Flujos transfronterizos de datos

Materializando los beneficios y eliminando las barreras

Septiembre de 2018

La GSMA representa los intereses de los operadores móviles de todo el mundo, reuniendo a más de 750 operadores con más de 350 compañías del amplio ecosistema móvil. Estas empresas incluyen fabricantes de teléfonos y dispositivos, empresas de software, proveedores de equipamiento y empresas de internet, así como también organizaciones de sectores adyacentes de la industria. La GSMA también organiza eventos líderes de la industria como el Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas y la serie de conferencias Mobile 360.

Para más información, visite el sitio de la GSMA en gsmala.com y el sitio de política pública en www.gsma.com/publicpolicy

Para visualizar los recursos relacionados con la GSMA en línea, visite www.gsma.com/mobileprivacy

Siga a la GSMA en Twitter: @GSMALatam y @GSMAPolicy

Autores

La GSMA encargó a Wickham Heath Consulting la investigación y redacción del presente reporte. Wickham Heath Consulting Limited es una consultora con sede en el Reino Unido cuya actividad principal es la regulación de nuevas comunicaciones y productos de plataformas de Internet.

ÍNDICE

Resumen

Hoy en día, el comercio depende de la capacidad de las organizaciones para transferir datos –incluidos los datos personales de los consumidores– a través de las fronteras, sin restricciones. Poder hacerlo genera resultados positivos, no sólo para las organizaciones, sino también para los ciudadanos y los países.

Siempre que la circulación de datos esté permitida, cualquier organización –independientemente de su tamaño– puede utilizar internet para comercializar y ofrecer sus ideas, bienes y servicios. Las transferencias transfronterizas de datos posibilitan el acceso a bienes y servicios digitales casi en forma instantánea y el pedido de bienes físicos para su envío, sin importar dónde se producen esos artículos. Al expandirse las organizaciones responden a la demanda de los consumidores para atender más mercados geográficos y así ofrecer mayor cantidad de opciones al consumidor. Al mismo tiempo, la eficiencia de las empresas que operan en múltiples países aumenta gracias a la centralización y virtualización del análisis, procesamiento y almacenamiento de los datos.

Algunos países introdujeron restricciones al flujo transfronterizo de datos, basadas en preocupaciones sobre la seguridad nacional y la privacidad de los datos o en la intención de proteger los mercados nacionales. Las restricciones adoptan diferentes formas, tales como la obtención del consentimiento expreso de los ciudadanos o de la autorización previa de las autoridades de protección de datos. Las normas más prohibitivas impiden a las organizaciones la transferencia de todo tipo de datos o metadatos personales.

Esas restricciones tienen diversos efectos. Por ejemplo, exigir que las organizaciones conserven una copia adicional de los datos generados a partir de sus actividades en un país aumenta los costos de producción de los bienes y servicios físicos y digitales en ese mercado. Los costos aumentan aún más cuando el análisis y el procesamiento de los datos, así como el almacenamiento, se deben realizar a nivel nacional.

Al igual que cualquier otra empresa internacional, los operadores de telecomunicaciones buscan materializar las eficiencias de la centralización y la virtualización. Sin embargo, los metadatos generados sobre las comunicaciones de las personas a menudo están sujetos a regulaciones específicas del sector u obligaciones de sus licencias anteriores a la era digital que prohíben la circulación de metadatos fuera del país y, por el contrario, exigen su recolección y almacenamiento. Las restricciones específicas a las telecomunicaciones ponen en desventaja a los operadores de telecomunicaciones respecto de los proveedores de servicios de telecomunicaciones no regulados, tales como las plataformas del internet.

En respuesta a la creciente incidencia de las medidas de localización de datos a nivel mundial, este documento presenta una serie de recomendaciones para que los gobiernos destraben los beneficios de los flujos transfronterizos de datos para las personas, las organizaciones, los gobiernos y la economía, al mismo tiempo que garantizan la implementación de normas de privacidad de datos suficientes como para proteger a los ciudadanos y mantener su confianza en el ecosistema digital.

Recomendación 1:	Comprometerse a facilitar los flujos transfronterizos de datos y a eliminar las medidas de localización innecesarias
Recomendación 2:	Garantizar que los marcos de privacidad estén preparados para la era digital
Recomendación 3:	Revisar las normas sobre privacidad heredadas específicas del sector
Recomendación 4:	Promover iniciativas regionales de privacidad de datos
Recomendación 5:	Evitar la localización dando un tratamiento pragmático a las preocupaciones de vigilancia extranjera
Recomendación 6:	Evitar la localización dando un tratamiento pragmático a las preocupaciones de ejecución de la ley y seguridad nacional

Introducción: Entendiendo los beneficios del libre flujo de datos

Hoy en día los datos son fundamentales para el comercio digital y físico, y constituyen un catalizador vital para la innovación. El desarrollo de la economía digital y el crecimiento continuo de la productividad de las industrias tradicionales dependen de la capacidad de las organizaciones para transferir datos, incluidos los datos personales de los consumidores, dentro y fuera del país, a fin de permitir un análisis, procesamiento y almacenamiento eficientes. La libertad para transferir datos personales entre países sin restricciones genera resultados positivos, no solo para las organizaciones, sino también para los ciudadanos y los países.

Beneficios para los ciudadanos

El acceso a internet ofrece a las personas un medio para interactuar con otras personas y organizaciones en cualquier parte del mundo, ya sea a nivel local, nacional, en un país limítrofe o en otro continente.

Los flujos internacionales de datos soportan el acceso a la amplia gama de bienes y servicios disponibles en línea. Se puede acceder a bienes y servicios digitales casi en forma instantánea y pedir bienes físicos para su envío, sin importar dónde se producen esos artículos.

Al expandirse a más mercados geográficos, las organizaciones responden a la demanda de los consumidores, ofreciendo a esos clientes acceso a una mayor variedad de bienes y servicios. En general, esta expansión del marketing digital y físico aumenta la satisfacción y las opciones del cliente. La libre circulación de datos a través de las fronteras permite que las organizaciones utilicen infraestructura común para atender múltiples mercados y así los bienes y servicios digitales puedan llegar más rápido a los clientes. Esto beneficia especialmente a las pequeñas y medianas empresas sin presencia internacional.

El escenario 1[1] describe cómo utiliza una persona el internet –que depende de transferencias de datos internacionales– para ampliar sus oportunidades, desarrollarse profesionalmente y buscar oportunidades de negocios.

1. Los escenarios de este documento son ficticios y pretenden ilustrar los beneficios de los flujos transfronterizos de datos y las desventajas de restringirlos. Si bien están inspirados y basados en análisis de experiencias reales con los operadores de telecomunicaciones y los representantes de la industria, no deben ser considerados como casos reales.

Escenario 1: **Las transferencias internacionales de datos facilitan las oportunidades individuales**

Luisa aprende a cocinar de niña mientras vive en España. De adulta, se muda a otro país y sigue cocinando, manteniéndose al día con las nuevas recetas de su país natal a través de internet. Su identidad y preferencias digitales mejoran su experiencia en internet y facilitan el acceso a información sobre cocina regional española, incluyendo recetas y videos de cocina.

Luisa arma un exitoso negocio *pop-up* móvil, cocinando comida regional española en fiestas y eventos. Luego, abre una escuela de cocina para adultos, dictando clases por la mañana y la noche en su casa y, más tarde, logra abrir un pequeño restaurante. Para crear comida distintiva, continúa utilizando internet, el correo electrónico y las transferencias de dinero electrónico para pedir ingredientes a mayoristas especializados, incluso algunos en España, que realizan envíos internacionales. Con el tiempo, el negocio se expande, se muda a un local más grande y emplea a más personal.

El éxito de Luisa al crear una empresa a pequeña escala depende del acceso internet y de la circulación transfronteriza de datos. Mientras expande gradualmente sus actividades profesionales para conseguir más trabajo para ella y otras personas, el gobierno se beneficia gracias a los impuestos. Y muchos clientes disfrutan de su cocina regional española.

Beneficios para los países y la sociedad

Permitir el intercambio de datos a través de las fronteras puede introducir más empresas y consumidores nacionales en el mundo digital, promoviendo la adopción de estrategias de negocios impulsadas por los datos y estimulando la economía nacional.

El crecimiento de los servicios de internet a nivel nacional debe apoyarse en enfoques flexibles para la transferencia de datos a través de las fronteras. La libre circulación de datos personales ofrece beneficios socioeconómicos más rápido que las opciones alternativas, donde se exige que las empresas estructuren sus funciones administrativas, de procesamiento y de almacenamiento para atender múltiples mercados individuales.

Los encargados de formular políticas han reconocido el rol estratégico de la transferencia transfronteriza de datos:

- El Consejo de Europa[2] explica que: "los flujos de información mundial desempeñan un papel cada vez más importante en la sociedad moderna, facilitando el ejercicio de derechos y libertades fundamentales mientras impulsan la innovación y promueven el progreso económico, además de desempeñar un papel fundamental para garantizar la seguridad pública".

- El Foro de Cooperación Económica Asia-Pacífico (APEC, por su sigla en inglés)[3] reconoce: "la importancia de desarrollar protecciones efectivas a la privacidad que eviten imponer barreras a los flujos de información, y aseguren el crecimiento continuo y el crecimiento económico en la región APEC. [...] Sistemas reguladores que restringen innecesariamente este flujo o le imponen cargas tienen implicaciones adversas para el comercio global y para las economías y las personas. Por lo tanto, para promover y hacer cumplir prácticas éticas de información, existe la necesidad de desarrollar sistemas para proteger la privacidad de la información, que den cuenta de estas nuevas realidades en el ambiente global".

- La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (CNUCYD)[4] cita investigaciones del McKinsey Global Institute: "En 2014, la dimensión internacional de los flujos [de bienes, servicios y finanzas] aumentó el PIB mundial casi un 10 por ciento, equivalente a un valor de USD7,8 billones. Los flujos de datos representan aproximadamente USD2,8 billones de este valor agregado".

- La OCDE[5] establece que: "Los flujos transfronterizos de datos aumentaron la productividad y la eficiencia económica, mejorando el bienestar y el nivel de vida".

- La Comisión Europea[6] sostiene que: "Es probable que las restricciones injustificadas a la libre circulación de datos limiten el desarrollo de la economía de los datos en la UE [...] se corre el riesgo de fragmentar el mercado, reducir la calidad de servicio para los usuarios y menoscabar la competitividad de los proveedores de servicios de datos, en particular de las entidades de pequeña envergadura".

- La Cámara de Comercio Internacional (CCI)[7] insta a que los gobiernos "garanticen que todos los ciudadanos y compañías puedan aprovechar al máximo el potencial del internet [...] mediante la adopción de políticas facilitadoras de la incorporación de nuevas tecnologías y la circulación internacional de los datos que las soportan".

- Respecto del rol de los flujos transfronterizos de datos en el sector de manufactura, la Junta Nacional de Comercio de Suecia[8] sostiene: "Un flujo constante y continuo de bienes, servicios, capital, personas y datos es necesario para la producción competitiva. [...] la circulación de datos ya es una

2. Consejo de Europa, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* [Informe Explicativo del Protocolo que modifica el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal], (CETS 223), 2018. Párrafo 12.
3. Foro de Cooperación Económica Asia-Pacífico, Actualizaciones del Marco de Privacidad de APEC, 2016/CSOM/012app17.
4. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (CNUCYD), *Data protection regulations and international data flows: Implications for trade and development* [Regulaciones sobre Protección de Datos y Flujos Internacionales de Datos: Implicancias para el comercio y el desarrollo], 2016.
5. OCDE, *2012 Internet Economy* [Economía del Internet 2012]. Documento 143.
6. Comisión Europea, *Building a European Data Economy* [Construcción de una Economía de Datos Europea], COM (2017) 9 final.
7. CCI, *Trade in the digital economy – A primer on global data flows for policymakers* [Comercio en la Economía Digital – Guía Básica sobre los Flujos de Datos Globales para los Encargados de Formular Políticas], 2016.
8. Junta Nacional de Comercio (Suecia), *No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods* [Sin transferencia no hay producción – Informe sobre las transferencias transfronterizas de datos, cadenas de valor globales y la producción de bienes], 2015.

> parte indispensable del proceso de producción actual [y] será aún más importante para la producción en el futuro".

Los regímenes regulatorios que facilitan la transferencia internacional de datos permiten que organizaciones especializadas de pequeña envergadura establezcan una presencia en internet que es, al mismo tiempo, nacional e internacional. Se pueden crear y adoptar con éxito servicios en un mercado nacional y, luego, expandirlos hacia otros mercados, generando beneficios para el segundo país y los subsiguientes.

Los departamentos de gobierno y los organismos del sector público también se benefician de los flujos transfronterizos de datos que les permiten ofrecer servicios públicos de mejor calidad a un costo más bajo y perseguir objetivos de política pública que, de otro modo, no se podrían alcanzar, como ilustran los dos escenarios a continuación.

Escenario 2: **Gobierno local promueve eficiencia**

Una autoridad del gobierno local es responsable de los servicios de atención al ciudadano, incluidos los servicios sociales, de vivienda, de atención a los adultos mayores y de recaudación de impuestos. Cuenta con múltiples bases de datos y sistemas de TI heredados que evolucionaron a través de los años, pero se volvieron difíciles de mantener y no funcionan de manera integrada. Los procesos internos para reserva de viajes, reintegro de gastos, procesamiento de nómina y administración de las relaciones con los interesados también se volvieron engorrosos.

En línea con el enfoque nacional que busca aumentar la eficiencia y efectividad del gobierno, la autoridad contrata a un proveedor internacional de TI que presta un servicio holístico gestionado que migrará todos los sistemas heredados a una única plataforma central con un sistema de administración de casos integrado. Esto acelerará los procesos, reducirá los costos y permitirá que los equipos trabajen juntos para alcanzar los objetivos de política pública. En última instancia, generará mejores resultados, no sólo para los residentes afectados, sino también para toda la comunidad que paga los impuestos locales y, probablemente, para el país, porque mejora la situación fiscal general.

El proveedor de TI utiliza una combinación de sus propios proveedores necesarios para ofrecer la infraestructura y el software de gestión de casos, todo alojado y mantenido en servidores seguros ubicados fuera del país. Solo el personal autorizado de la autoridad del gobierno local tiene acceso a los datos.

Escenario 3: **Macrodatos para el bien social**

La alcaldesa de una ciudad capital estableció objetivos ambiciosos para reducir la contaminación. Su equipo encarga un proyecto que combina datos de estaciones meteorológicas, sensores fijos de calidad del aire y operadores de telecomunicaciones. Los datos anónimos y agregados de los operadores de telecomunicaciones ofrecen información detallada y contínua de los patrones de traslado de las personas que viajan diariamente al trabajo y de los visitantes. Esto permite que la ciudad incentive viajar en otros horarios o medios de transporte y facilita el monitoreo más específico y rentable de la contaminación en la ciudad, comparado con una red de sensores estática que recolecta datos similares.

Para obtener aún mejores resultados, el proyecto contempla colaborar con otras ciudades del mundo para comparar la gravedad de los niveles de contaminación entre ciudades y descubrir patrones e información sobre las decisiones de política más efectivas. Esto redundará en beneficios para todas las ciudades participantes, sus habitantes y visitantes.

Con el objetivo de lograr una colaboración efectiva, las ciudades y compañías participantes firman un acuerdo y designan conjuntamente a un proveedor líder de análisis de datos, que aloja los datos anónimos y agregados en una plataforma común. Si bien se analizan todos los conjuntos de datos aportados, ninguna ciudad ni compañía tiene acceso a los datos sin procesar lo que aporta la otra parte. Sin embargo, todos acceden a los beneficios de la información procesable generada por el análisis. Gracias a estas medidas, la alcaldesa alcanza las metas ambiciosas y las personas obtienen mejoras en la calidad de vida diaria y en los resultados de salud a largo plazo.

Beneficios para las organizaciones

Siempre que la circulación de datos esté permitida, cualquier organización –independientemente de su tamaño– puede utilizar internet para comercializar y ofrecer sus ideas, bienes y servicios. Sin la circulación de datos entre países, sería imposible que las organizaciones puedan ofrecer información y productos en respuesta a las solicitudes de las personas.

Los flujos transfronterizos de datos también mejoran la eficiencia de las organizaciones multinacionales gracias a la centralización y virtualización de sus operaciones internas. Estas organizaciones pueden expandir sus negocios en forma rentable, utilizando infraestructura flexible basada en la red y proveedores de servicios de aplicaciones especializados, minimizando así la inversión en equipos de TI adicionales.

Todo tipo de empresas internacionales está adoptando estrategias de transformación digital impulsadas por los datos para asegurar su futuro. Esto puede implicar la reforma de los procesos internos o TI externa y la subcontratación comercial. Estas estrategias competitivas dependen de poder recopilar, analizar, procesar y almacenar datos en operaciones de múltiples países. La circulación de datos posibilita nuevas formas de análisis de datos que permiten que las organizaciones generen información sobre las opiniones de los clientes y el desempeño de sus operaciones y productos.

Facilitar la libre circulación de los datos personales a nivel internacional permite que las empresas mejoren la calidad del servicio y reduzcan los costos y, en caso de competencia, esto redunda en precios más bajos para el consumidor. Los proveedores de infraestructura de internet, los proveedores de computación en la nube y los operadores móviles pueden estructurar los servicios de forma tal de atender a una gran cantidad de clientes en múltiples mercados al menor costo total.

Por ejemplo, el Escenario 4 describe a un importante operador de telecomunicaciones asiático que utiliza las transferencias transfronterizas de datos para mejorar la calidad de su servicio de red móvil y demuestra los beneficios para clientes y gobiernos.

Escenario 4: **La centralización y virtualización de datos optimiza la calidad del servicio de red móvil**

Un importante operador de telecomunicaciones asiático mejora la calidad de su servicio de red móvil creando un único centro para ofrecer gestión de redes y aseguramiento de la calidad optimizados a sus operaciones nacionales. El nuevo centro para todo el grupo monitorea el desempeño de la red, la congestión y los incidentes de fallas. Esta capacidad virtual permite al operador acceder y comparar datos sobre desempeño y condiciones de falla en toda su organización: esto sería imposible solo con gestión de redes a nivel nacional.

El nuevo centro tiene acceso a herramientas más sofisticadas de gestión de redes y servicios de proveedores de equipos y puede utilizar herramientas de monitoreo y diagnóstico de un solo proveedor en múltiples mercados nacionales. Esto redundó en mejoras en la calidad de la red móvil y en la optimización de las inversiones. Al crear un 'centro de excelencia' para mejorar la gestión de redes y servicios, el operador pudo desarrollar las capacidades técnicas de los empleados nacionales a través de transferencias temporarias de las empresas nacionales en funcionamiento y otras actividades de desarrollo profesional.

Gracias al análisis de los datos recolectados en los mercados nacionales, el operador puede diagnosticar proactivamente las condiciones de falla, incluidas las fallas de red más complejas, mientras distribuye los costos de capital y de personal entre todos sus clientes. La centralización de datos mejora la calidad de los servicios móviles de voz, datos e internet para los clientes y los gobiernos nacionales.

Los gobiernos pueden ayudar a conseguir todos los beneficios anteriores a través de marcos de política pública que faciliten al máximo los flujos transfronterizos de datos, mientras alcanzan otros objetivos de política pública, tales como la privacidad y la seguridad de los datos.

Restricciones a los flujos transfronterizos de datos

Motivos dados para la imposición de restricciones

Algunos países introdujeron restricciones a los flujos transfronterizos de datos. Si bien los motivos de la introducción de restricciones difieren entre los países, en general, comparten una o más de las siguientes justificaciones:

- **Privacidad y seguridad de los datos.** Es posible que el procesamiento de los datos se realice en países que no cuentan con una reglamentación sobre privacidad equivalente y podrían ser más vulnerables al hackeo.
- **Vigilancia extranjera.** Los datos mantenidos a nivel internacional pueden ser vulnerables a la vigilancia por parte de gobiernos extranjeros o terceros.
- **Seguridad nacional.** Es posible que las compañías de plataformas del internet y los operadores de telecomunicaciones que mantienen los datos a nivel internacional no estén obligados a ofrecer el mismo soporte a los organismos de aplicación de la ley o de seguridad nacional.
- **Economía digital nacional.** Es posible que promover el análisis, procesamiento y almacenamiento de datos en el país se perciba como una forma de proteger o estimular la economía digital nacional.

Tipos de restricciones

Para las organizaciones, el impacto de las restricciones sobre los flujos transfronterizos de datos varía dependiendo de la naturaleza de la restricción aplicada. Los tipos de restricciones incluyen:

- **Flujos de datos condicionales** – Cuando la restricción se basa en la privacidad y seguridad de los datos, es posible que se exija que las organizaciones obtengan autorización previa de los reguladores, incluidas las autoridades de protección de datos, así como también el consentimiento de los ciudadanos, o ejecuten cláusulas contractuales prescritas con cada receptor de los datos ubicado aguas abajo en la cadena de procesamiento. Los marcos que ofrecen permisos generales, tales como las Reglas de Privacidad Transfronteriza de APEC y las Normas Corporativas Vinculantes de la EU, pueden ser más atractivos porque permiten la transferencia continua de los datos por parte de las organizaciones dentro de un grupo corporativo o a receptores específicos. Sin embargo, los procesos para obtener esos permisos pueden ser complejos y costosos. Cuando un país considere que otro país cuenta con un sistema de privacidad que ofrece un 'nivel de protección adecuado' o que es 'equivalente' al propio, los datos se podrán transferir libremente entre los países. Sin embargo, descubrir esos niveles de 'adecuación' toma mucho tiempo y se aplican a muy pocos países.

- **Localización + flujos posteriores** – Las organizaciones pueden estar obligadas a conservar una copia de todos los metadatos y datos personales en su país de origen, mientras que se pueden transferir copias adicionales de los datos al exterior para análisis, procesamiento y almacenamiento centralizado.

- **Localización** – Las organizaciones pueden estar sujetas a normas más prohibitivas que impiden directamente la transferencia de datos personales o metadatos. Estas pueden ser el resultado de obligaciones históricas de licencias u otros permisos requeridos por los operadores de telecomunicaciones u otros proveedores, o de reglamentaciones más nuevas que hoy en día se pueden aplicar a cualquier compañía activa en la prestación de servicios digitales.

- **Normas indirectas** – El efecto de las normas indirectas (y, en algunos casos, tácitas) pueden ser conservar los datos en un país específico o exigir su conservación a un proveedor nacional.

Impacto de las restricciones

Cuando se requieren protecciones adicionales relativas a cada transferencia de datos personales, tales como consentimientos o cláusulas contractuales estándares, esto puede representar una carga administrativa significativa para las organizaciones. Además, es posible que la protección se perciba como un mero ejercicio administrativo con poco beneficio real para los titulares de los datos. Los mecanismos son mucho más efectivos cuando alientan a las organizaciones a implementar programas holísticos para proteger los datos personales en cualquier lugar donde se puedan procesar. Estos mecanismos otorgan permisos generales a las organizaciones para transferir datos a través de las fronteras y les permiten concentrarse en la identificación y mitigación de los riesgos.

Exigir que las organizaciones conserven una copia adicional de los datos generados a partir de sus actividades en un país aumenta los costos de producción de los bienes y servicios en ese mercado. Las compañías deben poner en servicio y operar centros de datos a escala nacional que, de otro modo, podrían brindar soporte a múltiples mercados nacionales o incluso recibir información a nivel mundial de uno o dos centros de datos (para aumentar la resiliencia).

Los costos aumentan aún más cuando el análisis, procesamiento y almacenamiento de los datos se deben realizar a nivel nacional. Efectivamente en este caso la regulación requiere que las organizaciones ofrezcan bienes y servicios digitales utilizando empresas duplicadas a escala nacional, ubicadas en mercados nacionales individuales regulados. Dependiendo de la arquitectura de sistemas y la implementación técnica de las compañías, este tipo de sistema más oneroso demora y fragmenta la introducción de bienes y servicios digitales y reduce su viabilidad.

Para ver algunos ejemplos, consulte el Escenario 5, que analiza la detección remota de fallas por parte de un fabricante de vehículos y el Escenario 6, que detalla la implementación internacional de un servicio del Internet de las Cosas Things (IoT, por sus siglas en inglés) por parte de un operador de telecomunicaciones internacional.

Escenario 5: **Detección de fallas en automóviles a través de las fronteras**

Los vehículos modernos son cada vez más inteligentes y están equipados con dispositivos para capturar datos sobre el rendimiento del motor y detectar fallas en el vehículo. Los mecánicos pueden consultar estos datos para realizar el diagnóstico de fallas con mayor eficiencia. Algunos fabricantes utilizan la tecnología *de máquina a máquina* (M2M, por su sigla en inglés) para vincular los datos de monitoreo de fallas a servidores centrales, lo que permite la detección y el diagnóstico de fallas antes de que el dueño del automóvil lo advierta. También se utiliza la tecnología M2M para alertar a los clientes sobre la necesidad de realizar mantenimiento al vehículo. Los flujos transfronterizos de datos aparecen firmes en estos escenarios que optimizan la confiabilidad y tienen el potencial de salvar vidas, ya que los automóviles y los vehículos comerciales cruzan las fronteras todo el tiempo.

Para aprovechar aún más los beneficios, los autos conectados permiten que los fabricantes utilicen *big data* analytics, que revela las características de rendimiento de toda la gama de vehículos conectados. Sin embargo, este escenario sólo se aplica a mercados o jurisdicciones donde los fabricantes pueden conectarse a los vehículos de los clientes y analizar los datos recabados. Como resultado, los países que no permiten el libre flujo de datos de los consumidores a través de las fronteras inhibirán el diagnóstico remoto de los vehículos y, en consecuencia, el acceso a transporte más seguro y confiable.

Escenario 6: **El servicio de IoT multinacional depende de un único centro de datos**

Un operador de telecomunicaciones internacional desarrolló un servicio que permite a los consumidores localizar, monitorear y realizar el seguimiento de artículos, tales como automóviles, mochilas, mascotas o ganado, a través de una aplicación móvil. A través de este servicio, se puede verificar la condición de los artículos en tiempo real, así como también encontrar artículos perdidos y establecer alarmas en base a la ubicación de un artículo.

El servicio se lanzó a nivel internacional utilizando un centro de datos común, de forma tal que se pueda atender cada mercado nacional sin replicar los sistemas informáticos para cada mercado. Los fabricantes también pueden experimentar con sus productos para descubrir qué consideran valioso los clientes en los diferentes mercados y segmentos nacionales. En los mercados que requieren un centro de datos localizado dentro del país, el proveedor de servicios tiene costos más altos para personalizar e implementar la arquitectura de los productos. Por eso, en este momento, decidió renunciar al lanzamiento del servicio en estos mercados. Como consecuencia de las restricciones a los flujos transfronterizos de datos, los clientes no tienen acceso al seguimiento y monitoreo de artículos personales a bajo costo; los fabricantes no pueden probar los productos para ver su valor en el mercado nacional; y los gobiernos pierden los beneficios económicos y fiscales de este servicio innovador y útil.

Cabe destacar que la forma en que las autoridades nacionales implementan o interpretan esas restricciones a la localización puede mitigar considerablemente el impacto negativo que, de otro modo, podrían tener. Por lo tanto, cuando los gobiernos insisten en aprobar este tipo de medidas, deben interactuar con la industria y otros interesados antes de implementarlas.

Ejemplos de restricciones nacionales

Algunos mercados se alejaron, o están considerando hacerlo, de un modelo que soporta el libre flujo transfronterizo de datos.

El alcance de la circulación de datos personales varía dentro de la categoría de restricciones que se basan en las preocupaciones sobre la privacidad de los datos. Por ejemplo, Corea del Sur impone estrictos requerimientos de consentimiento para las transferencias de datos personales con mínimas excepciones, tales como la transferencia de datos exigidos por ley, necesarios para desempeñar una función pública o para proteger los intereses vitales en una emergencia. Costa de Marfil solo permite transferencias de datos personales en base a autorización previa, o hacia países que tienen un nivel de protección adecuado, pero no queda claro cuáles son esos países. Otros países ofrecen a las organizaciones la opción de elegir entre un conjunto de excepciones y mecanismos de transferencia más flexibles que reducen significativamente el impacto de la restricción.

Las restricciones que causan las mayores dificultades para las organizaciones son aquellas que requieren, directa o indirectamente, que los datos se conserven dentro del país. Rusia, por ejemplo, exige a las organizaciones (incluidas las subsidiarias de sociedades extranjeras) que recolecten los datos personales de todos los ciudadanos a través de comunicaciones electrónicas para almacenarlos a nivel nacional.[9] Los datos personales se deben guardar en una base de datos primaria localizada y mantenida en Rusia. Si bien los datos se pueden transferir posteriormente al exterior y guardar en bases de datos secundarias, siempre que se

9. La Ley Federal Nº 242-FZ del 21 de julio de 2014 reformó ciertos actos legislativos de la Federación Rusa relativos a la información sobre el procesamiento de datos personales y las redes de telecomunicaciones.

cumpla cualquier otro requerimiento legal[10] para el tratamiento de los datos, el requisito de conservar los datos originales en Rusia requiere recursos adicionales.

En Indonesia, los operadores de telecomunicaciones, las compañías de plataformas del internet y otros actores que prestan un 'servicio público' a clientes indonesios a través de un sistema electrónico están obligados a establecer un centro de datos y un centro de recuperación ante desastres nacionales.[11] Esto incluye los servicios prestados por instituciones no gubernamentales en los sectores de banca, comunicaciones, salud, seguro, servicios industriales, seguridad y redes sociales. La aplicación de la ley y la protección de datos justifican la creación de un centro de datos y un centro de recuperación ante desastres nacionales. En principio, las transferencias transfronterizas de datos están permitidas, conforme al acuerdo del Ministerio de Comunicaciones e Informática Indonesio, aunque este proceso está sujeto a aclaraciones adicionales.

La Autoridad de Telecomunicaciones de Pakistán y el Banco Estatal de Pakistán prohíben a las compañías de telecomunicaciones y financieras la transferencia de datos de clientes al exterior. Sin embargo, es lícito transmitir y almacenar otros datos fuera del país, incluido el contenido del correo electrónico. En India se aplican condiciones de licencia similares.

En Vietnam, el requerimiento existente de almacenar datos en servidores locales fue recientemente reemplazado por un requerimiento para que los proveedores extranjeros de telecomunicaciones y servicios del internet con más de 10.000 usuarios cuenten con oficinas centrales o de representantes en Vietnam y almacenen datos personales de los usuarios de Vietnam dentro del país.

En Alemania, los operadores de telecomunicaciones están obligados a conservar los datos de tráfico y localización dentro de Alemania (si bien esto aún no se aplica debido a múltiples objeciones legales). Kazakstán está analizando una ley que obligaría a los operadores de telecomunicaciones a almacenar datos de suscriptores solo en Kazakstán, además de cuando fuese necesario para fines de roaming.

Respuestas a las preocupaciones sobre privacidad nacional

Cuando el fundamento declarado para restringir los flujos transfronterizos de datos es la protección de datos, los encargados de formular políticas sostienen que los datos personales no se pueden proteger durante transferencias internacionales y que las personas quizás no tengan suficientes derechos en países que no tienen las mismas protecciones.

Si bien esta inquietud es válida, una respuesta proporcional y efectiva debería ser un marco nacional o regional para la privacidad de los datos, que proteja a ciudadanos y consumidores a nivel nacional, mientras ofrece mecanismos adecuados para la transferencia de datos internacionales con protecciones asociadas.

Cuando las preocupaciones sobre privacidad se relacionan con la seguridad de la información, probablemente se basan en la idea equivocada de que los datos almacenados en un mercado nacional específico son más seguros que los datos almacenados a nivel internacional. Sin embargo, la seguridad efectiva de la información no se puede reducir a un único elemento, tal como dónde se almacenan físicamente los datos. Depende de una amplia combinación de factores, incluyendo la infraestructura de almacenamiento, la inteligencia de los protocolos de seguridad, el uso de encriptación y otras mejores prácticas de TI.

Exigir el almacenamiento nacional de datos crea fricción con la seguridad de datos, porque requiere una inversión separada para cada mercado a escala nacional. Esto es más costoso y más vulnerable a la intrusión que las defensas corporativas internacionales a mayor escala.[12]

Hoy en día, muchos países y regiones están adoptando modelos regulatorios para asegurar que los datos puedan circular a través de las fronteras, sujetos a los requerimientos de protección de datos adecuados.

10. Incluyendo la Ley de Datos Personales Nº 152-FZ del 27 de julio de 2006 que prohíbe la transferencia transfronteriza de datos a países que no ofrecen protección adecuada a los titulares de los datos.
11. Regulación Nº 20 del 1 de diciembre de 2016 sobre Protección de Datos Personales en Sistemas Electrónicos, que implementa la Regulación del Gobierno 82 de 2012: Respecto de la Prestación de Sistemas y Transacciones Electrónicos.
12. El Amazon *Data Residency Whitepaper* [Documento Técnico de Residencia de Datos de Amazon], de febrero de 2018 ofrece un análisis extendido de la seguridad desde la perspectiva de un proveedor de servicios en la nube a *'hiperescala'* en: https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

En Estados Unidos, la privacidad de los datos se regula a diferentes niveles. Algunas leyes federales apuntan a sectores o actividades particulares, tales como el reporte de crédito justo o el uso de datos de salud, mientras que las leyes estatales contemplan desde reportes sobre violaciones de seguridad hasta leyes más abarcativas. A nivel federal y a través de su jurisdicción, la Comisión Federal de Comercio aplica buenas prácticas de privacidad de datos a los actos y prácticas comerciales injustos y engañosos, así como a algunas cuestiones específicas, tales como la privacidad de los niños. La Comisión Federal de Comunicaciones supervisa y establece normas para los proveedores de redes. En general, estas leyes no restringen la circulación de datos fuera de EE.UU., sino que se focalizan en hacer responsables a las organizaciones por el uso de los datos por parte de sus proveedores. Estados Unidos interactúa positivamente con los marcos regionales para facilitar los flujos transfronterizos de datos, participando en el sistema de las Reglas de Privacidad Transfronteriza (CBPR) de APEC y en el acuerdo *Privacy Shield* con la UE. El enfoque de EE.UU., centrado en la responsabilidad, facilitó el rápido crecimiento de las empresas nacionales de bienes y servicios digitales y, posiblemente, su dominio sobre gran parte de la economía internacional en bienes y servicios digitales.

La Unión Europea adoptó la influyente Directiva de Protección de Datos[13] en 1995. Este enfoque evolucionó hasta convertirse en el Reglamento General de Protección de Datos[14] (GDPR, por su sigla en inglés). El objetivo del GDPR es ofrecer protección consistente de los datos personales en toda la UE, permitiendo la circulación dentro de la UE y hacia otros países que cuentan con sistemas de protección de datos considerados 'adecuados'. Conforme al GDPR, las organizaciones que puedan demostrar el manejo responsable de los datos personales ante las autoridades de protección de datos, ya sea a través de 'normas corporativas vinculantes' o a través de certificaciones, pueden aprovechar los permisos generales para transferir datos personales fuera de la UE. La ley también ofrece una variedad de mecanismos y excepciones adicionales[15] destinados a otorgar a las organizaciones cierto grado de flexibilidad para hacer frente a las necesidades de flujo de datos de la forma más conveniente para la organización. En varios países del mundo, las últimas propuestas comenzaron a seguir el modelo del GDPR. En Brasil, por ejemplo, se permitirán las transferencias de datos personales conforme a la nueva ley, siempre que el tercer país cuente con mecanismos adecuados para proteger los datos personales y facilitar la cooperación institucional y judicial.

En septiembre de 2017, la Comisión Europea publicó una propuesta adicional diseñada para asegurar el libre flujo de datos 'no personales' y así mejorar la economía digital europea. Esta medida propone:

- La libre circulación de datos no personales dentro de la UE (para complementar la transferencia de datos personales);
- Acceso de la autoridad pública a los datos ubicados en otro Estado Miembro de la UE o en la nube; y
- Un enfoque de autorregulación para la transferencia entre proveedores de servicios en la nube destinado a usuarios profesionales.

Aún no queda claro cómo operará la medida para regular los datos no personales. Sin embargo, la Comisión Europea sostiene que garantizar la libre circulación de datos dentro de la UE ayudará a respaldar la economía digital europea y generará un PIB adicional del 0,7% para 2020, un incremento respecto del 0,2% en 2013.[16]

Los países de la región de Asia-Pacífico desarrollaron un modelo común de regulación del flujo internacionales de datos bajo el auspicio de APEC, cuyas Reglas de Privacidad Transfronteriza (CBPR, por sus siglas en inglés) estipulan cómo deberían operar los flujos de datos entre las economías de APEC.

Las CBPR de APEC presentan tres elementos principales:

- Adopción de principios compartidos en el tratamiento de los datos personales;
- Creación de mecanismos de aplicación donde la transferencia de los datos se realiza entre economías de los países miembros; y
- Responsabilidad de las organizaciones, que deben poder demostrar que cuentan con ciertas protecciones antes de recibir un permiso general para transferir datos.

En la actualidad, las economías participantes son seis: EE.UU., México, Japón, Canadá, Singapur y la República de Corea, con otras que buscan activamente sumarse en el futuro cercano.

13. Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
14. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. El GDPR se acordó en 2016 y el 25 de mayo de 2018 comenzó a aplicarse a las organizaciones que procesan datos.
15. Para más información sobre los diferentes mecanismos disponibles a nivel general, consulte el documento de CIPL: *Cross-Border Data Transfer Mechanisms* [Mecanismos de Transferencia Transfronteriza de Datos], agosto de 2015.
16. *SMART 2013/0043 - Uptake of cloud in Europe* [SMART 2013/0043 - Incorporación de la computación en la nube en Europa] estudio de IDC sobre estimaciones cuantitativas de la demanda de computación en la nube en Europa y de los posibles obstáculos para su aceptación. Citado en *Measuring the economic impact of cloud computing in Europe* [Medición del impacto económico de la computación en la nube en Europa] de Deloitte, que, a su vez, es citado por la CE en respaldo de la Directiva propuesta.

La Ley de Protección de la Información Personal de Japón, que se aprobó inicialmente en 2003, fue sometida a reformas en 2015 y entró definitivamente en vigencia el 30 de mayo de 2017. Además de establecer una autoridad de protección de datos independiente totalmente funcional, el objetivo de la reforma era facilitar los flujos transfronterizos de datos a través de una variedad de mecanismos, reconociendo la importancia de los flujos de datos para la economía digital. Estos mecanismos incluyen expresamente la posibilidad de que las organizaciones demuestren la gobernanza responsable de los datos a través de la certificación conforme a CBPR.

Después de las recientes conversaciones entre Japón y la UE, en julio de 2018 la Comisión Europea anunció que reconocerán formalmente que los sistemas de protección de datos de la otra parte ofrecen un nivel de protección equivalente para los consumidores en ambos mercados. Esto dará lugar al área más grande del mundo –que representa un valor del 37 por ciento del comercio mundial– dentro de la cual los datos personales pueden circular libremente mientras reciben un nivel de protección consistente. Antes de fines de 2018, la UE y Japón esperan ratificar el proceso de comprobar que los sistemas de protección de datos de la otra parte son 'adecuados'. Actualmente, Japón está bien posicionada para respaldar el libre flujo de datos internacionales tanto en Asia-Pacífico como en la UE, aunque conforme a los diferentes marcos de privacidad.

Los países que adoptan enfoques de protección de datos internacionalmente aceptados se benefician económicamente de la infraestructura de servicios digitales compartidos que opera a escala mundial. Estos mercados 'conectados por datos' forman una corriente principal de flujos de datos integrados a nivel internacional, donde los bienes y servicios digitales se pueden producir a escala y calidad global.

Respuestas a las preocupaciones sobre vigilancia extranjera y seguridad nacional

La información divulgada por Edward Snowden en 2013 sobre las actividades de la Agencia de Seguridad Nacional (NSA, por su sigla en inglés) de EE.UU. reveló la existencia de acuerdos con una serie de compañías de plataformas del internet para obtener acceso a los datos privados de ciudadanos no estadounidenses. Como era de esperar, la revelación de la amplia vigilancia secreta por parte de la NSA de datos privados de servicios digitales ubicados en EE.UU. preocupó a los gobiernos de todo el mundo. Esto disparó las preocupaciones sobre la vigilancia extranjera de los datos mantenidos en otros mercados nacionales.

En los cinco años posteriores a la divulgación de datos de Snowden, estas preocupaciones obtuvieron una respuesta parcial a través de la diversificación de países donde las compañías de plataformas del internet y los proveedores de computación en la nube operan centros de datos o hubs regionales. Esto permite que las organizaciones y los gobiernos preocupados por las actividades de vigilancia extranjeras eviten mantener datos en jurisdicciones particulares. Sin embargo, permitir este nivel de control geográfico a las organizaciones inevitablemente tiene un precio que debe pagar el cliente comercial o, en última instancia, el cliente *downstream*.

Además, los proveedores de computación en la nube pueden ofrecer a los clientes, tales como los operadores de telecomunicaciones, la capacidad de encriptación segura de los datos digitales para poder guardar las claves de esos datos a nivel nacional, volviéndolas invulnerables a la decodificación. Para impedir la identificación de datos personales transmitidos a nivel internacional también se pueden utilizar otras técnicas, como la anonimización y agregación. La combinación de estos desarrollos reduce sustancialmente los riesgos de vigilancia extranjera cuando los datos se mantienen a nivel internacional.

A diferencia de las medidas destinadas a las preocupaciones de vigilancia extranjera, no hubo un avance tan marcado para resolver las preocupaciones de aplicación de la ley y seguridad nacional de los países. Es lógico que los gobiernos estén preocupados por perder el acceso a datos que pueden ser útiles para las autoridades de aplicación

de la ley, pero que son procesados y controlados por compañías de internet ubicadas fuera del país. Si bien se pueden utilizar las disposiciones multilaterales existentes para compartir datos en respaldo de la aplicación de la ley, su operación es considerada lenta e imperfecta.

En vista de estas imperfecciones, los intereses de aplicación de la ley y seguridad nacional se manifestaron a favor del almacenamiento y/o la operación de servicios de datos nacionales porque ofrecen un punto de control sobre las actividades de las compañías de plataformas de internet y los operadores de telecomunicaciones. Algunos gobiernos fueron más allá y limitaron las actividades de las compañías de plataformas del internet cuando se detectó que no cooperaron con la aplicación de la ley nacional o que afectaron la seguridad nacional.

Sin embargo, los últimos desarrollos al respecto incluyen la *US CLOUD Act*, en inglés, la propuesta sobre prueba electrónica, *eEvidence*, de la UE y un protocolo adicional al Convenio sobre Ciberdelicuencia de Budapest. Estas iniciativas renuevan la esperanza de encontrar otras formas de ofrecer marcos claros y previsibles que otorguen seguridad jurídica a las organizaciones y acceso más directo y oportuno a los datos en el exterior que necesitan las autoridades, eliminando así la necesidad de medidas de localización.

Resolver las preocupaciones de aplicación de la ley y vigilancia extranjera requiere pragmatismo, tanto por parte de los países como de las empresas. En última instancia, los países que dan la espalda a los servicios disponibles en la economía digital mundial deben recurrir a la producción de bienes y servicios a escala nacional. Por su parte, los principales actores comerciales del mercado nacional tendrán dificultades para garantizar un negocio sostenible si se percibe que sus operaciones van en detrimento de la aplicación de la ley o la seguridad nacional.

Respuestas a las preocupaciones sobre la economía digital nacional

La reglamentación de los flujos transfronterizos de datos también se puede percibir como una forma de proteger los intereses económicos de las naciones y sus empresas. Sin embargo, esta noción todavía tiene fallas importantes. En particular, exigir el procesamiento y almacenamiento de datos a nivel nacional o la producción nacional de servicios digitales:

- Restringe estas actividades a la escala de operación nacional correspondiente y es probable que redunde en costos de operación por cliente atendido significativamente más altos;
- Incorpora otros factores de producción nacional a los servicios digitales (por ejemplo, si un país está sujeto a restricciones de suministro eléctrico, se pueden resolver, en parte, mediante el uso de almacenamiento de datos y producción de servicios digitales internacionales);
- Probablemente demore, limite o incluso impida el acceso de los ciudadanos a servicios digitales innovadores que surjan en el ámbito mundial; y
- No reconoce el valor que las habilidades y la información, que solo están disponibles si los datos pueden circular a través de las fronteras, significan para la economía nacional.

Una vez más, un enfoque de política pública alineado y coordinado, que elimine las restricciones y libere el flujo de datos, ofrecerá beneficios a los mercados nacionales.

Por ejemplo, el Escenario 7 ilustra cómo las restricciones a los flujos transfronterizos de datos afectan no solo el desarrollo de productos digitales, sino también la eficiencia de la manufactura tradicional.

Escenario 7: **Las aplicaciones M2M respaldan el comercio internacional y reducen los residuos**[17]

Las cadenas de manufactura y logística pueden ser muy complejas, independientemente de que se encuentren en la misma compañía multinacional o entre proveedores y clientes. Esta complejidad se maneja con 'envoltorios electrónicos' que realizan el seguimiento de los productos por depósito y puerto, del origen al destino.

Gracias a la telemetría M2M, ahora se utiliza documentación electrónica que amplía la capacidad de los proveedores de logística para realizar el seguimiento de los productos durante el viaje internacional. Por ejemplo, se puede realizar el seguimiento de un contenedor de partes de máquinas desde la fábrica hasta el puerto y durante su travesía por mar hasta el arribo al país de destino y la entrega al cliente.

Los flujos transfronterizos de datos permiten mayor eficiencia y seguridad en la logística y el seguimiento, reduciendo los costos de manufactura y los residuos. Esto facilita el respaldo de cadenas de suministro internacionales integradas y beneficia a los consumidores con precios más bajos. Gracias a esto, los gobiernos mejoran su habilidad para analizar el comercio internacional y aplicar tarifas correctamente.

Los países que exigen el manejo de los datos M2M en servidores nacionales limitarán la capacidad del país para participar en la economía mundial.

17. Junta Nacional de Comercio (Suecia), *No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods* [Sin transferencia no hay producción – Informe sobre las transferencias transfronterizas de datos, cadenas de valor globales y la producción de bienes], 2015.

En ausencia de enfoques regionales compartidos, es probable que las restricciones nacionales al libre flujo de datos por parte de ciertos mercados generen dos caminos divergentes en el desarrollo del mercado digital:

- **Mercados conectados por datos,** incluidos los mercados más desarrollados y muchos mercados emergentes donde es económico producir bienes y servicios digitales, que se ofrecen a ciudadanos y clientes a escala y calidad mundial.
- **Mercados digitales a escala nacional,** sujetos a restricciones a la circulación transfronteriza de datos y, por lo tanto, limitando las oportunidades de los proveedores y el beneficio económico para los consumidores.

Dadas las divergencias en las políticas actuales, es probable que los mercados conectados por datos tengan ventaja respecto de los sitios de producción y consumo y, con el tiempo, amplíen gradualmente su participación en el comercio internacional digital y físico.

Los encargados de formular políticas que consideran un modelo alternativo de mercado digital a escala nacional deben contemplar con cuidado las consecuencias económicas de separar el análisis, procesamiento y almacenamiento en el país de la corriente principal de flujos de datos integrados a nivel internacional. El riesgo de este enfoque es dejar a los países en un callejón sin salida a nivel nacional, que limitará el crecimiento digital en el mercado si se comparan con los competidores internacionales.

Impacto de las restricciones a los flujos transfronterizos de datos en el sector de las telecomunicaciones

El objetivo central de los operadores de telecomunicaciones es conectar a las personas, independientemente de la ubicación y la distancia. Si bien las telecomunicaciones comenzaron con telegramas y evolucionaron hasta convertirse en llamadas de voz, SMS y correos electrónicos, hoy en día incluyen el intercambio de datos a escala y la infraestructura y los servicios de los operadores que transportan estos datos.

Los operadores de telecomunicaciones comparten un objetivo común con otras empresas internacionales: desean que los datos circulen para poder materializar las eficiencias de la centralización y la virtualización. Sin embargo, como tradicionalmente eran considerados actores nacionales con infraestructura física en un país, los metadatos generados sobre las comunicaciones de las personas –con quién se conectan, desde dónde y durante cuánto tiempo– a menudo están sujetos a regulaciones específicas del sector u obligaciones de licencia anteriores a la era digital que prohíben la circulación de metadatos fuera del país y, por el contrario, exigen su recolección y almacenamiento.

Las restricciones específicas a las telecomunicaciones actúan como una barrera para alcanzar el tipo de eficiencia que se convirtió en el estándar para la mayoría de las demás empresas internacionales y ponen en desventaja a los operadores de telecomunicaciones respecto de los proveedores de servicios de telecomunicaciones no regulados, tales como las plataformas de internet.

Además, los operadores de telecomunicaciones están a la vanguardia del incipiente Internet de las Cosas y respaldan los avances en la automatización, desde sensores meteorológicos remotos hasta automóviles conectados. Para permitir estas tecnologías y destrabar sus potenciales beneficios, los operadores necesitan modelos de negocios y tecnologías comunes que funcionen en cualquier parte del mundo. Si los operadores de telecomunicaciones cargan con las restricciones heredadas específicas de las telecomunicaciones a los flujos transfronterizos de datos estarán en desventaja respecto de las plataformas de internet, y el desarrollo de estas tecnologías y modelos de negocios será mucho más lento y costoso.

Siempre que las restricciones específicas a las telecomunicaciones se basen en la sensibilidad percibida de los metadatos y en la necesidad de proteger la privacidad de las personas afectadas, este documento sostiene que es más efectivo proteger la privacidad de las personas a través de mecanismos de protección de datos horizontales basados en riesgos. Más que una categoría separada de datos que siempre se consideran sensibles, la sensibilidad de los metadatos depende del contexto en el cual se procesan y de las protecciones aplicadas a cada caso. Las leyes de privacidad de datos horizontales aplicables al procesamiento de todos los datos personales ofrecen suficiente protección al imponer obligaciones a las organizaciones para identificar y mitigar los riesgos de ocasionar daños a las personas. Cuando los datos se trasladan al exterior, estas

protecciones se pueden adaptar para que se apliquen por extensión sin interrumpir el flujo de datos.

Las restricciones específicas a las telecomunicaciones también se imponen para permitir que las autoridades de aplicación de la ley y los servicios de inteligencia obtengan acceso lícito y adecuado a los datos. Históricamente, los operadores de telecomunicaciones fueron los blancos naturales de este tipo de requerimiento porque ya contaban con la infraestructura física y los centros de procesamiento de datos en cada país y porque, antes de la llegada de internet, sus metadatos eran una de las mejores –y más evidentes– fuentes de inteligencia. Sin embargo, también se debe reconocer que la industria de las telecomunicaciones enfrenta la presión de aprovechar la infraestructura y los servicios de software basados en la nube de la misma forma en que lo hicieron otros sectores. Además de ser eficiente y bueno para los consumidores, el uso de servicios basados en la nube significa que no existe la necesidad operativa de realizar ciertas actividades de procesamiento dentro de la proximidad física del hardware de comunicaciones de un país.

Son legítimas las preocupaciones de las autoridades de aplicación de la ley que ya no podrán acceder a los datos que necesitan para las investigaciones. Sin embargo, en el futuro, más que exigir la recolección y el almacenamiento local de todos los datos u obligar a los operadores de telecomunicaciones a brindar acceso a todo el tráfico de internet que circula por sus redes, los gobiernos deberían recurrir a iniciativas de políticas tales como la *US Cloud Act* y la propuesta sobre prueba electrónica de la UE para resolver estas preocupaciones.

Mientras tanto, los operadores de telecomunicaciones que comienzan a centralizar y virtualizar sus operaciones también deben ofrecer a las autoridades nacionales la garantía pragmática de que continuarán respaldando las solicitudes legítimas de aplicación de la ley.

Enfoques mejorados para facilitar los flujos transfronterizos de datos

La industria móvil considera que los flujos transfronterizos de datos son vitales para destrabar los beneficios para las personas, las organizaciones, los gobiernos y la economía, tanto a nivel nacional como internacional. Identificar los beneficios de la libre circulación de datos no significa sugerir que no existe regulación en esta área. Una versión compartida por muchos formuladores de políticas, organizaciones y la sociedad civil es que la regulación inteligente de la privacidad de los datos puede facilitar el flujo de datos y proteger a los ciudadanos, desarrollando la confianza de los consumidores y los encargados de formular políticas en los bienes y servicios digitales.

Para posibilitar los beneficios destacados en este documento, la GSMA alienta a los gobiernos a observar las siguientes recomendaciones:

Recomendación 1: Comprometerse a facilitar los flujos transfronterizos de datos y a eliminar las medidas de localización innecesarias

Los gobiernos deben asumir el firme compromiso de facilitar los flujos transfronterizos de datos y eliminar las medidas de localización innecesarias a fin de materializar los beneficios de la libre circulación de datos para las personas, las empresas y los gobiernos.

El compromiso público, ya sea a nivel nacional o en el contexto de un órgano regional o multilateral, puede marcar con claridad el rumbo y la visión estratégica para estimular la economía digital a nivel nacional y promover la alineación en toda la región. Cuando se avanza con las medidas de localización, los gobiernos deberían consultar a los interesados sobre cómo se interpretarán e implementarán las medidas.

Recomendación 2: Garantizar que los marcos de privacidad estén preparados para la era digital

Los encargados de formular políticas deben asegurar que los marcos legales atiendan con efectividad las preocupaciones de protección de datos de su país. Estos marcos deben describir los derechos a la privacidad de los ciudadanos y los consumidores y las obligaciones de las organizaciones durante la recolección, análisis, procesamiento y almacenamiento de los datos.

A fin de estar preparados para la era digital, los marcos nacionales de privacidad se deben basar en "el conjunto de principios centrales de protección de datos subyacente a la mayoría de las leyes nacionales y sistemas internacionales [de privacidad]".[18] Estos enfoques deben reflejar las preocupaciones de los consumidores sobre la privacidad y seguridad de los datos[19] y deben operar sobre una base neutral a nivel tecnológico y sectorial para garantizar a los clientes el tratamiento consistente de sus datos. Además, deben contemplar la creación y el uso de una autoridad nacional de protección de datos.

La regulación sobre privacidad se debe focalizar en los riesgos de ocasionar daños a las personas y debe incluir medidas para garantizar la responsabilidad de las organizaciones por la recolección de datos, posibilitando una implementación flexible para que las organizaciones innoven rápido, alcancen una mayor escala y reduzcan sus costos de producción.

Recomendación 3: Revisar las normas sobre privacidad heredadas específicas del sector

Históricamente, fue común que los operadores estuvieran sujetos a restricciones específicas del sector a los flujos de datos internacionales. El objetivo central de los operadores de telecomunicaciones es conectar a las personas, independientemente de la ubicación y la distancia. Si bien las telecomunicaciones comenzaron con telegramas y evolucionaron hasta convertirse en llamadas de voz, SMS y correos electrónicos, hoy en día incluyen el intercambio de datos a escala y la infraestructura y los servicios de los operadores que transportan estos datos. Como los datos son la fuerza que impulsa la economía digital, ya no tiene sentido tratar los datos de los operadores de telecomunicaciones de una forma diferente de los datos generados por otros proveedores de comunicaciones electrónicas o, de hecho, por la economía digital en general. Promulgar un marco de privacidad nacional preparado para la era digital ofrece la oportunidad de revisar las normas sobre privacidad heredadas específicas del sector para garantizar que aún sean aplicables.

Recomendación 4: Promover iniciativas regionales de privacidad de datos

Diversos organismos supranacionales, como APEC y la Unión Europea, adoptaron modelos regulatorios para la protección y la privacidad de los datos mientras aseguran la libre circulación de los datos en toda la región. Estos modelos ofrecen una respuesta proporcional y efectiva para los encargados de formular políticas que desean proteger a los ciudadanos y consumidores y, al mismo tiempo, respaldar el futuro comercio internacional de bienes y servicios físicos y digitales.

Las iniciativas regionales de privacidad de datos se deben promover e implementar sobre la base de principios comunes, deben respaldar los flujos de datos interregionales y deben ser interoperables con los enfoques existentes de APEC y la UE[20] y con enfoques nacionales similares. Las iniciativas regionales crean capacidad regulatoria en privacidad de datos y el desarrollo de las mejores prácticas de la industria para el tratamiento de los datos. Esto establece confianza entre los países, facilita la posibilidad de compartir las mejores prácticas entre los encargados de formular políticas y permite a los reguladores de privacidad de datos detectar y resolver el incumplimiento con mayor facilidad.

El tratamiento consistente de las preocupaciones nacionales de privacidad y seguridad del consumidor a nivel regional facilitará los flujos transfronterizos de datos y ofrecerá mecanismos de gobernanza de datos para garantizar la responsabilidad de la industria a nivel nacional e internacional.

18. CNUCYD, *Data protection regulations and international data flows: Implications for trade and development* [Regulaciones sobre Protección de Datos y Flujos Internacionales de Datos: Implicancias para el comercio y el desarrollo], 2016. Consulte: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
19. Consulte, por ejemplo, las investigaciones sobre privacidad publicadas por la GSMA en 2014: https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf
20. En particular, ser interoperables con las Reglas de Privacidad Transfronteriza (CBPR) de APEC, las Normas Corporativas Vinculantes de la UE (BCR) y el modelo de referencia común asociado desarrollado por un grupo de trabajo conjunto de APEC / UE.

Recomendación 5: Evitar la localización dando un tratamiento pragmático a las preocupaciones de vigilancia extranjera

Más que exigir la localización, los gobiernos deben considerar la variedad de opciones disponibles para la protección de los datos considerados sensibles. Estas opciones incluyen encriptación, anonimización y agregación y, en ciertas circunstancias, pueden incluir la especificación de *hubs* regionales particulares para tipos de datos específicos.

Recomendación 6: Evitar la localización dando un tratamiento pragmático a las preocupaciones de ejecución de la ley y seguridad nacional

Los gobiernos deben participar en iniciativas tales como el protocolo adicional al Convenio sobre Ciberdelicuencia de Budapest, la *US Cloud Act* y la propuesta sobre prueba electrónica de la UE para ofrecer marcos claros y previsibles que otorguen seguridad jurídica a las organizaciones, y acceso más directo y oportuno a los datos en el exterior que necesitan las autoridades, eliminando así la necesidad de medidas de localización.

La adopción de estas recomendaciones:

- Permitirá que la economía digital opere con mayor eficiencia y ofrezca beneficios socioeconómicos más rápido en múltiples naciones y regiones;
- Permitirá que las personas accedan a una variedad y alta calidad de servicios globales, superando restricciones del mercado nacional, si hubiese; y
- Permitirá que las empresas establecidas, incluidos los operadores de telecomunicaciones, adopten estrategias de transformación digital impulsadas por los datos para reducir costos y, por lo tanto, los precios de los bienes digitales y físicos en el mercado.

GSMA LATIN AMERICA
Av. Del Libertador 6810 Piso 15
(Edificio Square Libertador)
C1429BMO, Buenos Aires, Argentina
Teléfono: +54 11 5367-5400