taylor E (2020). Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy*, 5(2): 239–264.

Huang T and Arnold Z (2020). Immigration Policy and the Global Competition for AI Talent. Center for Security and Emerging Technology, Georgetown University, Washington, DC, June. Available at: https://cset.georgetown.edu/publication/immigration-policy-and-the-global-competition-for-ai-talent/.

Hummel P, Braun M, Tretter M and Dabrock P (2021). Data sovereignty: A review. *Big Data & Society*, 8(1): 1–17.

Hunt SD and Morgan RM (1995). The Comparative Advantage Theory of Competition. *Journal of Marketing*, 59(2): 1–15.

Hurst D (2019). Japan Calls for Global Consensus on Data Governance. *The Diplomat*, 2 February. Available at: https://thediplomat.com/2019/02/japan-calls-for-global-consensus-on-data-governance/.

Iazzolino G and Mann L (2019). Harvesting Data: Who Benefits from Platformization of Agricultural Finance in Kenya? *Developing Economics*, 29 March. Available at: https://developingeconomics.org/2019/03/29/harvesting-data-who-benefits-from-platformization-of-agricultural-finance-in-kenya/.

Ichilevici de Oliveira A, Heseleva K and Ramos VJ (2020). Towards a Multilateral Consensus on Data Governance. Policy Brief, Global Solutions Initiative Foundation, Berlin, 20 May. Available at: https://www.global-solutions-initiative.org/wp-content/uploads/2020/05/Towards-a-Multilateral-Consensus-for-Data-Governance_Ramos_deOliveira_Heseleva.pdf.

IDC (2020a). Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide. International Data Corporation, Needham, MA, 18 June. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS46609320.

IDC (2020b). IoT Growth Demands Rethink of Long-Term Storage Strategies. IDC Media Center, International Data Corporation, Singapore, 28 July. Available at: https://www.idc.com/getdoc.jsp?containerId=prAP46737220.

IDC (2021a). Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts. International Data Corporation, Needham, MA, 24 March. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS47560321.

IDC (2021b). The Role of Satellite as an Augmented Connectivity. Market Perspective - Doc # AP45983020. International Data Corporation, Needham, MA, February. Available at: https://www.idc.com/getdoc.jsp?containerId=AP45983020.

IDC and OpenEvidence (2017). European Data Market, Final Report. SMART 2013/0063. European Commission, Brussels, 1 February. Available at: https://datalandscape.eu/study-reports.

IEA (2020). Data Centres and Data Transmission Networks. Tracking Report. International Energy Agency, Paris. Available at: https://www.iea.org/reports/data-centres-and-data-transmission-networks.

Imbrie A, Fedasiuk R, Aiken C, Chhabra T and Chahal H (2020). Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI. Center for Security and Emerging Technology, Georgetown University's Walsh School of Foreign Service, Washington DC, February. Available at: https://cset.georgetown.edu/publication/agile-alliances/.

International Chamber of Commerce (2021). Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce. International Chamber of Commerce (ICC), Paris, 26 January. Available at: https://iccwbo.org/content/uploads/sites/3/2021/01/multi-industry-statement-on-crossborder-data-transfers-and-data-localization.pdf.

Internet Society (2015). Policy Brief: Internet Exchange Points (IXPs). Internet Society, 30 October. Available at: https://www.internetsociety.org/policybriefs/ixps/.

Internet Society (2020a). White Paper: Considerations for Mandating Open Interfaces. Internet Society, 4 December. Available at: https://www.internetsociety.org/wp-content/uploads/2020/12/ConsiderationsMandatingOpenInterfaces-03122020-EN.pdf.

Internet Society (2020b). Discussion Paper: An analysis of the "New IP" proposal to the ITU-T. Internet Society, 24 April. Available at: https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

Internet Society (2020c). Internet Way of Networking Use Case: Data Localization. Internet Society, September. Available at: https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-Use-Case-Data-Localization-EN.pdf.

Ismail Y (2020). E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint Statement. International Institute for International Development (IISD), Winnipeg, 31 January. Available at: https://www.iisd.org/publications/e-commerce-world-trade-organization-history-and-latest-developments-negotiations-under.

ITIF (2019). Submarine Cables: Critical Infrastructure for Global Communications. Information Technology and Innovation Foundation, April. Available at: http://www2.itif.org/2019-submarine-cables.pdf.

ITU (2018). Powering the Digital Economy: Regulatory Approaches to Securing Consumer Privacy, Trust and Security. International Telecommunication Union, Geneva. Licence: CC BY-NC-SA 3.0 IGO. Available at: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.POW_ECO-2018-PDF-E.pdf.

ITU (2020). *Measuring digital development, Facts and figures 2020*. International Telecommunication Union, Geneva. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

ITU and UNESCO (2020). *State of Broadband Report 2020: Tackling digital inequalities – A decade for action*. Geneva: International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, 2020. License: CC BY-NC-SA 3.0 IGO. Available at: http://handle.itu.int/11.1002/pub/8165dc3c-en.

Jain S and Gabor D (2020). The Rise of Digital Financialisation: The Case of India. *New Political Economy*, 25(5): 813–28.

James D (2020). Digital Trade Rules: A disastrous new constitution for the global economy written by and for Big Tech. Rosa-Luxemburg-Stiftung, Brussels. Available at: https://cepr.net/wp-content/uploads/2020/07/digital-trade-2020-07.pdf.

Janow ME and Mavroidis PC (2019). Digital trade, e-commerce, the WTO and regional frameworks. *World Trade Review*, 18(S1), S1–S7.

Jha S and Germann S (2020). How can we make health data a global public good? MMS Bulletin 148, Medicus Mundi Schweiz, Basel and Geneva. Available at: https://www.medicusmundi.ch/de/advocacy/publikationen/mms-bulletin/digital-health-fluch-oder-segen-fuer-die-globale-gesundheit/neue-herausforderungen-durch-kuenstliche-intelligenz/how-can-we-make-health-data-a-global-public-good.

Jurowetzki R, Hain DS, Mateos-Garcia J and Stathoulopoulos K (2021). The Privatization of AI Research(-ers): Causes and Potential Consequences. From university-industry interaction to public research brain-drain? Cornell University, Ithaca, NY, 15 February. Available at: https://arxiv.org/abs/2102.01648.

Kanth DR (2019). India boycotts 'Osaka Track' at G20 summit. *Mint*, 30 June. Available at: https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html.

Kathuria R, Kedia M, Varma G and Bagchi K (2019). Economic Implications of Cross-Border Data Flows. Internet and Mobile Association of India, November. Available at: http://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.

Kavacs A and Ranganathan N (2019). Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India. Data Governance Network Working Paper, No. 3, November.

Kawalek P and Bayat A (2017). Data As Infrastructure. National Infrastructure Commission, 14 December. Available at: https://aura.abdn.ac.uk/handle/2164/11906.

Kelsey J (2018). How a TPP-Style E-Commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO). *Journal of International Economic Law*, 21(2): 273–295.

Kesan JP, Hayes CM and Bashir MN (2016). A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy. *Indiana Law Journal*, 91(2): 267–352.

Kilic B and Avila R (2019). Cross border data flows, privacy, and global inequality. Public Citizen, Washington, DC. Available at: https://www.citizen.org/article/crossborder-data-flows-privacy/.

Kimura F (2020). Developing a policy regime to support the free flow of data: A proposal by the T20 Task Force on Trade, Investment and Globalization. VoxEU.org, 7 January. Available at https://voxeu.org/article/developing-policy-regime-support-free-flow-data.

Kitchin R and McArdle G (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. *Big Data & Society*.

Komaitis K (2017). The 'Wicked Problem' of Data Localisation. *Journal of Cyber Policy*, 2(3): 355–365.

Krotova A and Eppelsheimer J (2019). Data governance in der wissenschaftlichen Literatur: Eine Begriffsklärung anhand einer Text-Mining-basierten Literaturrecherche. *IW-Trends-Vierteljahresschrift zur empirischen Wirtschaftsforschung*, 46(3): 55–71, Institut der deutschen Wirtschaft (IW), Köln. Available at: http://hdl.handle.net/10419/209531.

Kukutai T and Taylor J (2016). Data Sovereignty for Indigenous Peoples: Current Practice and Future Needs. In: Kukutai T and Taylor J, eds. *Indigenous Data Sovereignty: Toward an Agenda*, ANU Press, The Australian National University, Canberra: 1–22.

Kuner C (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD Digital Economy Papers*, No. 187. OECD Publishing, Paris.

Kuner C (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press, Oxford.

Kurbalija J and Höne K (2021). 2021: The emergence of digital foreign policy. DiploFoundation, Geneva. Available at: https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_foreign_policy.pdf.

Kurlantzick J (2020). China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom? *The Diplomat*, 17 December. Available at: https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/.

Kwet M (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4): 3-26.

Leblond P (2020). Digital Trade: Is RCEP the WTO's Future? Center for International Governance Innovation, Waterloo, ON, 23 November. Available at: https://www.cigionline.org/articles/digital-trade-rcep-wtos-future.

Leblond P and Aaronson SA (2019). A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma. CIGI Papers Series, No. 226. Centre for International Governance Innovation, Waterloo, ON.

Lee JA (2018). Hacking into Chinese Cybersecurity Law. *Wake Forest Law Review*, 53(1): 57–104.

Leviathan Security Group (2015). Quantifying the Cost of Forced Localization. Leviathan Security Group, Seattle, WA. Available at: https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

Lewis D (2020). Why many countries failed at COVID contact-tracing — but some got it right. *Nature*, 588:384–388.

Linden O and Dahlberg E (2016). Data flows – a fifth freedom for the internal market? Kommerskollegium (National Board of Trade Sweden), Stockholm. Available at: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016/publ-data-flows.pdf.

Liu J (2020). China's Data Localization. *Chinese Journal of Communications*, 13(1): 84–103.

Liu L (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, 56: 45–67. Available at: https://link.springer.com/article/10.1007/s12116-021-09319-8.

Lowry A (2020). Russia's Digital Economy Program: An Effective Strategy for Digital Transformation? In: Gritsenko D, Wijermars M and Kopotev M, eds., *The Palgrave Handbook of Digital Russia* Studies, Palgrave Macmillan: 53–76.

Ly B (2020). Challenge and perspective for Digital Silk Road. *Cogent Business & Management*, 7(1): 1804180.

MacFeely S (2020a). In search of the data revolution: Has the official statistics paradigm shifted? *Statistical Journal of the IAOS*, 36(4): 1075–1094.

MacFeely S (2020b). A Global Data Convention? UN World Data Forum, 23 October. Available at https://theunbrief.com/2020/10/23/a-global-data-convention/.

Malcolm J (2016). TISA Proposes New Global Rules on Data Flows and Safe Harbors. The Electronic Frontier Foundation, 24 October. Available at: https://www.eff.org/deeplinks/2016/10/tisa-proposes-new-global-rules-data-flows-and-safe-harbors.

Malik F, Nicholson B and Morgan S (2016). Assessing the Social Development Potential of Impact Sourcing. In: Nicholson B, Babin R and Lacity MC, eds., *Socially Responsible Outsourcing: Global Sourcing with Social Impact, Technology, Work and Globalization.* Palgrave Macmillan UK, London: 97–118.

Maréchal N (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communications*, 5(1): 29–41.

Martin N, Matt C, Niebel C and Blind K (2019). How Data Protection Regulation Affects Startup Innovation. *Information Systems Frontiers*, 21: 1307–1324.

Mattoo A and Meltzer JP (2018). International Data Flows and Privacy: The Conflict and Its Resolution. *Journal of International Economic Law*, 21(4): 769–789.

Mayer J (2020). Development strategies for middle-income countries in a digital world – impacts from trade costs, data and innovation policies. TMCD Working paper series No. TMD-WP-80, Technology and Management Centre for Development (TMCD), Oxford Department of International Development, University of Oxford. Available at: https://www.oxfordtmcd.org/publication/development-strategies-middle-income-countries-digital-world-impacts-trade-costs-data.

Mayer-Schönberger V and Cukier K (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, Boston.

Mazzucato M (2018). Let's make private data into a public good. *MIT Technology Review*, Massachusetts Institute of Technology, Cambridge, MA, 27 June. Available at: https://www.technologyreview.com/2018/06/27/141776/lets-make-private-data-into-a-public-good/.

Mazzucato M, Entsminger J and Kattel R (2020). Public value and platform governance. UCL Institute for Innovation and Public Purpose, Working Paper Series IPP WP 2020-11, University College London, London.

McKinsey (2014). Global flows in a digital age: How trade, finance, people, and data connect the world economy. McKinsey Global Institute, April.

McKinsey (2016). Digital Globalization: The New Era of Global Flows. McKinsey Global Institute, March.

McKinsey (2019). Globalization in transition: The future of trade and value chains. McKinsey Global Institute, January.

McLaughlin M and Castro D (2019). The Case for a Mostly Open Internet. Information Technology and Innovation Foundation, Washington, DC, 16 December.

Medhora RP and Owen T (2020). A Post-COVID-19 Digital Bretton Woods. Available at https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/.

Meltzer JP (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia and the Pacific Policy Studies*, 2(1): 90–102.

Meltzer JP (2018). A Digital Trade Policy for Latin America and the Caribbean. Technical Note, No. IDB-TN-1483, Inter-American Development Bank, Washington, DC.

Meltzer JP (2019). Governing Digital Trade. *World Trade Review*, 18(S1), S23–S48.

Meltzer JP (2020). The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security. VoxEU.org, 5 August. Available at: https://voxeu.org/article/impact-gdpr-data-flows-and-national-security.

Micheli M, Ponti M, Craglia M and Berti Suman A (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2): 1–15.

Microsoft (2018). A Cloud for Global Good: A policy road map for a trusted, responsible and inclusive cloud – The 2018 Update. Microsoft. Available at: https://news.microsoft.com/cloudforgood/_media/downloads/a-cloud-for-global-good-2018-english.pdf.

MIKTA (2016). MIKTA E-commerce Workshop Reflections. Mexico, Indonesia, the Republic of Korea, Turkey and Australia (MIKTA). The Ministry of Foreign Affairs MIKTA, 8 August. Available at: http://www.mikta.org/document/others.php?at=view&idx=235&ckattempt=1.

Mishra N (2019). Building Bridges: International Trade Law, Internet Governance and the Regulation of Data Flows. *Vanderbilt Journal of Transnational Law*, 52(2): 463–509.

Mishra N (2020a). The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance. *Journal of World Trade*. 54(4): 567–90.

Mishra N (2020b). Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review*, 19(3): 341–64.

Mitchell AD and Hepburn J (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *Yale Journal of Law and Technology*, 19(1): 182–237.

Mitchell AD and Mishra N (2019). Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. *Journal of International Economic Law*, 22(3): 389–416.

Monteiro J-A and Teh R (2017). Provisions on Electronic Commerce in Regional Trade Agreements. WTO Working Paper, No. ERSD-2017-11, Economic Research and Statistics Division, World Trade Organization, Geneva, July.

Moorthy V, Henao Restrepo AM, Preziosi M-P and Swaminathan S (2020). Data Sharing for Novel Coronavirus (COVID-19). *Bulletin of the World Health Organization*, 98(3): 150.

Morgan Stanley (2020). Space: Investing in the Final Frontier. Research, Morgan Stanley, New York, NY, 24 July. Available at: https://www.morganstanley.com/ideas/investing-in-space.

Morozov E (2017). Digital intermediation of everything: at the intersection of politics, technology and finance. 4th Council of Europe Platform Exchange on Culture and Digitisation, Council of Europe, "Empowering Democracy through Culture – Digital Tools for Culturally Competent Citizens", ZKM Center for Art and Media, Karlsruhe, 19–20 October. Available at: https://rm.coe.int/digital-intermediation-of-everything-at-the-intersection-of-politics-t/168075baba.

Mosoti V (2006). Africa in the first decade of WTO dispute settlement. *Journal of International Economic Law*, 9(2): 427–453.

Mozilla Insights, van Geuns J and Brandusescu A (2020). Shifting Power Through Data Governance. Mozilla, 16 September. Available at: https://foundation.mozilla.org/en/data-futures-lab/data-for-empowerment/shifting-power-through-data-governance/.

Mueller M (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Polity Press, Cambridge, CB2 and Malden, MA.

National Telecommunications and Information Administration (2016). Measuring the Value of Cross-Border Data Flows. United States Department of Commerce, Washington, DC, 30 September. Available at: https://www.ntia.gov/report/2016/measuring-value-cross-border-data-flows.

NewVantage Partners (2021). Big Data and AI Executive Survey 2021 Executive Summary of Findings: The Journey to Becoming Data-Driven: A Progress Report on the State of Corporate Data Initiatives. Available at https://c6abb8db-514c-4f5b-b5a1-fc710f1e464e.filesusr.com/ugd/e5361a_76709448ddc6490981f0cbea42d51508.pdf.

Nguyen D and Paczos M (2020). Measuring the economic value of data and cross-border data flows: A business perspective. *OECD Digital Economy Papers*, No. 297, OECD Publishing, Paris.

Nicholson JR and Noonan R (2017). Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services. *Current Politics and Economics of the United States, Canada and Mexico*, 19(1): 53–83.

Noble SU (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, New York, NY.

Nocetti J (2015). Contest and Conquest: Russia and Global Internet Governance. *International Affairs*, 91(1): 111–130.

Nussipov A (2020a). How China Governs Data, Center for Media, Data and Society, The CMDS Blog, 27 April, available at https://medium.com/center-for-media-data-and-society/how-china-governs-data-ff71139b68d2.

Nussipov A (2020b). How Data Became a Trade Issue. The CMDS Blog, Centre for Media, Data and Society, Medium, 16 April. Available at https://medium.com/center-for-media-data-and-society/how-data-became-a-trade-issue-e4676eb048e8.

NVTC (2020). The Impact of Data Centers on the State and Local Economies of Virginia. North Virginia Technology Council, Richmond, VA. Available at: http://biz.loudoun.gov/wp-content/uploads/2020/02/Data_Center_Report_2020.pdf.

Nyokabi DM, Diallo N, Ntesang NW, White TK and Ilori T (2019). The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa. *Global Campus Human Rights Journal*, 3(2): 147–172.

O'Hara K (2019). Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship. Web Science Institute White Papers 1, University of Southampton, Southampton.

OECD (2007). OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. OECD, Paris.

OECD (2013a). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, No. 220, OECD Publishing, Paris.

OECD (2013b). Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines. *OECD Digital Economy Papers*, No. 229. OECD Publishing, Paris.

OECD (2014). OECD Principles for Internet Policy Making. OECD, Paris.

OECD (2015). Data-Driven Innovation: Big Data for Growth and Well-Being. OECD Publishing, Paris.

OECD (2019a). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. OECD Publishing, Paris.

OECD (2019b). Unlocking the potential of e-commerce, OECD Going Digital Policy Note, OECD, Paris.

OECD (2019c). State of Play in the Governance of Critical Infrastructure Resilience. In: *Good Governance for Critical Infrastructure Resilience*, OECD Publishing, Paris: 45–82.

OECD (2020). Mapping Approaches to Data and Data Flows. Report for the G20 Digital Economy Task Force, Saudi Arabia. OECD, Paris.

OECD (2021). OECD Secretary-General Tax Report to G20 Finance Ministers and Central Bank Governors – April 2021. OECD, Paris.

OECD and WTO (2017). *Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development*. WTO and OECD publishing. Geneva and Paris.

OECD, WTO, and IMF (2020). Handbook on Measuring Digital Trade, Version 1. OECD, Paris. Available at: https://www.oecd.org/sdd/its/handbook-on-measuring-digital-trade.htm.

OHCHR (2020). Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights. A/HRC/43/29. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General. Human Rights Council, forty-third Session, 24 February–20 March.

Ohm P (2010). Broken Promises of Privacy: Responding to the Surprising Failures of Anonymization. *UCLA Law Review*, 57(6): 1701–1777.

Open Data Institute (2019a). Data Trusts: Lessons from Three Pilots. Open Data Institute, London, 15 April. Available at: https://theodi.org/article/odi-data-trusts-report/.

Open Data Institute (2019b). What are the Links Between Data Infrastructure and Trade Competitiveness? Open Data Institute, London, 3 July. Available at: https://theodi.org/article/what-are-the-links-between-data-infrastructure-and-trade-competitiveness/.

Open Rights Group (2014). TTIP's threat to our privacy and culture. London, 14 October. Available at: https://www.openrightsgroup.org/blog/ttips-threat-to-our-privacy-and-culture/.

Organ J (2017). EU citizen participation, openness and the European Citizens Initiative: the TTIP legacy. *Common Market Law Review*, 54(6): 1713–1747.

Our World is Not for Sale (2019). Civil Society Letter Against Digital Trade Rules in the World Trade Organization (WTO). 1 April. Available at: http://www.ourworldisnotforsale.net/2019/Digital_trade_2019-04-01-en.pdf.

Pamment J (2019). Accountability as Strategic Transparency: Making Sense of Organizational Responses to the International Aid Transparency Initiative. *Development Policy Review*, 37(5): 657–671.

Panday J (2017). Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms. Electronic Frontier Foundation, 14 August. Available at: https://www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms.

PDPC (2018). Guide to Basic Data Anonymisation Techniques. Personal Data Protection Commission, Singapore, 25 January. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

Pew Research Center (2019). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. Pew Research Center, Washington, DC, 5 February. Available at: https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.

Pisa M, Dixon P, Ndulu B and Nwankwo U (2020). Governing Data for Development: Trends, Challenges, and Opportunities. CGD Policy Paper, No. 190, Center for Global Development, Washington, DC.

Pisa M and Polcari J (2019). *Governing Big Tech's Pursuit of the "Next Billion Users"*. Harvard University Press, Cambridge, MA.

Pohle J, Gorwa R and Miller H (2020). The turn to trade agreements in global platform governance. AoIR Selected Papers of Internet Research, Association of Internet Researchers, Annual Conference, Virtual Event, 27–31 October 2020. Available at: https://doi.org/10.5210/spir.v2020i0.11305.

Pohle J and Thiel T (2020). Digital sovereignty. *Internet Policy Review*, 9(4). Available at: https://doi.org/10.14763/2020.4.1532.

Potluri SR, Sridhar V and Rao S (2020). Effects of Data Localization on Digital Trade: An Agent-based Modelling Approach. *Telecommunications Policy*, 44(9): 102022.

Quismorio BA (2019). Capability building for data analytics and artificial intelligence. Presentation at the Third Session of the Intergovernmental Group of Experts on E-commerce and the Digital Economy. Available at: https://unctad.org/system/files/non-official-document/tdb_ede3_2019_p11_BQuismorio_en.pdf.

Raghavan C (2018). Development and free data flow rules are incompatible. *Third World Economics: Trends and Analysis*, 678/679: 6–7. Third World Network (TWN), Penang.

Rentzhog M and Jonströmer H (2014). No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden. Kommerskollegium (National Board of Trade Sweden), Stockholm. Available at: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no_transfer_no_trade_webb.pdf.

Rikap C (2021). Intellectual monopoly capitalism and its effects on development. *Developing Economics*, 7 April. Available at: https://developingeconomics.org/2021/04/07/intellectual-monopoly-capitalism-and-its-effects-on-development/.

Roberts A, Moraes HC and Ferguson V (2019). Toward a Geoeconomic Order in International Trade and Investment. *Journal of International Economic Law*, 22(4): 655–76.

Rodriguez K and Alimonti V (2020). A Look-Back and Ahead on Data Protection in Latin America and Spain. Electronic Frontier Foundation, 21 September. Available at: https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

Rodrik D (2020). The Coming Global Technology Fracture. Project Syndicate, 8 September. Available at: https://www.project-syndicate.org/commentary/making-global-trade-rules-fit-for-technology-by-dani-rodrik-2020-09.

The Royal Society (2021). Data for international health emergencies: governance, operations and skills. Statement by the Science Academies of the G7 nations, March. Available at: https://www.interacademies.org/publication/data-international-health-emergencies-governance-operations-and-skills.

Rühlig TN (2020). Technical standardisation, China and the future international order – A European perspective. E-Paper, Heinrich-Böll-Stiftung European Union, Brussels. Available at: https://eu.boell.org/en/2020/03/03/technical-standardisation-china-and-future-international-order.

Sacks S and Sherman J (2019). Global Data Governance: Concepts, Obstacles, and Prospects. New America, Washington, DC. Available at: https://www.newamerica.org/cybersecurity-initiative/reports/global-data-governance/.

Sadowski J (2019). When Data Is Capital: Datafication, Accumulation, and Extraction. *Big Data and Society*, 6(1): 1–12.

Sandvine (2020). *The Global Internet, Phenomena Report, COVID-19 Spotlight*. Sandvine, May. Available at: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf.

Sargsyan T (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. *International Journal of Communication*, 10: 2221–2237.

Savelyev A (2016). Russia's New Personal Data Localisation Requirements: A Step-Forward or a Self-Imposed Sanction? *Computer Law and Security Review*, 32(1): 128–145.

Scassa T (2018). Data Ownership. CIGI papers, No. 187, Center for International Governance Innovation, Waterloo, ON.

Schneider I (2019). Models for the governance of data economics. Presentation at "Who Governs the Data Economy?" session at MyData Conference, Helsinki, 26 September. Available at: https://attachment.rrz.uni-hamburg.de/f89c3ccd/Helsinki-MyData-Schneider-Data-Governance-26092019.pdf.

Selby J (2017). Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology*, 25(3): 213–232.

Sell SK (2009). Cat and mouse: Forum-shifting in the battle over intellectual property enforcement. Draft prepared for the American Political Science Association Meeting, 3–6 September. Available at: https://ipgovernance.eu/conferences/2009APSAToronto/Sell_APSA2009_Cat_and_Mouse.pdf.

Shadlen K (2008). Globalisation, Power and Integration: The Political Economy of Regional and Bilateral Trade Agreements in the Americas. *Journal of Development Studies*, 44(1): 1–20.

Sherman J and Morgus R (2018). The Digital Deciders and the Future of the Internet. New America, Washington, DC, 2 December. Available at: https://www.newamerica.org/cybersecurity-initiative/in-the-news/digital-deciders-and-future-internet/.

The Shift Project (2019). Lean ICT: Towards Digital Sobriety. The Shift Project, Paris, March. Available at: https://theshiftproject.org/wp-content/uploads/2019/03/Lean-ICT-Report_The-Shift-Project_2019.pdf.

Singh PJ (2018a). Digital Industrialisation in Developing Countries – A Review of the Business and Policy Landscape. Research Paper for the Commonwealth Secretariat, IT for Change, Bangalore, January.

Singh PJ (2018b). Data Localisation: A Matter of Rule of Law and Economic Development. Policy Brief, IT For Change, Bangalore, September.

Singh PJ (2019). India Should Aim for a Digital Non-Alignment. IT for Change, Bangalore, July.

Singh PJ and Vipra J (2019). Economic Rights Over Data: A Framework for Community Data Ownership. *Development*, 62: 53–57.

Sinha A and Basu A (2019). The Politics of India's Data Protection Ecosystem. *Economic & Political Weekly*, 54(49).

Slaughter MJ and McCormick DH (2021). Data Is Power. *Foreign Affairs*, May/June 2021.

Spiezia V and Tscheke J (2020). International agreements on cross-border data flows and international trade: A statistical analysis. *OECD Science, Technology and Industry Working Papers*, No. 2020/09, OECD, Paris.

Srikrishna Committee Report (2018). Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Ministry of Electronics and Information Technology, Government of India. Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Srnicek N (2016). *Platform Capitalism*. Polity Press, Cambridge, United Kingdom.

Statista (2021). Amazon Leads $130-Billion Cloud Market. 4 February. Available at: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

Statistics Canada (2019). Measuring investment in data, databases and data science: Conceptual framework. Catalogue No. 13-605-X, 24 June. Available at: https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00008-eng.htm.

Steinberg RH (2002). In the shadow of law or power? Consensus-based bargaining and outcomes in the GATT/WTO. *International Organization*, 56(2): 339–374.

Stiglitz JE (2012). *The Price of Inequality: How Today's Divided Society Endangers Our Future*. W.W. Norton and Company, New York, NY.

Streinz T (2021). RCEP's Contribution to Global Data Governance. *Afronomicslaw*, 19 February. Available at: https://www.afronomicslaw.org/category/analysis/rceps-contribution-global-data-governance-0.

Suominen K (2018). Fueling Digital Trade in Mercosur: A Regulatory Roadmap. Technical note, No. IDB-TN-01549, Inter-American Development Bank, Washington, DC, October.

Suranovic SM (2002). International labour and environmental standards agreements: Is this fair trade? *World Economy*, 25(2), 231–245.

Synergy Research Group (2021a). Microsoft, Amazon and Google Account for Over Half of Today's 600 Hyperscale Data Centers. Synergy Research Group, Reno, NV, 26 January. Available at: https://www.srgresearch.com/articles/microsoft-amazon-and-google-account-for-over-half-of-todays-600-hyperscale-data-centers.

Synergy Research Group (2021b). Cloud Market Ends 2020 on a High while Microsoft Continues to Gain Ground on Amazon. Synergy Research Group, Reno, NV, 2 February. Available at: https://www.srgresearch.com/articles/cloud-market-ends-2020-high-while-microsoft-continues-gain-ground-amazon.

Tang C (2021). *Data Capital. How Data is Reinventing Capital for Globalization*. Springer International Publishing. Available at: https://www.springer.com/gp/book/9783030601911.

Taylor RD (2020). "Data localization": The internet in the balance. *Telecommunications Policy,* 44(8): 102003.

TeleGeography (2015). International Bandwidth Trends in Africa. What Has (and Hasn't) Changed in the Past Five Years, 27 August. Available at: http://isoc-ny.org/afpif2015/AfPIF2015_Teleography.pdf.

TeleGeography (2019). Back to the Future. Presentation by Alan Mauldin, TeleGeography Workshop at Pacific Telecommunications Council (PTC), 20 January. Available at: https://www2.telegeography.com/hubfs/2019/Presentations/TeleGeo-PTC2019.pdf.

TeleGeography (2021a). *The State of the Network: 2021 Edition*. TeleGeography, San Diego, CA. Available at: https://www2.telegeography.com/hubfs/assets/Ebooks/state-of-the-network-2021.pdf.

TeleGeography (2021b). Exploring the Cloud, Overland and Undersea. Trends in Cloud Infrastructure and Global Networks, 17 Februrary. Available at: https://www2.telegeography.com/hubfs/2021/Presentations/2021%20Cloud%20Trends.pdf.

Tomiura E, Ito B and Kang B (2019). Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms. *RIETI Discussion Paper Series*, No. 9-E-088. Research Institute of Economy, Trade and Industry (RIETI), Tokyo. Available at: https://www.rieti.go.jp/jp/publications/dp/19e088.pdf.

Trade Justice Movement (2020). Digital trade (e-commerce). Trade Justice Movement, London. Available at: https://www.tjm.org.uk/trade-issues/digital-trade-e-commerce.

Triolo P, Allison K and Brown C (2020). The Digital Silk Road: Expanding China's digital footprint. Eurasia Group, New York, NY, 29 April. Available at: https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint.

UNCITRAL (2020). Legal issues related to the digital economy – data transactions. United Nations Commission on International Trade Law, Fifty-third session. A/CN.9/1012/Add.2. Available at: https://undocs.org/en/A/CN.9/1012/Add.2.

UNCTAD (2016). *Data protection regulations and international data flows: Implications for trade and development.* United Nations publication, UNCTAD/WEB/DTL/STICT/2016/1/iPub. New York and Geneva.

UNCTAD (2017). *Information Economy Report 2017: Digitalization, Trade and Development*. United Nations publication, Sales No. E.17.II.D.8. New York and Geneva.

UNCTAD (2019a). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. United Nations publication, Sales No. E.19.II.D.17. New York and Geneva.

UNCTAD (2019b). Competition issues in the digital economy. Note by the UNCTAD secretariat. TD/B/C.I/CLP/54. Trade and Development Board, Intergovernmental Group of Experts on Competition Law and Policy, Eighteenth session, Geneva, 10–12 July.

UNCTAD (2021a). *COVID-19 and E-commerce: a Global Review*. United Nations publication, Sales No. E.21.II.D.9. Geneva.

UNCTAD (2021b). *What is at stake for developing countries in trade negotiations? – The case of joint statement initiative*. United Nations publication, UNCTAD/DITC/TNCD/2020/5. Geneva.

UNCTAD (2021c). *The UNCTAD B2C E-commerce Index 2020: Spotlight on Latin America and the Caribbean.* UNCTAD Technical Notes on ICT for Development, No. 17. Geneva.

UNCTAD (2021d). *Technology and Innovation Report 2021: Catching technological waves: Innovation with equity*. United Nations publication, sales No. E.21.II.D.8. New York and Geneva.

UNCTAD (2021e). E-Commerce and Digital Economy Programme: Year in Review 2030: Facilitating inclusive digital economies in challenging times. Available at https://unctad.org/system/files/official-document/dtlstictinf2021d2_en.pdf.

UNDP (2020). Data Philanthropy, International Organizations and Development Policy: Ethical Issues to Consider. Discussion Paper, United Nations Development Programme, New York, April.

UNEP (2020). UNEP's contribution to Round Table 1B on Digital Public Goods. Environmental data as digital public goods within a digital ecosystem for the planet. United Nations Environment Programme, Nairobi.

UNESCO (2020). Outcome document: first draft of the recommendation on the ethics of artificial intelligence. Document code: SHS/BIO/AHEG-AI/2020/4 REV.2. Ad Hoc Expert Group for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, Paris, 7 September.

United Nations (2019). The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation, New York.

United Nations (2020a). Roadmap for Digital Cooperation. Report of the Secretary-General. New York.

United Nations (2020b). Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020–22. New York.

United Nations (2020c). The Highest Aspiration – A Call to Action for Human Rights. New York.

United Nations (2021). Tax consequences of the digitalized economy – issues of relevance for developing countries. E/C.18/2021/CRP.1. Co-Coordinators' Report, Committee of Experts on International Cooperation in Tax Matters, twenty-second session, 19–28 April.

United States Chamber of Commerce Foundation (2014). The Future of Data-Driven Innovation. U.S. Chamber of Commerce Foundation, Washington, DC.

United States Department of Justice (2019). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, Washington, DC. Available at: https://www.justice.gov/opa/press-release/file/1153446/download.

United States Trade Representative (2020). United States–Kenya Negotiations: Summary of Specific Negotiating Objectives. Washington, DC, May. Available at: https://ustr.gov/sites/default/files/Summary_of_U.S.-Kenya_Negotiating_Objectives.pdf.

Varas A, Varadarajan R, Goodrich J and Yinug F (2021). Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. Boston Consulting Group and Semiconductor Industry Association, April.

Véliz C (2019). The Internet and Privacy. In: Edmonds D, ed., *Ethics and the Contemporary World*. Routledge, Abingdon: 149–159.

Verhulst SG (2017). A distributed model of Internet governance. Global Partners Digital, London. Available at: https://www.gp-digital.org/publication/a-distributed-model-of-internet-governance/.

Verhulst SG (2019). Sharing Private Data for Public Good. Project Syndicate, 27 August. Available at: https://www.project-syndicate.org/commentary/private-data-public-policy-collaboration-by-stefaan-g-verhulst-1-2019-08.

Verizon (2016). *2016 Data Breach Investigations Report*. Available at: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf.

Verizon (2017). *2017 Data Breach Investigations Report*. Available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/highlights-of-the-2017-verizon-dbir-analyzing-the-latest-breach-data-in-10-years-of-incident-trends/.

Verizon (2018). *2018 Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

Verizon (2019). *2019 Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/dbir/2019/data-breaches-by-industry/.

Verizon (2020). *2020 Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/dbir/.

Vestager M and Borrell J (2021). Why Europe's Digital Decade Matters. Project Syndicate, 10 March. Available at: https://www.project-syndicate.org/commentary/europe-digital-decade-by-margrethe-vestager-and-josep-borrell-2021-03?barrier=accesspaylog.

Viljoen S (2020). Democratic Data: A Relational Theory for Data Governance. Forthcoming, *Yale Law Journal*, 131.

Villani C (2018). For a Meaningful Artificial Intelligence: Towards a French and European Strategy. A French parliamentary mission (8 September 2017–8 March 2018), AI for Humanity, Paris. Available at: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.

Voss GW (2020). Cross-Border Data Flows, the GDPR, and Data Governance. *Washington International Law Journal*, 29(3): 485–532.

Washington State Department of Commerce (2018). State of the Data Center Industry. Department of Commerce, Office of Economic Development and Competitiveness, State of Washington, Olympia, WA. Available at: https://www.commerce.wa.gov/wp-content/uploads/2018/01/Commerce-Data-Center-Study-and-appendices-2017.pdf.

Weber S (2017). Data, Development and Growth. *Business and Politics*, 19(3): 397–423.

WEF (2019). Exploring International Data Flow Governance - Platform for Shaping the Future of Trade and Global Economic Interdependence. White Paper, World Economic Forum, Geneva, December. Available at: http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.

WEF (2020a). State of the Connected World: 2020 Edition. Insight Report, World Economic Forum, Geneva, December.

WEF (2020b). A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy. White Paper, World Economic Forum, Geneva, June.

WEF (2020c). *The Global Risks Report 2020*. Insight Report, 15th Edition. World Economic Forum, Geneva.

WEF (2020d). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. White Paper, World Economic Forum, Geneva, May.

WEF (2021). Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT). White Paper, World Economic Forum, Geneva, March.

Weller D and Woodcock B (2013). Internet Traffic Exchange: Market Developments and Policy Challenges. *OECD Digital Economy Papers*, No. 207. OECD Publishing, Paris, France.

Wesolowski A, Buckee CO, Bengtsson L, Wetter E, Lu X and Tatem AJ (2014). Commentary: Containing the Ebola Outbreak – the Potential and Challenge of Mobile Network Data. PLOS Currents Outbreaks, Edition 1, 29 September. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4205120/.

Woods AK (2018). Litigating Data Sovereignty. *Yale Law Journal*, 128(2): 328–406.

World Bank (2016). *World Development Report 2016: Digital Dividends*. doi:10.1596/978-1-4648-0671-1. World Bank, Washington, DC.

World Bank (2021). *World Development Report 2021: Data for Better Lives*. doi:10.1596/978-1-4648-1600-0. World Bank, Washington, DC.

Wu M (2017). Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange, Overview Paper, International Centre for Trade and Sustainable Development and Inter-American Development Bank, Geneva.

Yakovleva S and Irion K (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, 10(3): 201–221.

Zhang D, Mishra S, Brynjolfsson E, Etchemendy J, Ganguli D, Grosz B, Lyons T, Manyika J, Niebles JC, Sellitto M, Shoham Y, Clark J and Perrault R (2021). *The AI Index 2021 Annual Report*. AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March.

Zwetsloot R, Dunham J, Arnold Z and Huang T (2019). Keeping Top AI Talent in the United States: Findings and Policy Options for International Graduate Student Retention. Center for Security and Emerging Technology, Georgetown's Walsh School of Foreign Service, December. Available at: https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

Printed at United Nations, Geneva – 2111046 **(S)** – March 2022 – 158 – **UNCTAD/DER/2021**