Leyes inteligentes de privacidad de datos

Cómo lograr los resultados deseados en la era digital

Junio de 2019

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

CONTENIDO

INTRODUCCIÓN 3

FACTORES QUE IMPULSAN LA ADOPCIÓN DE LEYES DE PRIVACIDAD DE DATOS HORIZONTALES 4

PRINCIPIOS RECTORES PARA LAS LEYES INTELIGENTES DE PRIVACIDAD DE DATOS 7

- El contexto local 7
- Marcos de privacidad de datos existentes 8
- Rendición de cuentas 8
- En base a principios 12
- En base a riesgos 13
- Horizontales (neutralidad en cuanto a sector y tecnología) 14
- Equilibrio entre *ex ante* y *ex post* 15
- Datos personales 17
- Consentimiento y fundamentos legales para el procesamiento 18
- Derechos 19
- Notificación de incidentes de seguridad 21
- Flujos transfronterizos de datos 22
- Autoridad de supervisión 24
- Recursos legales, aplicación de la ley y sanciones 25

CONCLUSIÓN 27

ANEXO 1: REFERENCIAS ÚTILES PARA LOS MARCOS DE PRIVACIDAD DE DATOS 28

Introducción

Los gobiernos, que perciben la gran oportunidad que implica la transformación digital, están dispuestos a establecer un ambiente regulatorio que apoye el crecimiento económico impulsado por los datos y, al mismo tiempo, fortalezca la confianza en la tecnología. Muchos países, por lo tanto, están considerando por primera vez establecer leyes de privacidad de datos, mientras que otros están reevaluando sus enfoques existentes.

En la economía mundial de hoy en día, el uso de los datos personales por parte de las organizaciones ya no puede ser contenido ni regulado de manera aislada dentro de un único país. Los marcos futuros que permitirán que los gobiernos, los negocios y, sobre todo, las personas se beneficien de la revolución de los datos deberán respetar las leyes, tradiciones y culturas nacionales. Sin embargo, también deben unirse en torno a un consenso emergente sobre cómo las leyes de privacidad de datos deben proteger la privacidad de las personas y, a la vez, permitir la innovación y los flujos de datos que son fundamentales para la economía digital.

Este documento es un recurso para aquellos involucrados en la elaboración y revisión de normas o legislación en materia de privacidad de datos, tomando lo que se ha aprendido de la implementación de leyes de privacidad de datos hasta la actualidad y resumiéndolo en principios rectores mediante los cuales se puede evaluar una propuesta

En pocas palabras, para que una ley de privacidad de datos sea exitosa, debe proteger de manera efectiva a las personas y, al mismo tiempo, debe darles a las organizaciones la libertad de operar, innovar y cumplir con el marco regulatorio de una manera que sea razonable para sus negocios y asegure resultados positivos en la sociedad. La ley debe estar regida por principios que pongan la responsabilidad de identificar y mitigar riesgos en las organizaciones, manteniéndose flexible y neutral en cuanto a tecnología y sector, y permitiendo que los datos circulen de manera transfronteriza fácilmente.

Sin estos principios rectores, existe el grave riesgo de que la ley o la regulación resultante termine siendo demasiado prescriptiva, demasiado rígida y quede obsoleta rápidamente. En cambio, si estos principios se cumplen, todas las partes interesadas pueden ganar: las organizaciones pueden priorizar sus recursos para lograr resultados de privacidad eficaces y operar e innovar de manera responsable; las autoridades de supervisión[1] pueden usar sus recursos para enfocarse en la prevención de daños; y los gobiernos y las personas pueden disfrutar de manera segura de los beneficios económicos y sociales de la transformación digital.

La privacidad de las personas debe ser el centro de toda estrategia de datos inteligente. Las personas deben poder confiar en el ecosistema digital, los gobiernos y los negocios impulsados por los datos con los que se relacionan a diario. Si las personas confían en las organizaciones que usan sus datos, entonces, los gobiernos y las industrias, incluida la industria móvil, se pueden beneficiar mediante una mayor adopción de tecnología e ideas de negocio nuevas, una mayor actividad económica y una población próspera y digitalizada.

Para lograrlo, se necesita un enfoque inteligente respecto de la privacidad de los datos, que comprenda cuatro áreas clave:

- **Una ley de privacidad de datos** que empodere y proteja a las personas y motive la innovación para beneficiar a la sociedad
- **Organizaciones que cuenten con prácticas de privacidad** que se centren en la minimización de los riesgos de daños a las personas
- **Autoridades de supervisión** que sean capaces de priorizar sus funciones y recursos para enfocarse en los riesgos de daños más apremiantes, instruyendo a las personas y los negocios, fomentando buenas prácticas y haciendo cumplir la ley debidamente
- **Personas** que cuenten con la información y las herramientas necesarias para tomar decisiones informadas sobre cómo se pueden utilizar sus datos y para comprender el intercambio de valor del que participan

Este documento se centra en la primera de esas áreas y pretende guiar a aquellos involucrados en la elaboración o revisión de las normas propuestas en materia de privacidad de datos. Examina los factores que impulsan las leyes de privacidad de datos en general y sus ventajas, y luego expone algunos principios rectores destinados a asegurar resultados de privacidad eficaces para los gobiernos, las organizaciones, la sociedad y, sobre todo, para las personas.

1. En este documento, el término "autoridad de supervisión" hace referencia a cualquier autoridad de protección de datos u otra autoridad que tenga una función de supervisión que cubra las implicancias de la privacidad en el uso de datos.

Factores que impulsan la adopción de leyes de privacidad de datos horizontales

En la era digital, los negocios exitosos recurren a análisis avanzados para obtener información procesable a partir de datos. Muchos de estos datos son datos personales que se corresponden con personas identificables. Los nuevos modelos de negocios, las nuevas tecnologías y las nuevas capacidades, como el Internet de las Cosas (IoT), el análisis de Big Data y la inteligencia artificial (AI), a menudo dependen de un gran volumen de datos personales y, por lo tanto, pueden causar un impacto en la privacidad de las personas. Para concretar los beneficios sociales y económicos de la innovación impulsada por los datos, las personas necesitan tener el poder y la confianza de que sus datos se usarán de manera justa y segura.

Sin embargo, las normas que rigen el uso de datos personales varían considerablemente de un sector a otro, de una tecnología a otra y de un país a otro. Esto puede resultar desconcertante para aquellos que, con razón, esperan la misma protección independientemente de quién use sus datos y cómo los procese.

Además, es posible que las leyes se vuelvan obsoletas rápidamente debido al cambiante y dinámico ecosistema digital, y el tradicional enfoque sectorial es cada vez menos relevante.

Puede que resulte un desafío para las organizaciones transitar este complejo camino regulatorio. Por ejemplo, una empresa que vende dispositivos para hogares inteligentes, como focos de luz, televisores o lavavajillas controlados por Internet, se ve forzada a hacer una distinción entre las normas que cubren a Internet y al comercio electrónico, las que cubren las comunicaciones electrónicas y las que cubren la privacidad de los datos de manera más general. Esto

es especialmente relevante para la industria móvil, ya que se diversifica hacia nuevas áreas y brinda, progresivamente, una plataforma sobre la que pueden prosperar los nuevos modelos de negocios y tecnologías impulsados por los datos.

También se ha puesto de manifiesto que habilitar los flujos transfronterizos de datos en una manera que proteja la privacidad puede beneficiar recíprocamente a la economía y la sociedad. Es por esto que los países están alineando sus enfoques y cooperando más en materia de observancia.

En este contexto, muchos países y organismos regionales de todo el mundo están considerando adoptar, por primera vez, una ley general de privacidad de datos o bien están revisando sus marcos existentes. Ya sea que las economías estén más o menos desarrolladas, más o menos digitalizadas, es probable que la alta intensidad de la actividad legislativa en materia de privacidad de datos continúe durante los próximos años.

A continuación, se exponen algunas de las ventajas que deberían tener en cuenta los encargados de la formulación de políticas públicas y los legisladores.

Las leyes de privacidad de datos horizontales satisfacen intereses fundamentales y consideraciones económicas

Las leyes generales de privacidad de datos han tenido siempre un enfoque doble. Por un lado, su objetivo es proteger los derechos fundamentales de las personas a la privacidad, en especial porque el volumen de los datos personales y la cualidad de la información extraída han aumentado muy rápidamente en las últimas décadas. Sin embargo, siempre se ha reconocido que la capacidad de usar y mover datos personales de manera responsable es importante para la economía y la sociedad. Muchas innovaciones que benefician a las personas se generaron, en parte, gracias a la información recopilada a partir de los datos personales. Por ejemplo, la posibilidad de que las mujeres embarazadas consulten a un médico a través de sus teléfonos celulares en áreas remotas de países pobres puede mejorar tanto la salud individual como la pública. Por ende, una ley general de privacidad de datos puede ayudar a los gobiernos a perseguir oportunidades para el desarrollo sostenible e inclusivo que emerge de la creciente conectividad, la penetración de la banda ancha móvil y la transformación digital.

Las leyes de privacidad de datos horizontales fomentan la confianza

Niveles más altos de confianza en la tecnología digital pueden motivar a las personas a interactuar más con nuevas tecnologías e innovaciones que, por su parte, aumentarán las posibilidades económicas y sociales de un país. Por lo general, una ley de privacidad de datos horizontal les brinda a las personas la protección que necesitan para poder confiar en la tecnología digital sin tener que hacer una distinción entre diferentes tecnologías o sectores. Las personas deben sentir la seguridad de que están protegidas en cualquier situación de procesamiento de sus datos. Esto puede funcionar como una herramienta valiosa para fomentar la confianza.

Las leyes de privacidad de datos horizontales adoptadas en otros países pueden facilitar los flujos transfronterizos de datos y la actividad económica local impulsada por los datos

Ahora que muchos países[2] cuentan con leyes de privacidad o las están adoptando, es posible lograr cierto nivel de consonancia internacional que permita que los gobiernos cooperen y confíen en los marcos regulatorios de sus pares. En particular, las autoridades de supervisión de países que cuentan con leyes generales de protección de datos tienen mayores probabilidades de cooperar de manera efectiva para proteger la privacidad de las personas. Esto aumenta las probabilidades de que los datos puedan circular hacia donde se los necesite, lo que estimula la actividad económica local impulsada por los datos y sus beneficios sociales.

Las leyes de privacidad de datos horizontales brindan una plataforma para mejorar la reputación de los negocios

Los negocios también se benefician de operar en virtud de leyes generales de privacidad de datos. Si las empresas se mantienen en un alto estándar de gobernanza y privacidad de datos, pueden ganar una ventaja competitiva. Al operar en múltiples jurisdicciones, las empresas, a menudo, eligen adoptar un alto estándar mundial, incluso si esto implica que vayan más allá de lo estrictamente exigido en algunos de esos países, debido a que es más eficaz incorporar una cultura de privacidad coherente en toda la organización, y a que ayuda a probar su compromiso con el manejo responsable de los datos frente a terceros, fomentando la confianza y la lealtad a la marca.

2. Según la UNCTAD (Privacidad y Protección de Datos en el Mundo, 1 de abril de 2018), al 1 de abril de 2018, había 107 países que contaban con leyes de privacidad de datos vigentes. Según el profesor Graham Greenleaf (Global Tables of Data Privacy Laws and Bills (5th Ed 2017)) al 1 de junio de 2017, había 120 países que contaban con leyes de privacidad de datos vigentes.

Las leyes de privacidad de datos horizontales reducen la necesidad de que existan normas de privacidad específicas para cada sector

Las leyes generales de privacidad de datos se aplican al procesamiento de todos los datos personales, independientemente de la tecnología o el sector en el que se procesen. Si los gobiernos adoptan una ley de privacidad de datos que se aplique de manera horizontal, también pueden generar una oportunidad para revisar las normas sectoriales anteriores.

Este aspecto es muy relevante para el sector de las comunicaciones, que siempre ha intentado proteger la confidencialidad de las comunicaciones y la privacidad de sus usuarios. Sin un alto estándar de privacidad y confidencialidad, sería difícil para los consumidores confiar en las redes de comunicaciones que usan. En muchos países, esta preocupación de privacidad y confidencialidad se ha codificado en leyes sectoriales o dentro de condiciones de licencias bajo las cuales están obligadas a operar las redes.

Ahora que las comunicaciones se multiplican en Internet y, cada vez más, entre objetos conectados a una variedad de redes, una ley general de privacidad de datos puede establecer normas comunes que todos deben seguir y brindar la oportunidad de eliminar requisitos sectoriales redundantes.

Por ejemplo, la adopción del Reglamento General de Protección de Datos (GDPR)[3] en la Unión Europea provocó una revisión de la "Directiva de Privacidad Electrónica" que regula las comunicaciones y los datos de tráfico.[4] Asimismo, en la India, ciertas condiciones de la licencia para operar que aplican a los operadores de redes móviles abordan aspectos de confidencialidad y privacidad de los datos de tráfico.[5] Dichas condiciones pueden volverse inútiles si se adopta la ley de privacidad de datos propuesta en la India.

3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, del 27 de abril de 2016, 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, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DA
4. Cuando un operador de red móvil presta un servicio de comunicación (incluida la navegación de Internet o la conexión a dispositivos mediante la red celular), la red genera datos sobre el tiempo, la duración, el origen, el destino y la ubicación de la comunicación. A estos datos se los conoce como "datos de tráfico" y también como "metadatos" o "registro de detalles de llamadas" (CDR).
5. Consulte las siguientes secciones de las Condiciones Unificadas de Licencias de la India: 37.1 (privacidad de la comunicación y prohibición de intercepciones no autorizadas), 37.2 (privacidad y confidencialidad de la información relativa a terceros), 37.2 a) (confidencialidad), 37.3 (confidencialidad de la información relativa al consumidor), 37.4 (partes que actúan en nombre del operador), 39.20 (retención de datos), 39.23 (viii) (prohibición de transferencias de información contable del suscriptor o de información del usuario).

Principios rectores para las leyes inteligentes de privacidad de datos

Esta sección expone una serie de principios para guiar la construcción de marcos de privacidad de datos que se adapten a esta era impulsada por los datos. Está destinada, en especial, a aquellos que participan en la propuesta y el análisis de nuevas leyes de privacidad de datos (o revisiones profundas de las leyes de privacidad de datos existentes) en todo el mundo.

El contexto local

Para aquellos que consideren adoptar nuevos marcos de privacidad de datos, el punto de partida debería ser siempre el contexto nacional o regional:

- ¿Cuán importante es la noción de privacidad en la cultura local?
- ¿Cómo afectará la transformación digital los comportamientos y enfoques individuales con respecto a la privacidad?
- ¿Qué dice la constitución de ese país sobre la privacidad o temas relacionados?
- ¿Qué leyes ya se han adoptado en este espacio que reflejen las inquietudes locales?
- ¿Cómo se relacionan las circunstancias económicas locales y los flujos de datos con la privacidad de los datos?

Todas estas preguntas deben tenerse en cuenta al elaborar propuestas de nuevos marcos o leyes de privacidad de datos.

Sin embargo, en sujeción a estas consideraciones nacionales, también debe ser el objetivo de los encargados de la formulación de políticas públicas encontrar la mayor consonancia posible con los marcos internacionales de privacidad de datos para facilitar la interoperabilidad y los flujos transfronterizos de datos que son fundamentales para las economías a escala nacional, regional y mundial.

Marcos de privacidad de datos existentes

Los marcos existentes adoptados por otros países, regiones, organizaciones multilaterales y autoridades de supervisión[6] pueden ser referencias extremadamente útiles para los países que están desarrollando leyes de privacidad de datos por primera vez. Sin embargo, no hay una única solución que sea la panacea. Si bien la ley general de privacidad de datos de la UE, el GDPR, ha recibido especial atención en los últimos años, no es, bajo ningún punto de vista, el único marco, y puede que no sea adecuado en el contexto o el estado de la concepción de privacidad en un país en particular. Por lo tanto, una investigación de marcos existentes debería evitar "copiar y pegar" y, en cambio, hacer un esfuerzo real para encontrar una inspiración apropiada a partir del amplio abanico de marcos existentes. El anexo 1 presenta una lista no exhaustiva de dichos marcos e indica dónde encontrarlos.

Rendición de cuentas

Una ley de privacidad de datos debe incentivar o exigir mecanismos de rendición de cuentas, basándose en las buenas prácticas que existan en otros instrumentos jurídicos.

En lugar de pensar en la privacidad de los datos como en la mera observancia de normas específicas o la adhesión a formalidades administrativas, la noción de "rendición de cuentas" sugiere que las organizaciones deberían adoptar "mecanismos eficaces que aporten una auténtica protección".[7]

Es beneficioso para todas las partes interesadas que la rendición de cuentas se ubique al centro de una ley general de privacidad de datos:

Las **personas** se benefician de la obligación de que las organizaciones vayan más allá de la mera observancia e implementen, en cambio, medidas eficaces para identificar riesgos y prevenir daños. Esto genera resultados de privacidad mucho mejores para las personas, ya que las organizaciones se pueden centrar en lo que realmente importa.

Las **organizaciones** se benefician gracias a que las prioridades operativas se pueden establecer según dónde se genere el riesgo para las personas, fomentando la confianza y permitiendo un grado de flexibilidad para la innovación.

Las **autoridades de supervisión** se benefician puesto que pueden diferenciar las organizaciones que demuestran cumplir con la ley de las que no. Esto también implica que las autoridades ya no tienen la carga de la expectativa poco real de tener que verificar todo. En cambio, pueden utilizar sus recursos de manera estratégica y eficiente en búsqueda de la protección de la privacidad de las personas.

A fin de implementar eficazmente la noción de rendición de cuentas, se necesitan tres elementos clave[8]:

- Rendición de cuentas en la ley
- Rendición de cuentas en la práctica
- Incentivos para la rendición de cuentas

6. Las autoridades de supervisión pueden coordinar su accionar mediante memorandos de entendimiento (MoUs), a través de organismos como la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (ICDPPC) o mediante redes especiales como la Red Global para la Aplicación de la Ley en Materia de Privacidad (GPEN). En este contexto, la Resolución de Madrid emitida por autoridades de protección de datos bajo la ICDPPC (consulte el Anexo 1) puede considerarse como un marco relevante.
7. Opinión del Grupo de Trabajo del Artículo 29 sobre "El Futuro de la Privacidad" (WP168), adoptada el 1 de diciembre de 2009. (El Grupo de Trabajo del Artículo 29 fue el foro en el que se reunieron las autoridades de supervisión de cada Estado Miembro de la UE. Fue reemplazado por la Junta Europea de Protección de Datos del GDPR).
8. Opinión 3/2010 del Grupo de Trabajo del Artículo 29 sobre el principio de rendición de cuentas (WP173), adoptada el 13 de julio de 2010.

La **rendición de cuentas en la ley** se logra cuando la ley exige que las organizaciones implementen medidas adecuadas y eficaces de manera obligatoria, y sean capaces de demostrar el cumplimiento de la ley ante la autoridad de supervisión.

Rendición de cuentas en la ley

1. Obligación de implementar medidas adecuadas y eficaces para asegurar la observancia
2. Obligación de ser capaces de demostrar la implementación de medidas eficaces de observancia

La **rendición de cuentas en la práctica** se logra cuando una organización implementa medidas eficaces para cumplir con los requerimientos de la ley de privacidad de datos. Estas medidas pueden incluir desde el nombramiento de un agente de protección de datos hasta la adopción de procedimientos de evaluación de riesgos y, por lo general, están destinadas a incorporar una cultura de buenas prácticas de privacidad de datos en toda la organización. En aras de la sencillez, estas medidas a menudo se organizan en determinadas categorías funcionales.[9]

Rendición de cuentas en la práctica

Categoría	Ejemplos de medidas
Liderazgo	Participación a nivel de la junta directiva, adopción de estrategia Nombramiento de un agente de protección de datos
Políticas y procedimientos	Políticas para el personal Inventario de datos Procedimiento para la evaluación de nuevos procesamientos Privacidad por diseño
Evaluación de riesgos	Evaluación del impacto de la privacidad de datos
Transparencia	Plantillas de avisos para casos de uso habituales
Capacitación y concientización	Capacitación del personal Orientación en el sitio web
Respuesta y aplicación de la ley	Denuncia de incidentes de seguridad de datos Solicitud de acceso del sujeto y otros derechos Reclamos Procedimiento disciplinario del personal
Monitoreo y verificación	Revisión periódica del programa Auditorías internas o llevadas a cabo por terceros

9. Por ejemplo, liderazgo, evaluación de riesgos, políticas y procedimientos, transparencia, capacitación y concientización, monitoreo y verificación, y respuestas y aplicación de la ley. Consulte, a modo de ejemplo, el enfoque de gestión de la privacidad propuesto por Nymity (*Privacy Management Accountability Framework – A Practical and Operational Structure for Complying with the World's Privacy Requirements*) o el concepto de "Rendición de cuentas de las organizaciones" impulsado por el CIPL (*The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*, Centre for Information Policy Leadership, 23 de julio de 2013).

Los **incentivos para la rendición de cuentas** toman diferentes formas. Si bien las organizaciones ya tienen el incentivo de rendir cuentas debido a la mejora de su reputación y la confianza que pueden fomentar entre sus clientes, también se benefician las autoridades de supervisión y las personas a medida que cada vez más organizaciones toman un enfoque eficaz con respecto a la privacidad. Las leyes de privacidad de datos de vanguardia también deberían, por lo tanto, incentivar prácticas de rendición de cuentas. Esto puede incluir la reducción de requisitos administrativos, como la eliminación de requisitos de registro detallado, la creación de mecanismos para probar la rendición de cuentas (como se menciona anteriormente) o que las autoridades de supervisión tengan en cuenta las buenas prácticas al determinar sanciones.

Los mecanismos como las Normas Corporativas Vinculantes de la UE, las Reglas de Privacidad Transfronteriza de APEC, los códigos de conducta o los esquemas de certificación en virtud de diferentes instrumentos internacionales[10], incluido el GDPR, les brindan a las organizaciones una clara manera de demostrar sus prácticas de rendición de cuentas. Estos mecanismos también pueden ser un incentivo para que las organizaciones adopten prácticas para la rendición de cuentas.

Incentivos para la rendición de cuentas

- Evitar los requisitos de registro detallado para el registro de actividades de procesamiento con la autoridad de supervisión
- Proporcionar mecanismos basados en la rendición de cuentas de manera que se reduzcan las cargas administrativas y puedan funcionar como un sello de aprobación, por ejemplo:
  - Normas corporativas vinculantes
  - Códigos de conducta
  - Certificación
- La ley da lugar a que las prácticas de rendición de cuentas se tomen en consideración al determinar:
  - Si debería iniciarse una investigación
  - El nivel de sanción adecuado en casos de infracción
- Permitir que se pueda recurrir a prácticas o mecanismos de rendición de cuentas en contextos contractuales
- Brindar mecanismos para permitir flujos transfronterizos de datos en base a prácticas de rendición de cuentas

10. Ahora el GDPR admite que la certificación sea reconocida como una posibilidad. También existen otras formas de certificación a través de organismos como la Organización Internacional de Normalización (ISO), que administra un conjunto de estándares para la seguridad de la información (ISO27000). Si bien es posible que estas formas no se centren completamente en la privacidad de los datos, pueden ayudar a una organización a demostrar sus prácticas de rendición de cuentas.

Además, en el contexto de los servicios móviles, están emergiendo diferentes mecanismos de rendición de cuentas. Por ejemplo, las Directrices de Seguridad de IoT de la GSMA[11] ya están ganando un reconocimiento generalizado, y se ha desarrollado una certificación para Dinero Móvil[12] para demostrar a los consumidores y a los reguladores cómo el sistema implementa protecciones efectivas. Otras iniciativas de la industria que requieren algún tipo de rendición de cuentas o adhesión a principios comunes incluyen a Mobile Connect.[13]

Una ley inteligente de privacidad de datos debería:

- Adoptar el concepto de rendición de cuentas incluyendo obligaciones explícitas para que las organizaciones responsables implementen medidas eficaces para cumplir con la ley y ser capaces de demostrar que dichos mecanismos están vigentes.
- Motivar a las organizaciones a adoptar prácticas de rendición de cuentas (por ejemplo, tener una función de privacidad de datos o contar con un agente de protección de datos, llevar registros apropiados, llevar a cabo evaluaciones del impacto de la privacidad de datos e implementar la privacidad por diseño) en la medida que dichas obligaciones acompañen la noción de rendición de cuentas.
- Incorporar disposiciones en la ley para incentivar las prácticas de rendición de cuentas:
  - Deberían evitarse los requisitos de registro detallado de las actividades de procesamiento con la autoridad de supervisión para que las organizaciones lleven registros internos apropiados
  - Debería minimizarse la necesidad de obtener autorizaciones previas, recurriendo, en cambio, a las prácticas de rendición de cuentas
- Permitir que las organizaciones que implementen prácticas de gestión de datos responsablemente se beneficien de mecanismos simplificados para permitirles transferir datos de manera transfronteriza (como las Normas Corporativas Vinculantes, las Reglas de Privacidad Transfronteriza de APEC o las certificaciones).
- Permitir que las prácticas de rendición de cuentas implementadas por una organización sean tomadas en cuenta al evaluar si debería iniciarse una investigación y determinar qué nivel de sanción corresponde.

11. Directrices de Seguridad de IoT de la GSMA: www.gsma.com/iot/iot-security/iot-security-guidelines/.
12. Certificación de Dinero Móvil de la GSMA, abril de 2018: gsmamobilemoneycertification.com.
13. La solución de Mobile Connect de la GSMA: https://mobileconnect.io/ y los Principios de Privacidad de Mobile Connect.

En base a principios

Las leyes de privacidad de datos no deberían ser demasiado prescriptivas. En cambio, deberían operar en base a principios[14], a fin de asegurar la flexibilidad y admitir cambios en las prácticas de los negocios y la tecnología. Asimismo, las leyes deberían centrarse menos en cómo se logra el cumplimiento y más en el resultado deseado. Por ejemplo, es posible que ordenar un estándar de cifrado específico no sea la mejor manera de lograr el resultado deseado de mantener seguros los datos personales. Un estándar técnico especificado en la ley puede quedar obsoleto muy rápidamente. Una ley basada en principios podría lograr el resultado deseado exigiendo que la organización implemente un nivel de seguridad apropiado según la naturaleza de los datos, el contexto en el que se procesan, los más recientes avances en tecnología y prácticas de seguridad de la información, y el costo. Un enfoque en base a principios también ayuda a que los países encuentren una equivalencia esencial entre sus respectivos marcos que pueda apoyar la implementación de mecanismos de flujos transfronterizos de datos.

Existen principios comunes en el centro de muchos marcos de privacidad de datos que tienen una aceptación generalizada, como la imparcialidad y la transparencia, la limitación de la finalidad, la necesidad, la proporcionalidad, la legitimidad del procesamiento de los datos, el periodo de retención limitado, la seguridad de los datos y la garantía de que los datos sean correctos, suficientes y actuales. Este documento no profundiza sobre estos principios, ya que se comprenden razonablemente bien[15]; en cambio, se centra en aquellos elementos de las leyes modernas de privacidad de datos que hacen que estas sean exitosas.

Una ley inteligente de privacidad de datos debería:

- Estar basada en principios y evitar obligaciones demasiado específicas

14. Muchos de los marcos enumerados en el Anexo 1 están basados en principios comunes que pueden atribuirse a los primeros intentos multilaterales por abordar la privacidad: las Directrices de Privacidad de la OCDE de 1980 y el Convenio 108 del Consejo de Europa de 1981.
15. Consulte, por ejemplo, la guía sobre principios de privacidad de la ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. La mayoría de los marcos enumerados en el Anexo 1 incluyen referencias a dichos principios básicos.

En base a riesgos

Las leyes generales de privacidad de datos deberían centrarse en los riesgos de daños a las personas. Las obligaciones o responsabilidades que no se centran en los riesgos de daños crean enfoques de cumplimiento parecidos a una lista de verificación que aportan poco valor a las personas y socavan la credibilidad de la ley. Por ejemplo, el requerimiento de consultar con una autoridad de supervisión cada vez que se utiliza un determinado tipo de datos o de tecnología no tiene en cuenta el contexto del procesamiento ni las protecciones establecidas por la organización. Por lo tanto, impondría una carga innecesaria sobre las organizaciones y saturaría de consultas innecesarias a las autoridades de supervisión. Un enfoque en base a riesgos exigiría que una organización lleve a cabo su propia evaluación de riesgos; en la medida que esté incluida la consulta con la autoridad en dicho marco, la organización estaría obligada a consultar con la autoridad solo en circunstancias excepcionales. Se debería aplicar la misma filosofía en toda la ley de privacidad de datos.

Un enfoque en base a riesgos también incluiría las nociones de privacidad por diseño y de evaluación del impacto de la privacidad de datos. La privacidad por diseño exige que las organizaciones identifiquen y mitiguen riesgos a lo largo de la vida útil de un producto, servicio o proceso. Las evaluaciones del impacto de la privacidad de datos representan un mecanismo que usan las organizaciones para evaluar el impacto que tienen ciertas actividades de procesamiento de datos de alto riesgo en las personas. Puede que sea conveniente que estas prácticas sean obligatorias por ley, ya que habilitan enfoques personalizados en materia de protección de la privacidad, en lugar de imponer un enfoque único y general. Esto evita la necesidad de que la ley establezca disposiciones más prescriptivas.

Una ley inteligente de privacidad de datos debería:

- Adoptar un enfoque en base a riesgos de manera integral
- Asegurar que cada disposición aborde los riesgos de daños a las personas
- Incluir privacidad por diseño y evaluaciones de impacto de privacidad

Horizontales (neutralidad en cuanto a sector y tecnología)

Las leyes generales de privacidad de datos se aplican, usualmente, a cualquier procesamiento de datos personales, independientemente del sector o la tecnología utilizada. Esto es positivo para los consumidores, ya que representa un nivel de protección consistente sin que deban preocuparse por qué tecnología están usando, ni averiguar si la actividad en la que participan cuenta con normas específicas o no.

Un enfoque horizontal beneficia a las organizaciones que hacen uso de datos personales y define un punto de referencia común en la economía de los datos, brindando claridad y facilitando la competencia para todos los participantes.

La incorporación de una ley general de privacidad de datos horizontal presenta la útil oportunidad de que los gobiernos revisen normas sectoriales anteriores.

Esto es particularmente relevante en el sector de las comunicaciones, que siempre ha tenido como eje la preocupación por la privacidad. Ahora que las comunicaciones pueden llevarse a cabo por Internet y, cada vez más, entre objetos conectados a una variedad de redes, una ley general de privacidad de datos puede establecer normas comunes que todos deban seguir. Uno de los resultados beneficiosos de esto es que las normas de privacidad anteriores innecesarias en leyes sectoriales, las pautas o las condiciones de licencias de telecomunicaciones se pueden revisar y eliminar para evitar confusiones.

En el mundo moderno digital, los datos personales deberían estar sujetos a las mismas protecciones, sin perjuicio de si se recopilan en un sitio web, una aplicación móvil, un dispositivo conectado, un establecimiento minorista, o un proveedor de comunicaciones.

✓ Una ley inteligente de privacidad de datos debería:

- Aplicarse de manera horizontal a cualquier procesamiento de datos personales, independientemente del sector o la tecnología utilizada
- Brindar un punto de referencia común para todos los actores del ecosistema digital y la economía impulsada por los datos
- Brindar una oportunidad para que los gobiernos revisen sus normas de privacidad anteriores en leyes sectoriales, pautas o condiciones de licencia de telecomunicaciones y, cuando corresponda, las eliminen

Equilibrio entre *ex ante* y *ex post*

En un mundo digital acelerado, resulta imposible para las autoridades de supervisión analizar todas las actividades de procesamiento de datos por adelantado (“*ex ante*”). Tiene más sentido establecer normas claras e imponerles a las organizaciones la responsabilidad de implementar medidas eficaces y de ser capaces de demostrar cómo cumplen con la ley (consulte la sección de Rendición de cuentas) y, a la vez, mantener el poder de intervención de las autoridades de supervisión en caso de que luego algo salga mal (“*ex post*”). Por ejemplo, el GDPR alejó el régimen de protección de datos de la UE del enfoque *ex ante* y lo acercó a un enfoque *ex post*, reemplazando los requisitos de registro complejos en todos los estados miembros de la UE por la rendición de cuentas y el mantenimiento de registros.

Los beneficios de este enfoque son trascendentales. Habilita a las autoridades de supervisión a solicitar información a las organizaciones para investigar o imponer sanciones o buscar otras medidas de rectificación, de ser necesario. Es importante que también permite a las autoridades de supervisión ser estratégicas en cuanto a cómo establecer sus prioridades y gestionar sus recursos limitados, por lo que pueden centrar su energía en los riesgos de daño a las personas en lugar de las cargas administrativas.

Este enfoque representa una carga significativa para que las organizaciones mantengan buenos registros internos e implementen programas integrales, pero también implica que pueden dirigir su energía a donde estén los riesgos, en lugar de estar ocupadas con tareas administrativas que, a fin de cuentas, no están al servicio de las personas.

Si bien es importante alejarse del enfoque *ex ante* y acercarse a un enfoque ex post, esto no quiere decir que debería abandonarse toda la actividad *ex ante*. A fin de facilitar un sistema de supervisión basado en la rendición de cuentas, las autoridades de supervisión, los agentes de verificación externos y la industria deberán, de todas formas, involucrarse positivamente antes de que comience el procesamiento en ciertos mecanismos. Por ejemplo, puede que las certificaciones y los códigos de conducta que permiten a las empresas y los sectores de la industria demostrar su cumplimiento con la ley necesiten ser analizados antes de que se pueda recurrir a ellos.

Si la ley se centra en mecanismos de rendición de cuentas mediante un enfoque *ex ante*, puede que se deje la responsabilidad diaria de evaluar y evitar los riesgos en manos de las organizaciones, en lugar de crear expectativas poco realistas de que las autoridades de supervisión puedan verificar una instancia de procesamiento por adelantado.

Una ley inteligente de privacidad de datos debería:

- Evitar o minimizar requisitos innecesarios de aprobación previa
- Reemplazar toda obligación de registrar detalles de las actividades de procesamiento de datos con la obligación de llevar registros internos
- Asegurarse de que las obligaciones de mantenimiento de registros no sean demasiado prescriptivas
- Exigir solamente la información mínima y esencial para mantenerse en contacto con las organizaciones, en caso de que se mantenga una obligación de registro
- Centrar la actividad *ex ante* en mecanismos de rendición de cuentas como las certificaciones o códigos de conducta que brindan permisos más generales para el procesamiento de datos

Datos personales

La definición de datos personales debe ser lo suficientemente amplia como para capturar cualquier información mediante la cual se pueda identificar a una persona viva. Así, se evitan múltiples conjuntos de normas y definiciones de datos personales que compiten entre ellas o incluso se contradicen, lo que entraría en conflicto con el principio de "horizontalidad".

La ley debería reconocer que el hecho de que algunos tipos de datos se consideren personales depende de factores como la facilidad con la que se pueden vincular a una persona y de cualquier compromiso que las organizaciones hayan hecho en relación con la vinculación de los datos.

Por ejemplo, puede que un número de teléfono celular o IMEI[16] no parezcan ser, de manera aislada, datos personales, pero si se los combina con datos de cuenta u otra información que tenga el receptor, se podría descubrir la identidad del usuario del teléfono.

Es posible que una ley inteligente de privacidad de datos también reconozca que los datos pueden categorizarse en un espectro de identificabilidad.[17] Los datos anonimizados son, por naturaleza, datos no personales. Los datos seudoanonimizados a partir de los cuales se puede, en potencia, identificar a una persona —por ejemplo, cuando una misma organización tiene un conjunto de datos que posibilita la reidentificación de los datos— se pueden considerar como datos personales. Dado que las actividades de análisis pueden, a menudo, depender del uso de datos seudoanonimizados, las leyes modernas de privacidad de datos han comenzado a definir la seudoanonimización y reconocer que puede ser una protección eficaz para mitigar el riesgo a la privacidad.

Si la ley busca prohibir la reidentificación, debe tenerse especial cuidado para dirigirse solo a aquellos actores que tengan intenciones maliciosas, y contar con un alto umbral de responsabilidad legal. En interés de la seguridad jurídica, también sería conveniente clarificar excepciones, por ejemplo, para la investigación, para las operaciones de negocios diarias, o cuando estén en juego los intereses vitales de una persona.

✓ Una ley inteligente de privacidad de datos debería:

- Incluir una definición de datos personales suficientemente amplia para darle horizontalidad a la ley
- Hacer que la definición de datos personales esté sujeta a una prueba de probabilidad de identificabilidad
- Reconocer que ciertas obligaciones no aplican a los datos seudoanonimizados
- Evitar o establecer un umbral alto para la responsabilidad jurídica con respecto a la reidentificación

16. El número de Identidad Internacional de Equipo Móvil se usa para identificar teléfonos celulares válidos y aquellos que se denunciaron como robados.
17. El Foro del Futuro de la Privacidad ha elaborado material útil sobre el tema de desidentificación y cuán identificables son los datos. https://fpf.org/issues/deid/.

Consentimiento y fundamentos legales para el procesamiento

Una ley general de privacidad de datos debería brindarles a las organizaciones un rango de fundamentos legales sobre los cuales se pueden procesar datos personales. Si bien el consentimiento puede ser apropiado en muchas instancias, la dependencia excesiva del consentimiento puede conducir a la "fatiga por consentimiento", produciendo, así, resultados de privacidad insatisfactorios para las personas. Los usuarios de smartphones, por ejemplo, se han acostumbrado a un aluvión de solicitudes de aplicaciones y otros proveedores de servicios para el consentimiento de la recopilación de datos de sus dispositivos. Si bien esto se puede controlar mediante las preferencias del sistema o los tableros de mando, no es razonable asumir que todos los usuarios tienen el tiempo para considerar plenamente qué términos están aceptando. El retiro del consentimiento de una persona también puede representar una carga poco razonable, por ejemplo, si el consentimiento se puede retirar para actividades relacionadas con la prevención del fraude o la mejora de productos y servicios.

Los servicios responsables basados en análisis de datos serán cada vez más importantes para lograr las metas de políticas públicas e impulsar el crecimiento económico en el futuro próximo. Todo consentimiento del consumidor en este contexto solo podría ser extremadamente general. Por lo tanto, se necesitan fundamentos más flexibles para el procesamiento para permitir que el sector privado y el sector público innoven y, al mismo tiempo, protejan la privacidad de los consumidores.

Estos fundamentos legales adicionales para el procesamiento pueden incluir el procesamiento que sea necesario para el cumplimiento de las obligaciones jurídicas, para la ejecución de un contrato, para proteger los intereses vitales de una persona, y por intereses legítimos del contralor que exija a la organización equilibrar los riesgos e intereses contrapuestos. También debería estar permitido un procesamiento de datos personales más profundo, siempre que sea compatible con el propósito original; y, cuando el consentimiento sea la opción más adecuada, debería existir un rango de maneras en las cuales la organización pueda obtener ese consentimiento.

Una ley inteligente de privacidad de datos debería:

- Reconocer que el consentimiento puede acarrear graves dificultades, como la "fatiga por consentimiento" en ciertas circunstancias
- Evitar depender exclusivamente del consentimiento
- Centrarse también en la transparencia y darles a las personas la información y las herramientas necesarias para que comprendan cómo se procesan sus datos
- Brindar un abanico de fundamentos legales para el procesamiento que incluyan los "intereses legítimos"
- Permitir el procesamiento cuando sea compatible con el propósito original por el cual se recopilaron los datos personales

Derechos

Las personas necesitan derechos claros de privacidad de datos para poder comprender qué datos sobre ellos tiene una organización y ejercer un nivel razonable de influencia sobre el uso de dichos datos. También deben ser capaces de exigir un resarcimiento si no se respetan esos derechos. Este aspecto es clave para que las personas confíen en las nuevas tecnologías y los nuevos modelos de negocios.

Estos derechos pueden incluir los siguientes:

- **Derecho de acceso del sujeto:** es importante que las personas, o los "titulares de los datos", sean capaces de averiguar quién está procesando qué datos personales que los identifican. Este derecho les da a las personas el poder de obtener una copia de toda la información personalmente identificada que una organización tiene sobre ellas.

- **Derecho a la explicación:** si bien las organizaciones han tenido, históricamente, la obligación de brindar información a las personas sobre qué datos recopilan y por qué, esta responsabilidad aparece a veces en la ley como un derecho a que se les explique a las personas cuáles son los procesos y los métodos del uso de los datos. Esto es potencialmente importante en los ámbitos del análisis de datos y de la inteligencia artificial, en los que los algoritmos cumplen un rol clave y pueden resultar difíciles de entender para las personas.

- **Derecho a la objeción:** ante la ausencia de un derecho a la eliminación, darles a las personas el poder de objetar el procesamiento puede ser una herramienta útil para que las personas soliciten que la organización detenga el procesamiento de sus datos.

- **Derecho a la corrección:** puede que las personas solo deseen que los datos incorrectos se rectifiquen. Sin embargo, cuando la organización impugna la solicitada corrección, estos derechos usualmente permiten que la organización continúe con los datos originales, siempre y cuando registren la diferencia de opinión.

- **Derecho a la eliminación:** recientemente, las leyes de privacidad de datos han avanzado, permitiendo que las personas pidan que los datos sobre ellas sean eliminados. Este tipo de derecho a veces se denomina "derecho al olvido".

- **Derecho a la portabilidad de los datos:** el GDPR introdujo un nuevo derecho por el cual las personas pueden solicitar que las organizaciones transmitan datos directamente a otras organizaciones. Las implicancias de la portabilidad de los datos para los individuos y la economía todavía no se conocen plenamente. Por lo tanto, toda propuesta que incluya este derecho deberá considerarse detenidamente.

La anterior lista no es exhaustiva ni excluyente. Cada uno de estos derechos debe considerarse por separado, y las excepciones cuidadosamente elaboradas deben evitar consecuencias no deseadas. Por ejemplo, no se debería exigir que las organizaciones reidentifiquen los datos que no se conservan de manera personalmente identificable ni que establezcan sistemas de datos para el mero propósito de cumplir con las solicitudes de acceso. También debería existir un límite sobre cuán profundo debe ir una organización para desenterrar y ocultar datos, y las organizaciones deberían estar protegidas contra solicitudes repetidas, frívolas o temerarias. Puede que el derecho a la eliminación deba ser equilibrado con excepciones para el interés público, como la protección contra el fraude y la libertad periodística. La portabilidad de los datos puede funcionar como una base interesante para la evolución de las economías digitales e impulsadas por los datos, pero la implementación de este derecho debe ser también consciente del impacto que puede tener en la competencia y las inversiones.

Una ley inteligente de privacidad de datos debería:

- Incluir derechos claros para las personas a fin de que puedan comprender e influir en el procesamiento de los datos y exigir un resarcimiento si algo sale mal
- Comprender el impacto que tendrán los derechos propuestos en todas las partes interesadas, la economía y la sociedad
- Incluir excepciones y limitaciones adecuadas para evitar consecuencias no deseadas

Notificación de incidentes de seguridad de datos

En la UE, hace mucho tiempo que los operadores móviles están obligados a informar incidentes de seguridad de datos a las autoridades. Las obligaciones de notificación de incidentes de seguridad son una herramienta útil para crear consciencia en general, y pueden motivar a las organizaciones a seguir mejorando sus disposiciones de seguridad de datos debido al daño reputacional que causan dichas divulgaciones.

Sin embargo, la notificación excesiva a las personas puede ser contraproducente, ya que conduce a la fatiga y socava la confianza en general. Por lo tanto, si se propone una norma para notificar a las personas sobre estos incidentes, debería aplicarse solamente cuando fuera probable que dicho incidente causará un alto riesgo de daños a las personas afectadas. Por ejemplo, la divulgación pública en Internet de un millón de cuentas bancarias, con sus detalles y contraseñas, ameritaría completamente notificar a las personas afectadas, mientras que sería contraproducente informar la pérdida de un documento que contiene los nombres de los participantes de una reunión de negocios.

El momento de la notificación ante la autoridad de supervisión también puede representar un problema. Las organizaciones necesitan tiempo para determinar si el incidente ha ocurrido y para tomar medidas correctivas. Por lo tanto, un enfoque sensato es establecer un estándar general (por ejemplo, “cuanto antes”, en lugar de una cantidad específica de horas o días) para el momento de notificar el incidente de seguridad de los datos y para que el tiempo empiece a correr una vez que la organización establezca (o haya establecido) que el incidente representa, en efecto, un incidente de seguridad de datos.

Una ley inteligente de privacidad de datos debería:

- Expresar el plazo límite para informar los incidentes de datos mediante un estándar general como “cuanto antes” o “sin demoras indebidas”, en lugar de establecer una cantidad específica de horas
- Delimitar un umbral para informar los incidentes de datos a las personas en base a un alto riesgo de daños a las personas afectadas
- Incluir excepciones para las aplicaciones, los archivos, el hardware o los datos cifrados

Flujos transfronterizos de datos

Las leyes generales de privacidad de datos deberían permitir que los datos personales circulen de manera transfronteriza. Los marcos de privacidad de datos como las Directrices de Privacidad de la OCDE^18, el Convenio 108 del Consejo de Europa[19], el Marco de Privacidad de APEC[20] y las normas de protección de datos de la UE siempre reconocieron que proteger los datos personales va de la mano con permitir el flujo de estos datos. Como se expone en el informe de la GSMA, Flujos transfronterizos de datos: Materializando los beneficios y eliminando las barreras, la GSMA confía en que permitir el flujo de datos y proteger, simultáneamente, la privacidad tiene resultados positivos para la sociedad y la economía.[21] Si cada vez más países se consideran a sí mismos y entre ellos como mercados interoperables "conectados por datos" con normas similares y la capacidad de hacerlas cumplir de manera recíproca, el beneficio será para todos. A la inversa, si los países imponen cada vez más requisitos de localización (lo que se denomina también "soberanía de los datos"), el Internet y los flujos de datos estarán cada vez más fragmentados y aislados. Estas medidas restrictivas podrían tener un efecto devastador en el despliegue de nuevos modelos de negocios, como en los mercados de IoT o de los automóviles conectados, en los que el procesamiento centralizado de los datos recopilados a partir de sensores remotos y, a menudo, móviles es fundamental para su viabilidad. También suponen un impedimento para los servicios de computación en la nube, que los operadores móviles compran —ya que intentan aprovechar la eficiencia de la nube para sus propios propósitos— y brindan, sacando provecho de la nube como oportunidad entre negocios. Por este motivo, la GSMA sostiene que se deberían evitar estas medidas.[22]

Una ley general de privacidad de datos debería brindar una variedad de mecanismos para permitir que los datos circulen[23] y asegurar, a la vez, un nivel adecuado de protección de datos personales. El primer mecanismo es que las organizaciones responsables (consulte la sección de Rendición de cuentas) deberían

18. Directrices de la OCDE (de 1980, con las modificaciones de 2013). Directrices que rigen la protección de la privacidad y los flujos transfronterizos de los datos personales: OECD Guidelines.
19. "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", adoptado por primera vez en 1981 y actualizado en 2018. El convenio cuenta con 54 signatarios, de los cuales 47 son estados miembros del Consejo de Europa y el resto está compuesto por Uruguay, las Islas Mauricio, Senegal, Túnez, Capo Verde, México y Argentina. En 2018, se firmó un protocolo que fortalece el convenio, el cual está actualmente en proceso de ratificación.
20. Marco de Privacidad de APEC (2005): https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.
21. Consulte el informe de la GSMA de 2018: Flujos transfronterizos de datos: Materializando los beneficios y eliminando las barreras: www.gsma.com/publicpolicy/resources/cross-border-data-flows-realising-benefits-and-removing-barriers.
22. Posición del Manual de políticas públicas de telecomunicaciones móviles de la GSMA sobre los Flujos transfronterizos de datos https://www.gsma.com/publicpolicy/mobilepolicyhandbook/consumer-protection#cross-border-flows-of-data.
23. Para obtener una guía útil sobre el rango de posibles mecanismos de transferencia de datos, consulte los Mecanismos de Transferencia Transfronteriza de Datos de Centre for Information Policy Leadership, de septiembre de 2017.

tener permitido transferir datos personales a otras organizaciones, dondequiera que estas se encuentren, siempre que la organización responsable este satisfecha con el nivel de protecciones vigentes. Por otra parte, las organizaciones responsables deberían tener la oportunidad de demostrar la efectividad de sus medidas mediante mecanismos similares a las Normas Corporativas Vinculantes de la Unión Europea, las Reglas de Privacidad Transfronteriza de APEC, las certificaciones o los códigos de conducta. Si se establecen dichos mecanismos, los procesos administrativos deben ser rápidos y sencillos para mejorar las probabilidades de que tengan éxito.

Otro mecanismo es permitir que los datos circulen hacia países que brinden un nivel de protección prácticamente equivalente. La UE y Japón, por ejemplo, accedieron hace poco a reconocer recíprocamente que sus respectivos marcos jurídicos brindan protecciones adecuadas. Se llegó a determinaciones de adecuación similares en relación con una creciente lista de países y con el Acuerdo Privacy Shield UE-EE. UU.[24] Si bien estos mecanismos son un buen catalizador para la aproximación gradual de las leyes de privacidad de datos en todo el mundo, pasará mucho tiempo antes de que la mayoría de los países llegue a determinaciones de adecuación mutuas y, mientras tanto, esto crea una complejidad significativa para las organizaciones que operan en múltiples países.

En la misma línea, el Convenio 108 del Consejo de Europa promueve la adopción de leyes de privacidad de datos en base a un alto estándar común establecido en el convenio. Consecuentemente, y como cuestión de derecho, los países que han ratificado el convenio se pueden beneficiar de un libre flujo de datos entre ellos. De hecho, la UE toma en consideración el estado del Convenio 108 al evaluar sus propias determinaciones de adecuación y el Relator Especial de la ONU sobre la Privacidad de los Datos incentiva a que los estados miembros de la ONU firmen y ratifiquen el convenio.

La ley también puede dar lugar a las transferencias mediante compromisos contractuales, utilizados por las organizaciones, que cumplan un determinado estándar o contengan disposiciones específicas.

Finalmente, los flujos de datos también pueden permitirse sobre la base del consentimiento, aunque esto supone desafíos importantes para las organizaciones cuando, por ejemplo, las personas retiran su consentimiento. Por ende, esta debería ser una opción solo para circunstancias excepcionales o como último recurso.

Una ley inteligente de privacidad de datos debería:

- Brindar una variedad de mecanismos para el flujo transfronterizo de datos
- Permitir que las organizaciones responsables transfieran datos que atraviesen las fronteras o brindar mecanismos para que las empresas responsables demuestren que cuentan con protecciones adecuadas vigentes (autorización, certificación, código de conducta)
- Ser clara con respecto a cuáles son los países que se considera que cuentan con un nivel adecuado de protección
- Permitir flujos de datos transfronterizos sobre la base de cláusulas contractuales o consentimiento
- Asegurar que los procesos administrativos sean mínimos, rápidos y sencillos
- Evitar o prohibir los requisitos de localización (soberanía de los datos)

24. Decisión de Ejecución (UE) 2016/1250 de la Comisión del 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU.

Autoridad de supervisión

Las autoridades de supervisión son un elemento esencial en la aplicación de una ley general de privacidad de datos. Estas pueden crear consciencia, educar a las personas y empresas, motivar buenas prácticas, lidiar con reclamos, realizar investigaciones y tomar medidas para la aplicación de la ley, por lo que son fundamentales para la construcción de la confianza. Según un documento de trabajo redactado por un Excomisionado de Información[25], el rol de una autoridad de supervisión se puede dividir en cuatro funciones diferentes: "líder", "oficial de policía", "gestor de reclamos", y "agente de autorización". A fin de cumplir estas funciones de manera eficaz, la autoridad de supervisión debe ser independiente y no recibir interferencias directas de otras partes del gobierno, y debe contar con las facultades adecuadas en virtud de la ley para accionar, y también con recursos suficientes.[26]

Las autoridades de supervisión pueden financiarse de muchas maneras. Por ejemplo, pueden recibir un presupuesto asignado por parte del gobierno central, o se les puede permitir quedarse con todas las tasas que cobren. En algunos países excepcionales, las autoridades de supervisión se han financiado con las multas que imponen, pero esto conduce al claro peligro de distorsionar las prioridades de la autoridad con respecto a su papel rector.

Las autoridades de supervisión también son intermediarios clave cuando se trata de flujos transfronterizos de datos, ya que deben ser capaces de cooperar para llevar a cabo funciones en nombre de la otra autoridad en el país de destino. En efecto, el sistema de Reglas de Privacidad Transfronteriza de APEC hace hincapié en que las "autoridades de aplicación de las normas de privacidad" deben estar dotadas de facultades y recursos suficientes para cooperar de manera eficaz. La versión actualizada del Convenio 108 refuerza las facultades de las autoridades de supervisión exigiéndoles brindarse asistencia mutua, coordinar investigaciones y llevar a cabo acciones conjuntas. A mayor escala, otras redes como GPEN[27] han tomado la iniciativa en "barridos" coordinados para la aplicación de la ley en múltiples jurisdicciones. Sin esta actividad coordinada de aplicación de la ley, la libertad de compartir datos de manera transfronteriza se vería ciertamente perjudicada.

✓ Una ley inteligente de privacidad de datos debería:

- Facultar a una autoridad de supervisión independiente para la privacidad de los datos
- Conferirle a dicha autoridad de supervisión facultades suficientes para que cumpla sus funciones básicas
- Ordenar que la autoridad de supervisión reciba o sea capaz de recaudar fondos suficientes para llevar a cabo sus funciones
- Evitar la recaudación de fondos a partir de multas
- Motivar la participación de la autoridad de supervisión en actividades transfronterizas de aplicación de la ley

25. Vigilar en Busca de Resultados: Estrategias y prioridades para promover el liderazgo y la construcción de relaciones efectivas, Centre for Information Policy Leadership, 10 de octubre de 2017.
26. El documento estima que, antes del GDPR, los presupuestos de las autoridades de protección de datos en la UE promediaban por debajo de €0,41 por ciudadano o cerca de €8 por negocio con bajas dotaciones de personal. Con la llegada del GDPR, tanto los presupuestos como las dotaciones de personal han aumentado.
27. La Red Global para la Aplicación de la Ley en Materia de Privacidad se formó en respuesta a una recomendación de la OCDE.

Recursos legales, aplicación de la ley y sanciones

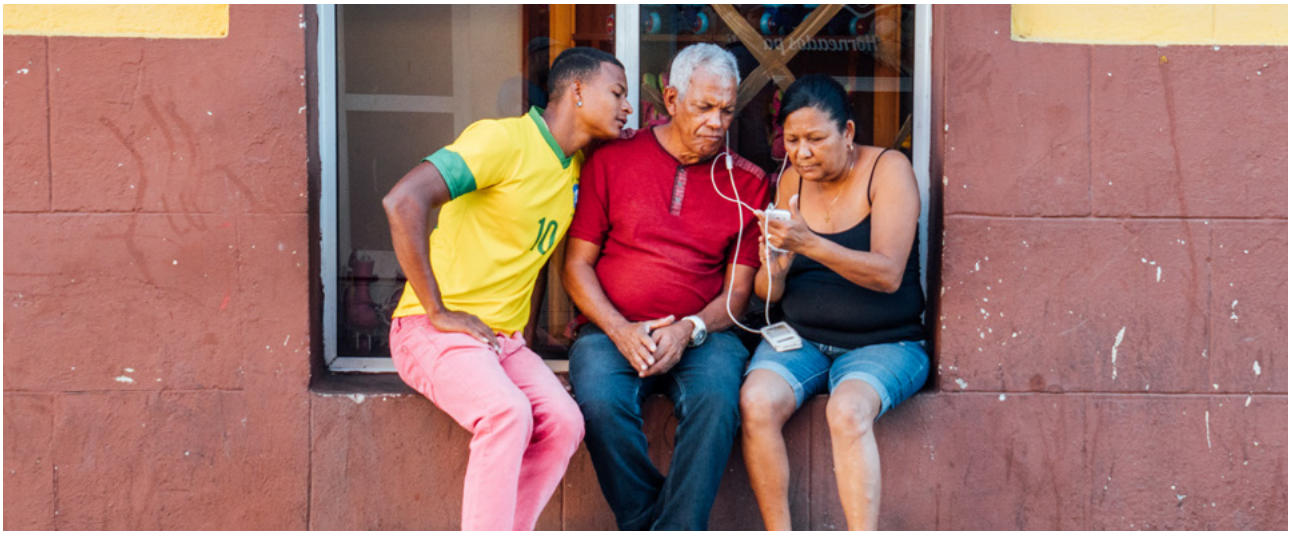
Cuando se infringe la ley, es común que la autoridad de supervisión o los tribunales consideren recurrir a sanciones (ordenar que la organización haga o deje de hacer algo) o a recursos legales (ayudar a que la persona vuelva a la situación en la que estaba antes de que se cometiera la transgresión).

Las sanciones y los recursos legales pueden incluir medidas no monetarias, como ordenar detener el procesamiento o eliminar los datos y, en algunos países, los daños se pueden resolver en los tribunales. Sean cuales fueren los recursos específicos estipulados por la ley, el objetivo de una ley inteligente de privacidad de datos siempre debería ser incentivar las buenas prácticas en primera instancia y, en caso de transgresión, brindar resarcimiento genuino y proporcionado para las personas que hayan sufrido un nivel de daño significativo. Esto evita que las personas deban recurrir a acciones basadas en el derecho privado y protege a las organizaciones contra reclamaciones frívolas. Sin la idea de proporcionalidad o un umbral de daño significativo, es posible que las autoridades de supervisión desperdicien sus recursos y que las personas no gocen de una protección efectiva.

Si se propone imponer multas, estas deben estar limitadas a un nivel razonable y se les debe exigir a las autoridades de supervisión que tengan en cuenta las prácticas responsables del manejo de datos de las organizaciones que rindan cuentas al momento de establecer los niveles de multas o imponer otras sanciones, a fin de incentivar la adopción generalizada de buenas prácticas.

Una ley inteligente de privacidad de datos debería:

- Asegurar que todos los recursos legales provistos por la ley tengan el objetivo de lograr un resarcimiento efectivo para las personas y sean proporcionados al riesgo de daño
- Establecer un umbral de daño adecuado debajo del cual ciertos recursos o reparaciones no estén disponibles
- Incluir un límite razonable para el nivel general en el cual se puede imponer una multa
- Exigir que las autoridades de supervisión tengan en cuenta las prácticas responsables de manejo de datos de organizaciones que rindan cuentas al momento de imponer multas u otras sanciones



Conclusión

Las oportunidades que presenta la transformación digital y las estrategias impulsadas por los datos son significativas. Las nuevas tecnologías y los nuevos modelos de negocios hacen uso de los datos personales para producir beneficios reales para la sociedad y la economía. Estos beneficios se pueden materializar solo si las personas cuyos datos son recopilados y usados pueden confiar en el ecosistema que emerge alrededor de ellas. Consecuentemente, muchos países están aprobando nuevas leyes de privacidad de datos para proteger y empoderar a las personas.

Este documento ha explorado los principios básicos que deberían guiar a aquellos involucrados en la elaboración de nuevas leyes de privacidad de datos. Para que estas leyes sean exitosas, deben proporcionarles a las personas una protección genuina y eficaz y, al mismo tiempo, deben darles a las organizaciones la libertad de operar, innovar y cumplir con el marco regulatorio de una manera que sea razonable para estas últimas. Para lograrlo, deben evitar requisitos administrativos innecesarios que, a fin de cuentas, no están al servicio de las personas, y deben evitar ser demasiado rígidas o prescriptivas. En cambio, las leyes de privacidad de datos deberían poner la responsabilidad de identificar y mitigar riesgos en las organizaciones, manteniéndose flexibles y neutrales en cuanto a tecnología y sector, y permitiendo que los datos circulen de manera transfronteriza fácilmente.

Sin estos principios rectores, existe el grave riesgo de que la ley o la regulación resultante termine siendo demasiado prescriptiva, demasiado rígida y quede obsoleta rápidamente. En cambio, si estos principios se cumplen, todas las partes interesadas se pueden beneficiar: las organizaciones pueden priorizar sus recursos para lograr resultados de privacidad eficaces y operar e innovar de manera responsable; las autoridades de supervisión pueden usar sus recursos para enfocarse en la prevención de daños; y los gobiernos y las personas pueden disfrutar de manera segura de los beneficios económicos y sociales de la transformación digital.

✓ Una ley inteligente de privacidad de datos es aquella que:

- Toma la ley, las tradiciones y las culturas nacionales y locales como punto de partida
- Se encuentra en consonancia con las normas y los marcos de privacidad de datos internacionales existentes
- Se basa en el concepto de rendición de cuentas
- Se basa en principios flexibles en lugar de requisitos excesivamente prescriptivos
- Se basa en la prevención o limitación del riesgo de daños
- Se aplica de manera horizontal, sin referencia a un sector o tecnología específicos
- Logra el equilibrio justo entre ex ante y ex post
- Cuenta con una definición de “datos personales” que se ajusta a las definiciones internacionales
- Brinda un rango de fundamentos legales flexibles para el procesamiento y reconoce las dificultades que plantea el consentimiento
- Incluye un rango de derechos que empodera a las personas
- Toma un enfoque pragmático con respecto a las notificaciones de violaciones de datos
- Promueve los flujos transfronterizos de datos
- Establece una autoridad de supervisión independiente para la privacidad de los datos
- Brinda un rango de recursos legales, medidas de aplicación de la ley y sanciones que es proporcionado con respecto al daño causado y que tiene en cuenta las buenas prácticas de una organización

Anexo 1: Referencias útiles para los marcos de privacidad de datos

Organización	Título	Link
Cooperación Económica Asia-Pacífico	**Marco de Privacidad de APEC (2005)**	Marco de Privacidad de APEC https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
Unión Africana	**Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (2014)**	Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
Asociación de Naciones del Sudeste Asiático	**Marco de la ASEAN sobre la Protección de Datos Personales (2016)**	Marco de la ASEAN sobre la Protección de Datos Personales https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf
Consejo de Europa	**Convenio 108+ (de 1981, con las modificaciones de 2013-2016)** Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, con el Protocolo CETS n° 223 que lo modificará.	Convenio 108+ https://rm.coe.int/16808ade9d
Unión Europea	**GDPR (2016)** Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y el Consejo (27 de abril de 2016)	GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj
Organización para la Cooperación y el Desarrollo Económicos	**Directrices de la OCDE (de 1980, con las modificaciones de 2013)** Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales	Directrices de la OCDE https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
Comunidad de Desarrollo de África Austral	**Ley Modelo de la SADC (2013)** Protección de Datos: Ley Modelo de la SADC	Ley Modelo de la SADC https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf
Red Iberoamericana de Protección de Datos	**Estándares Iberoamericanos de Protección de Datos Personales (2017)** Estándares de Protección de Datos Personales para los Estados Iberoamericanos	Estándares Iberoamericanos de Protección de Datos Personales http://www.redipd.es/noticias_todas/2017/novedades/common/Estandares_eng_Con_logo_RIPD.pdf#Texto%20en%20inglés
Comunidad Económica de Estados de África Occidental	**Ley Complementaria de la ECOWAS (2010)** Ley Complementaria A/SA.1/01/10 sobre la protección de datos personales dentro de la ECOWAS	Ley Complementaria de la ECOWAS https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf
GSMA	**Principios de Privacidad Móvil de la GSMA (2011)** Promoviendo la privacidad de los consumidores en el ecosistema móvil	Principios de Privacidad Móvil de la GSMA https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf
Conferencia Internacional de Comisionados de Protección de Datos y Privacidad	**Resolución de Madrid (2009)** Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal	Resolución de Madrid https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

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