



Empresarios respaldan a OCDE en desarrollo de mecanismo confiable de acceso a datos personales

- *Declaración empresarial conjunta sobre el trabajo del Comité de Políticas de Economía Digital de la OCDE para desarrollar un instrumento que establezca principios de alto nivel u orientación para el acceso fiable de los gobiernos a los datos personales en poder del sector privado*

Felicitamos al Comité de Políticas de Economía Digital de la OCDE (CDEP por sus siglas en inglés) por su esfuerzo por reafirmar la confianza y minimizar las interrupciones en los flujos de datos globales con un conjunto de principios de alto nivel sobre el acceso de los gobiernos a los datos personales en poder del sector privado.

Los miembros de la OCDE comparten intereses comunes en la prevención, investigación y persecución de delitos graves, así como en la respuesta a las amenazas a la seguridad nacional. Los miembros de la OCDE también comparten el firme compromiso de proteger los derechos y las libertades de las personas, incluido el derecho fundamental a la privacidad, cuando el gobierno tiene acceso a los datos personales de los individuos. Si los gobiernos pierden de vista estos valores comunes, hacer negocios puede volverse costoso e inviable para organizaciones de todos los tamaños y sectores, especialmente cuando se restringe la libre circulación transfronteriza de datos, que es esencial para las comunicaciones y operaciones comerciales nacionales y multinacionales.

El "CDEP" tiene la oportunidad de articular principios sobre el acceso confiable del gobierno a los datos personales en poder del sector privado que son comunes a los

miembros de la OCDE con fuertes tradiciones de respeto por los Derechos Humanos y el Estado de Derecho. Puede ofrecer claridad y transparencia respecto a estos valores compartidos, lo que contribuirá a aumentar la confianza entre los gobiernos sobre estos temas, y por otro lado para las empresas y los usuarios de Internet en relación con la suficiente protección que se garantiza cuando los datos de los individuos se transfieren a un tercer país o el gobierno de un tercer país accede a ellos. Un entorno más predecible para los flujos de datos globales permitirá mantener el ritmo actual de transformación digital, en un momento donde la recuperación económica es una prioridad para los gobiernos de todo el mundo.

Como miembros de la comunidad empresarial, apoyamos firmemente este esfuerzo y esperamos 1) contribuir con nuestro punto de vista sobre el impacto económico de la actual falta de seguridad y claridad jurídica, y 2) apoyar la articulación de principios compartidos y salvaguardas importantes para garantizar el acceso gubernamental confiable a los datos personales.

Creemos que los beneficios del comercio dependen del flujo confiable de datos entre países. Por poner un ejemplo, las colaboraciones internacionales en la investigación y las respuestas ante el COVID-19 demuestran cómo estos flujos han permitido nuevos descubrimientos, el intercambio de información, y la colaboración, para ayudar a mitigar la crisis global al permitir una mejor comprensión del virus, el seguimiento de la propagación de la pandemia y la evolución de las diferentes variantes, así como el desarrollo y distribución de vacunas. Al mismo tiempo, los flujos de datos globales han permitido una producción, fabricación y distribución más eficientes de equipo médico, junto con los servicios digitales que son fundamentales para la continuidad de nuestras vidas, comunidades, sociedades y gobiernos.

Sin embargo, vemos cómo la confianza en los flujos de datos internacionales está siendo erosionada por la preocupación de que las demandas de los gobiernos para acceder a datos puedan entrar en conflicto con los derechos humanos y las libertades, incluidos los derechos de privacidad, o incluso violar las leyes nacionales cuando dicho acceso trasciende fronteras. Estas crecientes preocupaciones han conducido a una incertidumbre que puede desanimar a las personas, empresas y gobiernos de participar en la economía global, y puede tener un impacto negativo en el crecimiento económico.

La interrupción de los flujos de datos transfronterizos tiene un impacto significativo en las empresas y economía: Se estima que las transferencias de datos contribuirán con \$2.8 billones al PIB mundial, una cifra que excede al comercio mundial de bienes y se espera que crezca a \$11 billones para 2025. Este valor es compartido por industrias tradicionales como la agricultura, la logística y la manufactura, que alcanzan 75% del valor de las transferencias de datos. Con el 60% del PIB mundial digitalizado para 2022, y el crecimiento en todas las industrias impulsado por los flujos de datos y la tecnología digital, las interrupciones en los flujos de datos transfronterizos tendrán amplias repercusiones que pueden conducir a una reducción de las ganancias potenciales del PIB, desalentar inversiones en los mercados locales, la pérdida de empleos y en consecuencia, la pérdida de bienestar, además del impacto adverso en los ecosistemas digitales locales/nacionales, en un momento en el que la recuperación económica es una de las prioridades de todos los gobiernos.

Consideramos que los tres factores siguientes son los que más contribuyen a esta erosión de la confianza.

1. La preocupación por el acceso de los gobiernos está impactando directamente los flujos de datos globales:

La falta de claridad, transparencia y consistencia entre los enfoques nacionales para el acceso de los gobiernos a los datos ha provocado un crecimiento constante en el número y en la restricción de las medidas para limitar los flujos de datos transfronterizos. Por ejemplo, las diferencias de los enfoques entre la Unión Europea (UE) y Estados Unidos en cuanto a la protección de datos personales han llevado al Tribunal de Justicia de la Unión Europea al fallo del *Comisionado de Protección de Datos contra Facebook Ireland Limited, Maximillian Schrems (Schrems II)*. Algunas interpretaciones de la sentencia ejercen una presión extraordinaria sobre las organizaciones para que restrinjan los flujos de datos transfronterizos entre la UE y otros países. El proyecto de recomendaciones del Consejo Europeo de Protección de Datos señala que las salvaguardas adicionales que se adoptarán cuando se utilicen Cláusulas Contractuales Estándar (SCC por sus siglas en inglés) podrían limitar severamente la capacidad de las empresas para realizar transferencias transfronterizas de datos y, en algunos casos, impedir estas transferencias, con un impacto potencial en operaciones multinacionales en conjunto.

2. Los requisitos obligatorios de localización de datos pueden ser contraproducentes en la práctica:

Las medidas de localización obligatoria de datos afectan tanto a las empresas locales que operan en una sola jurisdicción (por ejemplo, impidiéndoles acceder a productos y servicios globales, cadenas de suministro globales y clientes en mercados extranjeros), como a empresas multinacionales que operan en múltiples jurisdicciones (lo que dificulta, por ejemplo, administrar las funciones de contratación y recursos humanos desde una sola sede, evaluar el desempeño de los vehículos conectados desde un solo centro de investigación y analizar las amenazas de ciberseguridad en diferentes puntos de las redes de comunicaciones).

En todos los sectores, cada vez se despliegan más medidas técnicas para responder a los requisitos obligatorios de localización de datos, incluidas las salvaguardas para intentar limitar el acceso del gobierno a los datos. En algunos casos, estas medidas pueden afectar los beneficios y la funcionalidad de cualquier empresa interconectada globalmente, independientemente de su tamaño. Por ejemplo, pueden impedir que las empresas ofrezcan una amplia gama de características que son de importancia crítica para los consumidores, como las medidas de ciberseguridad, y también pueden evitar el análisis de datos que se originan en múltiples fuentes de una manera que conduce a perspectivas globales y acciones correctivas. En conjunto, estos factores corren el riesgo de minar las economías de escala que están en el centro de la transformación digital, incluyendo la habilitación de las micro, pequeñas y medianas empresas y el crecimiento de los ecosistemas de innovación a nivel nacional.

Los mandatos de duplicación de datos también aumentan el coste de hacer negocios en una jurisdicción al exigir a las empresas que mantengan una copia de seguridad de los datos constantemente actualizada en el país.

Por último, los mandatos de localización de datos obligatorios por parte de los gobiernos no resuelven los conflictos legales existentes entre países que constantemente impiden que las empresas respondan a las solicitudes legítimas de cumplimiento de la ley de un gobierno extranjero. Por el contrario, es probable que agraven esos conflictos, lo que puede poner a las empresas en una posición difícil.

3. La falta de confianza tiene consecuencias sociales más amplias:

La preocupación por el acceso de los gobiernos a los datos personales contribuye significativamente a la reticencia de los sectores públicos a aprovechar los beneficios de la economía digital, a medida que aumentan los temores de que gobiernos de terceros tengan acceso a datos sobre los cuales anteriormente mantenían el control exclusivo.

Por estas razones, enfatizamos en la **urgencia de articular prácticas comunes compartidas por los miembros de la OCDE sobre el acceso gubernamental confiable a los datos personales en poder del sector privado** y creemos que la OCDE se encuentra en una posición única para encabezar este esfuerzo global. El CDEP puede reforzar las sólidas tradiciones de los miembros de la OCDE en el respeto del Estado de Derecho, aliviar la incertidumbre sobre estos temas y como última instancia, ayudar a expandir la confianza en el comercio y las tecnologías digitales. Un instrumento de la OCDE que establezca principios y orientaciones de alto nivel, describiendo las salvaguardas compartidas necesarias para garantizar un estándar alto de privacidad, sería una contribución fundamental para establecer una base firme para generar confianza, similar a las Directrices de Privacidad de la OCDE y sus Recomendaciones del Consejo sobre Inteligencia Artificial.

Concordamos con el enfoque del CDEP sobre las salvaguardas, incluidas las limitaciones de acceso y uso, la transparencia en los informes y la supervisión independiente, que son comunes a los Estados miembros de la OCDE en los contextos de aplicación de la ley y la seguridad nacional. La OCDE también tiene oportunidades para enmarcar estos temas dentro de un marco de políticas de transformación digital más amplio, adoptando un enfoque más holístico que consideraría otros puntos de vista y acuerdos de políticas relevantes.

Una vez que estos cimientos sean firmes, exhortamos a los gobiernos de ideas afines a reconocer los principios identificados por la OCDE como base para los mecanismos políticos y legalmente seguros a largo plazo que apoyan la continuidad y el desarrollo de los flujos de datos internacionales. Además, los gobiernos que apoyen este proyecto deben reconocer la importancia y la necesidad de resiliencia de dichas soluciones y trabajar con los reguladores y las empresas para asegurar una orientación armonizada y pragmática que refleje estos principios comunes a los miembros de la OCDE. Este trabajo colaborativo aumentará la confianza y la certeza regulatoria al dar como resultado una mayor transparencia y comprensión de cómo los gobiernos cumplen con sus compromisos compartidos para proteger la privacidad. Este esfuerzo es fundamental para ayudar a desarrollar soluciones

duraderas y escalables que aborden los obstáculos actuales al flujo transfronterizo de datos confiable en todo el mundo.

Como observó el CDEP en su declaración del 22 de diciembre, "establecer la confianza y minimizar las interrupciones en los flujos de datos es un factor fundamental para aprovechar los beneficios de la digitalización". Apoyamos firmemente este trabajo y estamos listos para brindar información o evidencia relevante para ayudar con su evaluación de las prácticas existentes o el desarrollo de una guía de políticas para el acceso gubernamental fiable a los datos.

Organizaciones de apoyo

Asociación Latinoamericana de Internet (ALAI)

BSA | The Software Alliance

Business at OECD (BIAC)

Cámara Nacional de la Industria Electrónica, Telecomunicaciones e Informática, México (CANIETI)

Coalition of Service Industries (CSI)

Computer & Communications Industry Association (CCIA)

Developers Alliance

DIGITALEUROPE

European Telecommunications Network Operators' Association (ETNO)

Global Data Alliance Information Technology Industry Council (ITI)

International Chamber of Commerce (ICC)

New Zealand Tech Alliance (NZTech)

Slovak Republic National Union of Employers (RUZ)

Social & Economic Research Institute of Malaysia (SERI)

Software & Information Industry Association (SIIA)

US Chamber of Commerce

US Council for International Business (USCIB)