



Declaración sobre el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado

Traducción no oficial

**Instrumentos
jurídicos de la OCDE**



El presente trabajo se publica bajo la responsabilidad del Secretario General de la OCDE. Las opiniones expresadas y los argumentos utilizados en el mismo no reflejan necesariamente el punto de vista oficial de los países miembros de la OCDE.

Tanto este documento, como cualquier dato y cualquier mapa que se incluya en él, se entenderán sin perjuicio alguno respecto al estatus o la soberanía de cualquier territorio, a la delimitación de fronteras y límites internacionales, ni al nombre de cualquier territorio, ciudad o área.

Este documento está disponible de manera gratuita. Puede ser reproducido y distribuido gratuitamente sin necesidad de ningún otro permiso, siempre que no se modifique de ninguna manera. No puede venderse.

Esta es una traducción no oficial. Si bien se ha puesto el mayor empeño para cerciorarse que correspondan con texto original, las únicas versiones oficiales son los textos en inglés y en francés disponibles en el sitio web de la OCDE, <https://legalinstruments.oecd.org>.

NOSOTROS, LOS MINISTROS Y REPRESENTANTES DE todos los Estados miembros de la OCDE y la Unión Europea, reunidos en la isla española de Gran Canaria los días 14 y 15 de diciembre de 2022, bajo el liderazgo de España, que ostenta la presidencia ministerial, y junto con Dinamarca, Japón, Turquía, el Reino Unido y los Estados Unidos, a cargo de las vicepresidencias, con ocasión de la Conferencia a nivel ministerial del Comité de Política de Economía Digital (CDEP) en torno el tema «Impulsar la recuperación a largo plazo y el crecimiento económico mediante la construcción de un futuro digital de confianza, sostenible e inclusivo».

Acceso legítimo de los gobiernos sobre la base de valores comunes

RECORDAMOS nuestro compromiso compartido de defender la democracia y el Estado de derecho, de proteger la privacidad y otros derechos humanos y libertades, de promover la libre circulación de datos con confianza en la economía digital y de mantener una Internet global, abierta, accesible, interconectada, interoperable, fiable y segura.

RECONOCEMOS que la transformación digital en curso está creando más datos, entre ellos datos personales, a medida que las tecnologías digitales se utilizan en todos los sectores de la economía mundial.

RECONOCEMOS ADEMÁS el papel central de los datos en el funcionamiento de nuestras sociedades y economías y que los flujos de datos transfronterizos sustentan el comercio internacional y mundial y la cooperación y el desarrollo económicos; contribuyen enormemente a la innovación y a la investigación y el desarrollo en todos los sectores, y son necesarios para llevar a cabo actividades empresariales y para impulsar objetivos económicos y sociales.

RECORDAMOS la Recomendación de 1980 relativa a las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, revisada por última vez en 2013 [[OECD/LEGAL/0188](#)] (en adelante, «Directrices de privacidad de la OCDE»), que proporciona un punto de referencia común básico para la protección de los datos personales, ya sea en el ámbito del sector público o en el privado, y promueve y facilita los flujos transfronterizos de datos personales al tiempo que defiende los valores democráticos, el Estado de derecho y la protección de la privacidad y otros derechos humanos y libertades.

RECONOCEMOS el deber y la responsabilidad soberanos de todo país de proteger la seguridad de sus ciudadanos mediante la prevención, la detección y la lucha contra las actividades delictivas y las amenazas al orden público y a la seguridad nacional, con arreglo a los valores democráticos, el Estado de derecho y la protección de la privacidad y de otros derechos humanos y libertades.

RECONOCEMOS que el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado está reconocido en nuestros marcos jurídicos nacionales como esencial para cumplir con estos deberes y responsabilidades soberanas, y que las autoridades encargadas de hacer cumplir la ley y de la seguridad nacional están, por lo tanto, facultadas para acceder legalmente a dichos datos.

RECHAZAMOS cualquier enfoque del acceso de los gobiernos a los datos personales en poder de las entidades del sector privado que, independientemente del contexto, sea incompatible con los valores democráticos y el Estado de derecho, y que sea ilimitado, excesivo, arbitrario o desproporcionado. Tales enfoques vulneran la privacidad y otros derechos humanos y libertades, infringen las obligaciones internacionales, socavan la confianza y suponen un grave impedimento para los flujos de datos en detrimento de la economía mundial. Por el contrario, el enfoque de nuestros países sobre el acceso de los gobiernos está en consonancia con los valores democráticos; la salvaguarda de la privacidad y otros derechos humanos y libertades, y el Estado de derecho, que incluye un poder judicial independiente. Asimismo, estas protecciones contribuyen a fomentar la confianza de las entidades del sector privado a la hora de cumplir con sus responsabilidades en este contexto.

DESTACAMOS, teniendo en cuenta las excepciones justificadas a las Directrices de privacidad de la OCDE por razones de orden público y de seguridad nacional, la importancia de reforzar la confianza sobre

la base de un consenso acerca de las protecciones que nuestros países aplican al acceder a los datos personales en poder de las entidades del sector privado en estas circunstancias.

RECONOCEMOS que nuestras prácticas y salvaguardias existentes, a este respecto, aunque no son idénticas entre sí, se basan en principios similares que reflejan un compromiso compartido con la protección de la privacidad y otros derechos humanos y libertades.

TOMAMOS NOTA de los llamamientos de los actores relevantes a que se continúe trabajando y asumiendo compromisos en la identificación de las salvaguardias comunes vigentes en los países miembros de la OCDE para proteger la privacidad y la libertad de expresión y, por lo tanto, promover la confianza, en el contexto de la compra de datos personales disponibles comercialmente, el acceso a los datos personales disponibles públicamente y la recepción de divulgaciones voluntarias de datos personales por parte de las fuerzas del orden y de seguridad nacional.

REITERAMOS nuestra ambición de alcanzar un consenso entre las democracias de ideas afines sobre las protecciones de la privacidad y otros derechos humanos y libertades vigentes en relación con el acceso de las fuerzas del orden y la seguridad nacional a los datos personales en poder de las entidades del sector privado, con el fin de servir de fundamento de los esfuerzos por promover la libre circulación de datos con confianza.

Promover la confianza en los flujos de datos transfronterizos

REAFIRMAMOS nuestro compromiso con la libre circulación de datos con confianza como medio para brindar confianza a los individuos y a las empresas respecto a las transferencias de datos personales a nivel internacional.

CONSIDERAMOS los siguientes principios como una importante expresión de nuestros valores democráticos compartidos y de nuestro compromiso con el Estado de derecho, que distingue a nuestros países de aquellos otros cuyo acceso a los datos personales por parte de las fuerzas del orden o de la seguridad nacional es incompatible con los valores democráticos y el Estado de derecho, ilimitado, excesivo, arbitrario o desproporcionado, o supone una vulneración de los derechos humanos.

RECONOCEMOS que en los supuestos en que nuestros marcos jurídicos exigen que los flujos de datos transfronterizos estén sujetos a salvaguardias, nuestros países tienen en cuenta la aplicación efectiva de estos principios por parte del país de destino como una contribución positiva para facilitar los flujos de datos transfronterizos en la aplicación de dichas normas.

Principios rectores del acceso de los gobiernos a los datos personales en poder de entidades del sector privado

DECLARAMOS que los siguientes principios compartidos reflejan aspectos comunes recogidos en las leyes y prácticas vigentes en los países miembros de la OCDE. Estos principios:

- se complementan entre sí para proteger la privacidad y otros derechos humanos y libertades;
- se aplican al acceso y al tratamiento por parte de los gobiernos de los datos personales que están en poder o control de las entidades del sector privado cuando los gobiernos persiguen fines de orden público y de seguridad nacional dentro de sus respectivos territorios, de conformidad con su marco jurídico nacional, incluidas las situaciones en las que los poderes públicos de un país están facultados, en virtud de su marco jurídico nacional, para ordenar a las entidades del sector privado que proporcionen datos al gobierno cuando la entidad del sector privado o los datos no se encuentran en su territorio (en lo sucesivo, «acceso de los gobiernos»);
- se interpretan con sujeción a los marcos jurídicos nacionales y pueden ser aplicados por los países de diferentes maneras, según el contexto y las circunstancias específicas, como el tipo de acceso que se pretende;
- debe leerse a la luz de las definiciones siguientes:

- a) con «Datos personales» se hace referencia a cualquier información relativa a un individuo identificado o identificable.
- b) el «marco jurídico» rector del acceso de los gobiernos a los datos personales comprende las leyes nacionales, órdenes ejecutivas o judiciales, reglamentos administrativos, jurisprudencia y otros instrumentos o requisitos jurídicamente vinculantes, incluidas las obligaciones legales derivadas del Derecho internacional y supranacional aplicables en el país.
- c) con «entidades del sector privado» se hace referencia a los individuos y a cualquier organización no gubernamental con o sin ánimo de lucro.

Estos principios son:

I. Base legal

El acceso de los gobiernos a los datos personales en poder de las entidades del sector privado está previsto y regulado en el marco jurídico del país, que es vinculante para las autoridades gubernamentales y que ha sido aprobado y es aplicado por instituciones democráticamente establecidas que operan con arreglo al Estado de derecho. El marco jurídico establece los fines, las condiciones, las limitaciones y las salvaguardias en relación con este acceso gubernamental, de modo que los individuos dispongan de garantías suficientes contra el riesgo de uso indebido y abuso.

II. Objetivos legítimos

El acceso de los gobiernos contribuye a la consecución de objetivos específicos y legítimos. Los gobiernos solo pretenden el acceso para tales fines, de conformidad con el Estado de derecho. El acceso de los gobiernos se lleva a cabo de una manera que no es excesiva en relación con los objetivos legítimos y de acuerdo con los principios legales de necesidad, proporcionalidad, racionalidad y otras normas que protegen contra el riesgo de uso indebido y abuso, de conformidad con lo establecido e interpretado en el marco jurídico del país.

Los gobiernos no pretenden acceder a los datos personales con el fin de reprimir o dificultar las críticas o la disidencia, o de perjudicar a personas o grupos únicamente en función de características como, por ejemplo, la edad, la discapacidad mental o física, el origen étnico, la condición de indígena, la identidad o expresión de género, la orientación sexual o la afiliación política o religiosa.

III. Aprobación previa

Los requisitos de aprobación previa (en adelante, «aprobación») para el acceso de los gobiernos se establecen en el marco jurídico para garantizar que el acceso se realiza de acuerdo con las normas, reglas y procedimientos aplicables. Son proporcionales al grado de injerencia en la intimidad y otros derechos humanos y libertades del acceso gubernamental. Dichos requisitos especifican los criterios para solicitar y conceder la aprobación, el procedimiento que debe seguirse y la entidad encargada de aprobar el acceso.

Existen requisitos de aprobación más estrictos para los casos de injerencia más graves, que pueden implicar la necesidad de solicitar la aprobación de autoridades judiciales o no judiciales imparciales. Las excepciones de emergencia a los requisitos de aprobación están legalmente previstas y claramente definidas, con indicación de sus justificaciones, condiciones y duración.

Las decisiones relativas a la aprobación están debidamente documentadas. Se han adoptan de forma objetiva, sobre la base de los hechos, en aras de un objetivo específico y legítimo y tras comprobar que se cumplen los requisitos de aprobación.

En las situaciones en las que no se requiere la aprobación, se aplican otras salvaguardias establecidas en el marco jurídico para proteger contra el uso indebido y el abuso, incluidas normas claras que imponen condiciones o limitaciones al acceso, así como una supervisión efectiva.

IV. Tratamiento de datos

Los datos personales obtenidos a través del acceso gubernamental solo pueden ser procesados y tratados por personal autorizado. Dicho tratamiento y procesamiento está sujeto a los requisitos previstos en el marco jurídico, que incluyen la aplicación de medidas físicas, técnicas y administrativas para mantener la privacidad, la seguridad, la confidencialidad y la integridad de los datos. También prevén mecanismos para garantizar que los datos personales se procesen de forma legal, se conserven solo durante el tiempo autorizado en el marco jurídico a la vista de la finalidad que se persigue y teniendo en cuenta la sensibilidad de los datos, así como que se mantengan exactos y actualizados siempre que sea apropiado habida cuenta del contexto.

Se establecen controles internos para detectar, prevenir y subsanar la pérdida de datos o los supuestos de acceso, destrucción, uso, modificación o divulgación no autorizados o accidentales de datos, y para informar de estos casos a los correspondientes organismos de supervisión.

V. Transparencia

El marco jurídico general que rige el acceso de los gobiernos a los datos es claro y de fácil acceso para el público, de modo que los individuos estén en condiciones de sopesar el impacto potencial de un acceso gubernamental en su privacidad y otros derechos humanos y libertades.

Existen mecanismos para dotar de transparencia al acceso de los gobiernos a los datos personales que equilibran el interés de los individuos y del público a ser informados con la necesidad de prevenir la divulgación de información susceptible de perjudicar la seguridad nacional o el mantenimiento del orden público.

Estos mecanismos incluyen la presentación de informes públicos por parte de los organismos de supervisión sobre el cumplimiento de los requisitos legales por parte del gobierno, así como los procedimientos para solicitar el acceso a los registros del gobierno. Otras medidas consisten, por ejemplo, en la presentación de informes periódicos por parte de los gobiernos y, cuando proceda, en la notificación individual.

Las entidades del sector privado están autorizadas a emitir informes estadísticos agregados sobre las solicitudes de acceso gubernamental de conformidad con el marco jurídico.

VI. Supervisión

Existen mecanismos para una supervisión eficaz e imparcial que garantice que el acceso de los gobiernos a los datos respeta el marco jurídico aplicable.

La supervisión se realiza a través de organismos como oficinas de cumplimiento interno, órganos jurisdiccionales, comisiones parlamentarias o legislativas y autoridades administrativas independientes.

Los sistemas de supervisión de los países están compuestos por estos organismos, que actúan de acuerdo con sus mandatos individuales y entre cuyas facultades se incluye la capacidad de obtener y revisar información relevante, realizar investigaciones o averiguaciones, llevar a cabo auditorías, comprometerse con las entidades gubernamentales en materia de cumplimiento y atenuación, y abordar el incumplimiento. Además, estos organismos reciben y responden los informes de incumplimiento para garantizar que las entidades gubernamentales rindan cuentas, y también pueden ejercer funciones de reparación en respuesta a las quejas de los particulares.

Los órganos de supervisión estarán protegidos de cualquier injerencia en el ejercicio de sus funciones y disponen de los recursos financieros, humanos y técnicos necesarios para desempeñar eficazmente su mandato. Documentan sus conclusiones, elaboran informes y hacen recomendaciones, que se ponen a disposición del público en la medida de lo posible.

VII. Reparación

El marco jurídico brinda a los individuos una efectiva reparación judicial y no judicial para identificar y resarcir las infracciones del marco jurídico nacional.

Tales mecanismos de reparación tienen en cuenta la necesidad de preservar la confidencialidad de las actividades de seguridad nacional y de mantenimiento del orden público. Esto puede implicar ciertas limitaciones a la hora de informar a los individuos sobre si se ha accedido a sus datos o si se ha producido una infracción.

Los medios de reparación previstos incluyen, en función de las condiciones aplicables, el cese del acceso, la supresión de los datos a los que se haya accedido o que se hayan conservado indebidamente, el restablecimiento de la integridad de los datos y el cese del tratamiento ilícito. También pueden contemplar, según las circunstancias, una indemnización por los daños y perjuicios que haya sufrido un individuo.

ACOGEMOS CON SATISFACCIÓN el trabajo de la OCDE sobre la libre circulación de datos con confianza y **PEDIMOS** a la Organización que apoye a los países en sus esfuerzos por promover esta Declaración.