Recomendaciones sobre la política

# El acceso gubernamental a los datos

## La oportunidad

Las tecnologías de nube ofrecen un enorme potencial, no solo para despertar la innovación y la eficiencia, sino también para servir como un lugar seguro para almacenar información confidencial y sensible. Las empresas y los individuos tienen la expectativa razonable de que la información que crean y almacenan en formato digital debe gozar de la misma protección de la privacidad que la información que manejan en papel.

## El desafío

Para luchar contra el crimen y proteger la seguridad pública, los gobiernos tienen una necesidad clara e imperiosa de acceder a los datos digitales. Equilibrar ese interés, con la expectativa de los ciudadanos de un sistema con garantías procesales y estado de derecho, es esencial para mantener la confianza en la tecnología. Esto hace que sea una prioridad crítica elaborar leyes modernas, que proporcionen a los organismos policiales y de seguridad nacional mecanismos apropiados para acceder a la información digital, de conformidad con el proceso legal. Estas leyes deben proteger los derechos fundamentales de privacidad de los ciudadanos, y respetar la soberanía de otras naciones.

Además, la rápida adopción de servicios en la nube, unida al correspondiente aumento de la actividad delictiva transnacional, plantea nuevos retos para la aplicación de la ley. Pero debido a que la mayor parte de las leyes de los países no han seguido el ritmo de la tecnología, hoy en día, cuando la información se mueve a la nube, hay incertidumbre acerca de los marcos legales que regulan el acceso a la información privada.

Además, debido a la falta de marcos internacionales para el acceso a las pruebas digitales, los gobiernos están tomando cada vez más medidas unilaterales para aprovechar la información almacenada fuera de sus fronteras. Esto puede crear conflictos jurisdiccionales irresolubles que

pueden socavar las leyes u obligar a las compañías a tener que optar por ignorar las leyes de un país con el fin de cumplir con las leyes de otro.

En lugar de eludir los mecanismos establecidos para la cooperación transfronteriza, corresponde a los gobiernos a modernizar los sistemas obsoletos y, en caso necesario, crear mecanismos complementarios que funcionen con la eficacia necesaria para afrontar los retos actuales y salvaguardar los valores consagrados por el tiempo, incluyendo la privacidad y los derechos humanos.

## Recomendaciones sobre la política

Para permitir que las fuerzas del orden protejan la seguridad pública, los gobiernos a veces requieren el acceso a la información digital, incluidos los datos almacenados en la nube. Sin embargo, al hacerlo, pueden perjudicar la confianza pública en la computación en la nube.

Por lo tanto, es importante que los gobiernos encuentren un equilibrio entre la seguridad pública por un lado y la privacidad personal y las libertades, por el otro, mediante la adopción de normas legales claras para incautar cualquier evidencia digital. En el desarrollo de estas normas, los gobiernos deben considerar lo siguiente:

**Permitir el acceso a la información digital solo en virtud de procesos legales.** Cualquier marco que regule la capacidad de un gobierno para acceder a la información digital almacenada con proveedores tecnológicos debe empezar por reconocer el principio general de que todo acceso debe ser conforme al estado de derecho.

**Derecho de los proveedores tecnológicos a impugnar.** Los proveedores tecnológicos deben tener la oportunidad de impugnar dicho proceso en nombre de sus clientes para asegurar que los gobiernos están actuando dentro de la ley y que están respetando los derechos de sus usuarios. Esta es una comprobación

crítica en el uso de los poderes de investigación del gobierno, la cual ha demostrado su eficacia en los Estados Unidos.

**Exigir rigor de las formas de los procesos legales de obtención de información más sensible.** Las empresas tecnológicas almacenan al menos tres tipos de informaciones para sus clientes: (1) contenido, que incluye información en los correos electrónicos y otros archivos electrónicos; (2) información sin contenido, que incluye información relativa a un usuario, pero excluye el contenido del usuario; y (3) información de abonado, como la identificación de los detalles sobre el suscriptor de un servicio. El contenido es la categoría más sensible de los datos, ya que contiene la sustancia o el significado de las comunicaciones o documentos de una persona. Por tanto, es conveniente exigir formas más rigurosas de proceso legal, sujeto a niveles adicionales de supervisión judicial, cuando el gobierno busca tener acceso al contenido. Aunque los gobiernos democráticos en todo el mundo van a determinar sus propias normas correspondientes, la exigencia de Estados Unidos de una orden para la toma del contenido emitido por un juez imparcial, basado en una determinación de causa probable, ofrece un modelo que vale la pena considerar.

**Autorizar la divulgación en situaciones de emergencia.** Aunque a los gobiernos solo se les permitirá acceder a la información digital almacenada en la nube a través de procesos legales, en algunos casos excepcionales puede ser apropiado permitirlo en situaciones de emergencia, como cuando hay una base de buena fe razonable para creer que es necesario el acceso para evitar la muerte o lesiones físicas graves. Una excepción de este tipo puede ser especialmente crucial cuando las fuerzas del orden se enfrentan a una emergencia en curso. A pesar de que es probable que las ocasiones en las que este tipo de excepción se requiera que sean relativamente raras (como lo demuestra el informe anual de transparencia de Microsoft, que incluye el número de solicitudes de emergencia que recibe según el país), estas excepciones pueden salvar vidas.

**Apoyar la transparencia.** En los últimos años, la industria tecnológica ha asegurado el derecho de publicar los datos agregados sobre el número y los tipos de solicitudes que recibe para pruebas digitales. Además de las leyes que permiten este nivel de transparencia, los gobiernos deberían permitir que las empresas publiquen información detallada (incluyendo el número de solicitudes recibidas y el número de clientes afectados) con el fin de asegurar que el público pueda entender cómo ejercen los gobiernos su autoridad para investigar la información almacenada en la nube. Las empresas de tecnología han estado publicando información sobre las solicitudes de aplicación de la ley durante años, y en 2014 los nuevos niveles de transparencia por parte de los Estados Unidos ayudaron a demostrar que la información similar acerca de las solicitudes de seguridad nacional puede ser puesta a disposición del público.

**Notificación al usuario.** Excepto en casos limitados, los individuos y las organizaciones tienen derecho a saber cuándo acceden los gobiernos a su información digital. La confidencialidad debería ser la excepción, no la regla. Cuando se requiere confidencialidad, los investigadores deben presentar su caso a una autoridad independiente, como un juez. Los gobiernos deberían estar obligados a proporcionar hechos específicos del caso para justificar cualquier limitación en la capacidad del proveedor de la nube de notificar la solicitud a sus clientes. Es igual de importante que cualquier obligación de confidencialidad impuesta a un proveedor en la nube deba estar limitada en su duración y alcance a los objetivos estrechamente definidos de la investigación específica. Cuando sea necesario, los proveedores en la nube deberían tener permitido impugnar estas órdenes para asegurar que los gobiernos actúan dentro de la ley. A pesar de que sigue siendo insuficiente y que aún necesita mejorar, la legislación estadounidense que regula la emisión de órdenes de secreto de sumario en un caso penal es mejor que las leyes análogas en otros muchos países.

**Modernizar las leyes que rigen los objetivos adecuados de las solicitudes de datos en la nube.** Con cada vez más organizaciones públicas y privadas que transfieren su información digital a la nube y muchas nuevas empresas que utilizan la infraestructura basada en la nube para ofrecer aplicaciones y servicios a los clientes, los gobiernos tienen a menudo múltiples fuentes para la información digital que buscan.

Siempre que sea posible, se deben obtener pruebas digitales de la compañía que ofrece el servicio más directamente a los clientes, lo cual en muchos casos no será el proveedor de la nube. En nuestra opinión, esto puede hacerse a menudo sin poner en peligro una investigación. En situaciones en las que este enfoque obstaculice la investigación, los gobiernos deberían estar obligados, en su lugar, a dirigir el proceso legal al cliente.

**Respetar las fronteras internacionales y la soberanía.** La falta de leyes modernizadas y marcos internacionales para el acceso a las pruebas digitales y el aumento de acciones unilaterales por parte de las fuerzas del orden para aprovechar la información almacenada fuera de sus fronteras amenaza con deteriorar la confianza del consumidor y está creando situaciones legales difíciles para las empresas que prestan servicios en la nube. El proceso de asistencia judicial mutua existente debería modernizarse y reestructurarse para asegurar que pueda continuar sirviendo a su propósito en un mundo moderno. Para ello, los gobiernos deben desarrollar un sistema que otorgue poder a los organismos de aplicación de la ley para combatir las múltiples amenazas a las que nos enfrentamos en la actualidad, desde el terrorismo hasta la ciberseguridad, mientras fortalece las protecciones globales de los derechos humanos y la privacidad, promocionando la libre circulación de la información. Ya se ha hecho un trabajo importante en esta materia por parte de académicos y un pequeño número de gobiernos que tratan de desarrollar un modelo que pueda ser replicado ampliamente.

**Promover la confianza a través de la seguridad.** En los últimos años, las agencias de aplicación de la legislación han argumentado que el cifrado impide investigaciones legítimas por poner la información encriptada fuera de su alcance. Sin embargo, algunas de las soluciones propuestas a este problema, desde el debilitamiento de los algoritmos de cifrado, a órdenes judiciales que proporcionen a los gobiernos claves de cifrado, generan importantes preocupaciones. El cifrado juega un papel importante en la protección de los datos privados contra los hackers y otros agentes maliciosos. Reformas legales o reglamentarias en este ámbito no deben perjudicar la seguridad, un elemento esencial de la confianza de los usuarios en la tecnología.