¿Quién defiende tus datos en América Latina y España?

UNA VISIÓN COMPARATIVA DE LOS COMPROMISOS DE LAS EMPRESAS DE TELECOMUNICACIONES CON LA PRIVACIDAD

ELECTRONIC FRONTIER FOUNDATION

Autora: Veridiana Alimonti
Editora: Karen Gullo

La Directora de Políticas para la Privacidad Global de la EFF, Katitza Rodríguez, revisó este informe. La Directora de Diseño de la EFF, Kim Carlson, junto con el Director de Arte de la EFF, Hugh D' Andrade, han dado formato a este informe. Carlos Wertheman ha traducido este informe al español. También damos las gracias a todas las organizaciones asociadas en el proyecto ¿Quién defiende tus datos?/¿Dónde están mis datos? por la serie continuada de informes y años de colaboración. Estas organizaciones son: Fundación Karisma, Hiperderecho, R3D, InternetLab, Derechos Digitales, TEDIC, ADC, Eticas e IPANDETEC.

Una publicación de la Electronic Frontier Foundation, 2023.

View this report online:
https://www.eff.org/es/wp/who-defends-your-data-latin-america-spain-comparative-view-telecom-companies-commitments-user

¿Quién defiende tus datos en América Latina y España?

UNA VISIÓN COMPARATIVA DE LOS COMPROMISOS DE LAS EMPRESAS DE TELECOMUNICACIONES CON LA PRIVACIDAD

VERIDIANA ALIMONTI
Associate Director for Latin American Policy

MAY 2023

Introducción

Este informe presenta una visión general y un análisis comparativo de la serie de informes ¿Quién defiende tus datos?/¿Dónde están mis datos? para Argentina, Brasil, Chile, Colombia, México, Nicaragua, Panamá, Paraguay, Perú y España. Desde 2015, las organizaciones locales de derechos digitales han evaluado los compromisos de las empresas de telecomunicaciones con la transparencia y la privacidad de los usuarios y usuarias en una iniciativa regional inspirada en el proyecto Who Has Your Back (Government Data Requests) de la EFF.

Los proveedores de servicios de Internet y telefonía tienen acceso a información sensible y privada de los usuarios que detalla gran parte de sus actividades diarias: desde qué vídeos comparten en las redes sociales, qué sitios web visitan y cuándo inician sesión en servicios en línea, hasta su paradero fuera de línea a través de los datos de localización. Esto puede revelar detalles íntimos de la vida, los movimientos, las acciones, las relaciones, los hábitos y los intereses de los usuarios. Los organismos gubernamentales y policiales solicitan a menudo a las empresas de servicios de Internet y telefonía que faciliten información sobre las personas usuarias. Las decisiones que toman las empresas para responder a estas peticiones afectan a la privacidad de cada uno de sus usuarios, y la forma en que generalmente recopilan, utilizan y comparten la información de las personas usuarias es vital para garantizar sus derechos. Por ello, deben contar con políticas y prácticas de protección y transparencia lo más estrictas posible para proteger los datos de las personas de una vigilancia gubernamental y empresarial injustificada y desproporcionada.

Según las normas internacionales de derechos humanos, las empresas tienen la responsabilidad de garantizar que sus prácticas respetan los derechos fundamentales, incluido el derecho a la intimidad. Esa responsabilidad existe independientemente de que un Estado cumpla sus propias obligaciones en materia de derechos humanos. Como señaló la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos

> *Cuando los gobiernos exigen a las empresas que les proporcionen acceso a los datos en contravención de las normas internacionales de derechos humanos, las empresas deben tratar de honrar los principios de derechos humanos en la medida de lo posible, y ser capaces de demostrar sus iniciativas en curso para hacerlo. Ello puede entrañar interpretar las demandas del gobierno de la manera más restringida posible, pedir aclaraciones a un gobierno en relación con el alcance y el fundamento jurídico de la demanda, requerir una orden judicial antes de acceder a las peticiones de datos del gobierno, y comunicar de forma transparente a sus usuarios los riesgos y la aceptación de las demandas del gobierno.*

Con estos estándares en mente, se han realizado informes *Quién defiende tus datos* (QDTD) en 10 países para empujar a los proveedores de telecomunicaciones a adoptar las mejores prácticas de privacidad y protección de datos.

La red clave de organizaciones que han dirigido los informes locales a lo largo de los años incluye:

Fundación Karisma (Colombia), primera edición publicada en 2015.

Hiperderecho (Perú), primera edición publicada en 2015.

R3D (México), primera edición publicada en 2015.

InternetLab (Brasil), primera edición publicada en 2016.

Derechos Digitales (Chile), primera edición publicada en 2017.

TEDIC (Paraguay), primera edición publicada en 2017.

ADC (Argentina), primera edición publicada en 2018.

Eticas (España), primera edición publicada en 2018.

IPANDETEC (Panamá y Nicaragua), primera edición publicada en 2019 y 2020, respectivamente.

Con cuatro secciones, este informe expone las principales conclusiones de los estudios de nuestros aliados desde una perspectiva amplia y regional. En la primera sección se explican los principales criterios del proyecto, se ofrecen datos generales sobre los resultados a lo largo de los años y se comparan los resultados de las empresas de telecomunicaciones regionales y/o mundiales en los países cubiertos por el proyecto. La segunda sección examina lo que los informes QDTD revelan sobre las tendencias problemáticas y los retos de la región en relación con la tan necesaria aplicación de las normas de derechos humanos al acceso de los gobiernos a los datos. La tercera sección analiza brevemente los avances y los puntos débiles de las empresas en los marcos de protección de datos, tal y como se reflejan en los informes. Por último, la cuarta sección esboza las conclusiones y recomendaciones.

1. Una visión general de los informes QDTD

1.1. Metodología y principales criterios comunes

Los informes QDTD en América Latina y España se centran principalmente en los proveedores locales y regionales de servicios de telecomunicaciones y banda ancha. Los informes se centran en los mercados nacionales y pretenden impulsar a las empresas a adoptar compromisos firmes en materia de privacidad de los usuarios para obtener una ventaja competitiva, ya que los clientes están cada vez más preocupados por la protección de datos. Algunas de las empresas mencionadas son grandes operadores regionales o mundiales que prestan servicios a través de sucursales o filiales locales, como Telefónica (Movistar/Vivo), América Móvil (Claro), Millicom (Tigo) y AT&T (DirecTV). Otros son proveedores de Internet locales e independientes.

La publicación de un informe QDTD requiere mucho trabajo. En primer lugar, los expertos y expertas de las organizaciones locales asociadas identifican los principales proveedores de servicios de Internet (ISP) locales y, a continuación, examinan las condiciones de servicio, las políticas de privacidad, los informes de transparencia y las directrices para el cumplimiento de la ley que están a disposición del público. Además, los expertos y expertas se ponen en contacto directo con las empresas para recabar más detalles y opiniones sobre sus políticas. Este compromiso también les permite vigilar si las empresas luchan por sus usuarios y usuarias en los tribunales, el Congreso y los debates de política pública.

Los criterios de evaluación se adaptan a las leyes y realidades locales, y las empresas reciben puntuaciones, normalmente estrellas, por sus mejores prácticas y compromisos. Las estrellas se otorgan generalmente sobre la base de información públicamente disponible a la que cualquier persona que accede a la Internet puede acceder y verificar. El cumplimiento parcial de las prácticas y políticas evaluadas da lugar a estrellas parciales, según la metodología de cada informe.

Los criterios de evaluación suelen cambiar de un país a otro. No obstante, los criterios se centran en tres aspectos principales: el compromiso público de cumplir las salvaguardias de privacidad; la adopción de prácticas y políticas favorables a las personas usuarias; y la transparencia. En general, los parámetros evalúan:

Políticas de protección de datos: ¿Tiene la empresa una copia de su contrato de servicios de internet y/o de su política de protección de datos publicada en su página web? A lo largo de los años, los informes han hecho más estricta la evaluación, detallando la información específica que los proveedores de servicios de internet deben facilitar en sus políticas.

Transparencia: ¿Publica la empresa regularmente un informe de transparencia? Los parámetros evaluados varían, pero muchos informes comprueban si la empresa revela el tipo de datos del usuario solicitados (contenido, metadatos, datos de identificación del abonado, datos de localización, ID de dispositivos, entre otros), junto con el número agregado de solicitudes gubernamentales que el ISP recibió, cumplió y rechazó.

Directrices para la aplicación de la ley: ¿Publica la empresa el procedimiento, los requisitos y las obligaciones legales que debe cumplir el gobierno cuando solicita información personal sobre sus usuarios y usuarias?

Autorización judicial: ¿Se compromete la empresa a aplicar la legislación local según la interpretación más protectora de las salvaguardias legales, como exigir una orden judicial antes de entregar los datos de la persona usuaria a las autoridades?

Notificación a los usuarios: ¿Se compromete la empresa a notificar a los usuarios y usuarias las solicitudes gubernamentales de información, y/o toma medidas concretas para que las personas usuarias puedan recibir dicha notificación?

Compromiso con la privacidad en los tribunales/sedes legislativas o políticas: ¿Ha defendido la empresa la privacidad y protegido activamente los datos de las personas usuarias, ya sea en los tribunales o como parte de un debate legislativo en el Congreso?

Seguridad digital: ¿Adopta la empresa medidas de seguridad digital adecuadas? Algunos informes QDTD comprueban el uso del cifrado (HTTPS) en los canales de comunicación y las funcionalidades de pago de los ISP. A lo largo de los años, algunos informes también han comprobado si los ISP adoptan otras medidas de seguridad, ofrecen contenidos de seguridad digital y publican las políticas de la empresa en materia de ciberseguridad y/o violación de datos.

1.2. Logros y deficiencias más destacadas

Las evaluaciones han evolucionado desde las primeras ediciones del proyecto. Aunque algunos parámetros se han convertido en buenas prácticas consolidadas del sector (por ejemplo, la publicación periódica de informes de transparencia) o en obligaciones legales específicas (por ejemplo, publicar las políticas de protección de datos), el rendimiento de algunas empresas sigue siendo deficiente, y la mejora en algunas categorías sigue siendo un reto persistente. Esta sección describe lo que podemos captar en los últimos años a partir de los esfuerzos de los informes QDTD y de otras iniciativas[1] destinadas a presionar a las empresas para que defiendan los derechos humanos y la privacidad y aboguen por avances fundamentales en la legislación y la jurisprudencia.

Políticas de protección de datos

Las leyes de protección de datos que establecen obligaciones de transparencia sobre el tratamiento de los datos de las personas usuarias desempeñan sin duda un papel relevante a la hora de conseguir que las empresas revelen información sobre cómo recopilan, utilizan y comparten los datos personales y de comunicación de sus usuarios y usuarias. Sin embargo, los informes de la QDTD han mostrado una relación desigual entre las obligaciones legales y las mejores prácticas para esta categoría de evaluación.

La existencia de marcos de protección de datos en vigor no se corresponde necesariamente con políticas de protección de datos accesibles, fáciles de entender y exhaustivas. Las tres primeras ediciones publicadas en 2015 procedían de países con leyes de protección de datos en vigor (Colombia, México y Perú). Y en los tres informes, las empresas obtuvieron malas puntuaciones, ya sea por tener políticas difíciles de encontrar o entender, por no incluir información relevante sobre el tratamiento de datos personales o por no publicar ninguna política.

[1] Podemos citar, por ejemplo, los informes Global Network Initiative (https://globalnetworkinitiative.org/) y Ranking Digital Rights (https://rankingdigitalrights.org/).

Con el tiempo, los informes QDTD han mostrado avances significativos no solo en *qué* información proporciona los ISP, sino también en *la forma en que* proporcionan esa información. Por ejemplo, la gran mayoría de las empresas evaluadas en Brasil tienen ahora *Centros de Privacidad* o *Portales de Privacidad* que reúnen detalles relevantes sobre la privacidad de las personas usuarias y el tratamiento de datos, y muestran esa información de una forma más fácil de usar. Telefónica y América Móvil ponen a disposición dichos portales en sus sitios web locales en los distintos países en los que operan, aunque América Móvil todavía no lo hace en todos los países cubiertos por los informes QDTD. La sección 1.4 detalla esta disparidad regional. El último informe de ADC Argentina señala, sin embargo, que las empresas aún pueden mejorar a la hora de organizar la información en dichos portales para asegurarse de que las personas usuarias no tengan que navegar por varias secciones para acceder a lo que es más relevante para ellas.

En España, el informe de Eticas, tras la aplicación del Reglamento General de Protección de Datos (RGPD) de la UE y la Ley Orgánica española 3/2018 relacionada, indicó cambios positivos significativos en el contenido de las políticas de las empresas disponibles en línea. Algunas empresas, por ejemplo, proporcionan detalles de contacto para los funcionarios de protección de datos y revelan sus prácticas con respecto a la toma de decisiones automatizadas y/o la elaboración de perfiles basados en datos. Por el contrario, a pesar de la presencia de leyes de protección de datos en vigor en Panamá y Nicarágua, los ISP de estos países no publican políticas exhaustivas de privacidad de datos para sus servicios de telecomunicaciones e Internet. En muchos casos, las políticas, cuando están disponibles, solo se refieren a la recopilación de datos a través de los propios canales de comunicación de los ISP, como sitios web y aplicaciones. Ni siquiera las políticas globales de protección de datos de Millicom y América Móvil se encontraban en los sitios web de las sucursales locales de Panamá y Nicaragua. Por otro lado, los informes de TEDIC sobre Paraguay han mostrado mejoras en esta categoría a lo largo de los años, a pesar de la ausencia de una legislación integral de protección de datos.

Por fin, el último estudio de Hiperderecho en Perú comprobó si las empresas de telecomunicaciones publicaban políticas o proporcionaban canales de atención al cliente en lenguas nativas, como el quechua y el aymara. El desequilibrio fue evidente en los resultados. Mientras que las cuatro empresas destacadas recibieron estrellas completas por sus políticas generales de protección de datos en español, solamente Telefónica-Movistar obtuvo una puntuación completa en la categoría de lengua nativa.

⇨ Consulte con más detalle la información proporcionada en las políticas de privacidad/protección de datos evaluadas en **la sección 3**.

Informes de transparencia y directrices para la aplicación de la ley

Los *informes de transparencia* de las empresas suelen revelar información estadística y distintos niveles de información cualitativa sobre las solicitudes gubernamentales de datos de usuarios durante un periodo concreto en los países y/o regiones en los que operan. Las *directrices de aplicación de la ley* (directrices LE) establecen los pasos que deben seguir las autoridades para solicitar datos de las personas usuarias y que las empresas deben seguir a nivel local a la hora de responder a las autoridades. En los informes de transparencia y en las directrices de aplicación de la ley se puede encontrar la legislación local aplicable sobre peticiones gubernamentales, tipos de datos de personas usuarias solicitados, autoridades competentes para solicitar datos, y

perspectivas sobre cómo interpretan las empresas la legislación y las salvaguardias locales, aunque el objeto principal del informe y de las directrices sea distinto.

La investigación del QDTD indica que la publicación de informes de transparencia es tanto una práctica asentada como una laguna persistente, dependiendo del ISP o país que consideremos (véanse más detalles en la sección 1.4).

En cuanto a las principales empresas de telecomunicaciones de la región, podemos destacar que:

- **AT&T (incluida DirecTV),** una empresa con sede en Estados Unidos que opera a nivel mundial a través de filiales en muchos países, publica informes de transparencia desde al menos 2015. El último informe publicado (sobre solicitudes en 2021/2022) es bastante detallado sobre las demandas legales relacionadas con Estados Unidos, pero proporciona muy poca información sobre las solicitudes recibidas por sus filiales en otros países. La sección sobre México es una excepción positiva: el ISP da algunas pinceladas sobre el marco legal mexicano para las exigencias de datos, incluidas las escuchas telefónicas y las solicitudes de información histórica y de localización en tiempo real. Desglosa los datos estadísticos de las solicitudes de las fuerzas de seguridad en peticiones de información histórica (datos de identificación de abonados, registros detallados de llamadas, información de localización de la celda de red móvil a cual se ha conectado un dispositivo y datos de identificación de dispositivos móviles), información de localización en tiempo real y escuchas telefónicas. También revela el número de demandas rechazadas/impugnadas o parcialmente respondidas. Lamentablemente, para todos los demás países de América Latina y más allá, AT&T solo proporciona el número de solicitudes de datos recibidas.

- **Telefónica (Movistar/Vivo)** publica informes globales de transparencia desde al menos 2016. El último informe publicado (sobre solicitudes en 2021) desglosa información estadística sobre las solicitudes de las autoridades gubernamentales *por país* y por los siguientes indicadores: interceptaciones legales (incluidas las solicitudes de nuevas interceptaciones, ampliaciones o para desconectar una interceptación existente), acceso a metadatos, bloqueo y restricción de contenidos, suspensión geográfica o temporal del servicio, solicitudes denegadas o parcialmente atendidas y número de accesos afectados por cada solicitud. El informe de Telefónica también especifica las autoridades competentes y las leyes aplicables para cada tipo de solicitud en cada país.

- **Millicom (Tigo)** ha publicado informes globales de transparencia desde al menos 2016. El último informe publicado (sobre solicitudes en 2022) revela tipos y números de solicitudes de aplicación de la ley recibidas *por región*, no por país, en las siguientes categorías: interceptación, metadatos de clientes y datos financieros de clientes (relacionados con los servicios financieros móviles que presta el ISP). La empresa no revela el número de solicitudes rechazadas o atendidas. Millicom agrupa los datos de los países en los que opera el ISP en dos bloques: *América del Sur* (Bolivia, Colombia, Paraguay) y *América Central* (Costa Rica, El Salvador, Guatemala, Nicaragua, Honduras, Panamá).

  El ISP señala que varios países en los que opera prohíben la revelación de números específicos de cada país y que, en su evaluación de riesgos y beneficios, "incluso iniciar conversaciones con las autoridades con respecto a la divulgación de las cifras [...] podría generar resultados negativos para nuestras operaciones y nuestra capacidad de promover prácticas más respetuosas de los derechos".

Sin embargo, los fundamentos jurídicos de tales prohibiciones no están claros. Por ejemplo, investigaciones anteriores sobre los marcos jurídicos de Paraguay, Colombia y Panamá no revelaron prohibiciones legales contra la publicación de datos agregados sobre solicitudes gubernamentales. El informe global de Millicom tampoco especifica qué legislación prohíbe publicar datos específicos de un país. A su vez, la investigación de la Global Network Initiative sobre los marcos legales de los países, citada en el informe de Millicom y elaborada con la colaboración del ISP, menciona legislación en los países cubiertos por Millicom que *no* aborda específicamente la publicación de datos agregados. Las prohibiciones explícitamente establecidas por ley son en general redactadas para abordar de manera amplia el secreto de las comunicaciones y la confidencialidad de los procedimientos de interceptación. Las autoridades estatales y las empresas no deben interpretar, como parece ser el caso de Millicom, que esas disposiciones impiden la divulgación de información estadística de las solicitudes de datos de los usuarios por parte de las fuerzas de seguridad. En virtud de las normas de derechos humanos aplicables, impedir que las empresas publiquen dichos datos va en contra de los principios fundamentales de transparencia y supervisión pública de la vigilancia gubernamental. Sin embargo, aunque Millicom se queda corto a la hora de revelar datos estadísticos específicos de cada país, el informe del ISP se destaca positivamente por la información cualitativa que proporciona sobre los marcos legales locales y las prácticas de los gobiernos a la hora de solicitar datos de los usuarios (por ejemplo, Millicom proporciona una descripción más detallada sobre los mandatos de acceso directo en determinados países; véase más abajo). El informe global de Millicom también enumera las autoridades competentes que pueden emitir solicitudes de interceptación y metadatos en cada país. A nivel local, la filial colombiana de Millicom publica un informe de transparencia específico, el único país que hemos encontrado que lo haga entre los estudios QDTD (véase la sección 1.4). Es interesante notar que, en dicho informe, Tigo Colombia revela las demandas de datos gubernamentales por autoridad solicitante y tipo de datos. Por ejemplo, en 2021, el ejército colombiano hizo cuatro peticiones de datos de abonados, mientras que las agencias de inteligencia solicitaron datos de abonados 10 veces y registros de llamadas seis veces. La gran mayoría de las solicitudes procedían de la fiscalía y la policía, seguidas de los tribunales.

- **América Móvil (Claro)** ha tardado más en publicar informes globales de transparencia. El primero que pudimos encontrar revela cifras de solicitudes de aplicación de la ley en 2020, aunque Claro Chile ha estado publicando una versión local desde 2018, tras la primera edición de QDTD en el país. No hay una manera fácil de acceder directamente a los informes globales de transparencia en el sitio web de América Móvil. El enlace está oculto en los informes de sustentabilidad del ISP.[2] La empresa proporciona información estadística sobre las demandas gubernamentales de datos *por región*, y no por país, y no las desglosa en categorías específicas de datos solicitados (por ejemplo, interceptación o metadatos de clientes). Sólo revela el número total de solicitudes de información sobre usuarios recibidas de las autoridades y la proporción de las que el proveedor de servicios de Internet atendió. Agrupa esta

[2] América Móvil. Informe de Sustentabilidad, 2020, en la página 95. https://s22.q4cdn.com/604986553/files/doc_downloads/2021/05/Informe-de-Sustentabilidad-2020.pdf
América Móvil. Informe de Sustentabilidad, 2021, en la página 51. https://s22.q4cdn.com/604986553/files/doc_downloads/sustainability/es/2022/Informe-de-Sustentabilidad-2021.pdf

información en las siguientes regiones *Norte América y el Caribe* (Estados Unidos y Puerto Rico, México y República Dominicana), *Centroamérica* (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá), *Cono Sur* (Argentina, Brasil, Paraguay y Uruguay) y *Región Andina* (Colombia, Chile, Ecuador y Perú). El informe no explica por qué el ISP no revela datos agregados por país, pero sí describe el marco legal aplicable y las autoridades competentes, además de ofrecer información sobre los pasos internos de la empresa para responder a las solicitudes. Sobre esto último, el grado de información facilitada para cada país puede variar significativamente. La descripción que hace el informe del marco jurídico aplicable es bastante normalizada y útil, ya que abarca la divulgación de registros de datos a las autoridades competentes, la geolocalización de dispositivos móviles en tiempo real, la interceptación de comunicaciones privadas, la interrupción de servicios de telecomunicaciones por orden judicial y el bloqueo de líneas de comunicación utilizadas para la comisión de delitos. Sin embargo, la información sobre las autoridades competentes sigue careciendo de claridad y normalización. Para Argentina, por ejemplo, el informe solo señala las autoridades competentes que pueden solicitar la interceptación de comunicaciones. En el caso de Paraguay, en general se refiere a jueces y fiscalías, sin distinción sobre las solicitudes que solo los jueces pueden autorizar (por ejemplo, interceptación), a diferencia de lo que pasa en el caso de Uruguay.

Consolidamos esta información en los cuadros siguientes:

ISP	Primer informe mundial encontrado (año de publicación)	Datos estadísticos por país o región	Informa sobre el número de solicitudes rechazadas	Informa sobre las autoridades competentes	Informa sobre el marco jurídico
AT&T	2015	País	Sí, para México y EE.UU.	No	Sí, para México y EE.UU.
Telefónica	2016	País	Sí	Sí	Sí
Millicom	2016	Región	No	Sí	Dirige al Country Legal Frameworks Resource de la GNI
América Móvil	2021	Región	Sí	Sí, pero carece de normalización	Sí

ISP	Tipos de datos/desglose de solicitudes
AT&T	México: información histórica (información sobre abonados/registros de llamadas e información de localización (celda de celular)), información de localización en tiempo real e intervenciones de líneas telefónicas. Otros países de Latinoamérica: información sobre abonados y bloqueo de IP/URL.
Telefónica	Interceptaciones legales (incluidas las solicitudes de una nueva interceptación, de ampliaciones o de desconexión de una interceptación existente), acceso a metadatos, bloqueo y restricción de contenidos, suspensión geográfica o temporal del servicio y número de accesos afectados por las solicitudes.
Millicom	Interceptación, metadatos de clientes y datos financieros de clientes (relacionados con los servicios financieros móviles que presta el ISP).
América Móvil	No hay desglose por tipo de datos/solicitud.

Los informes de transparencia podrían ofrecer más detalles sobre los motivos por los que las empresas han rechazado solicitudes gubernamentales y sobre la proporción de solicitudes relativas a blancos específicos (dirigidas o individualizadas) *frente a las* no dirigidas , o masivas, que han recibido (por ejemplo, solicitudes masivas de datos de todos los dispositivos que se conectaron a una torre de telefonía móvil). Explicamos esto último con más detalle a continuación. Por ahora, cabe destacar que de los cuatro informes globales descritos anteriormente, solo Millicom y AT&T mencionan directamente las solicitudes masivas o colectivas.

En su informe, Millicom dice que una solicitud que busca información sobre varios individuos o dispositivos cuenta como una sola solicitud en la tabla de datos, lo que significa que "las solicitudes no son iguales en magnitud". AT&T explica que, aunque las autoridades mexicanas pueden solicitar todos los números de teléfono registrados en una torre celular concreta durante un periodo determinado, el ISP no lleva un registro de cuántos números de teléfono proporciona a las fuerzas de seguridad en esos casos. Ambas observaciones levantan una bandera roja sobre el reporte incompleto del número de líneas, dispositivos o personas afectadas por las medidas de vigilancia. El informe de Telefónica incluye una métrica adicional para captar esta información, revelando tanto el *número de solicitudes* como el *número de accesos afectados*.[3] Si se consideran las solicitudes masivas no dirigidas, las cifras con respecto al número de solicitudes serían a menudo menores que las cifras relativas al número de accesos afectados (por ejemplo, una solicitud para que un ISP revele todos los teléfonos móviles conectados a una torre de telefonía móvil durante un día y una hora específicos es una solicitud que afecta a

[3] El informe de Telefónica no define lo que el proveedor entiende por "accesos" afectados, pero en general entendemos que el término se refiere a las líneas o números de teléfono y a las conexiones a Internet móviles o fijas que la empresa proporciona a sus usuarios y usuarias.

cientos o incluso miles de accesos). Sin embargo, esta relación varía a lo largo del informe de Telefónica, con países en los que ocurre lo contrario o en los que estos dos indicadores presentan la misma cifra. Telefónica podría dar más explicaciones sobre la relación de ambos indicadores en futuros informes.

En cuanto a las razones por las que se rechazan las solicitudes de datos de personas usuarias hechas por las autoridades, Telefónica proporciona una descripción general en la sección introductoria de su informe.[4] Los ISP chilenos comenzaron a detallar dicha información en los últimos años y, desde octubre de 2021, Claro Chile desagrega el número de solicitudes rechazadas por motivo de rechazo. Un número importante de solicitudes rechazadas no provienen de direcciones de correo electrónico institucionales, o no presentan una orden judicial, entre otros problemas.

Al igual que ocurre con los informes de transparencia, existe una tendencia creciente a consolidar la publicación de directrices sobre aplicación de la ley (directrices LE) como mejor práctica. Sin embargo, seguimos observando un grado muy variable de información facilitada. A menudo, los ISP divulgan directrices globales resumidas sin ofrecer detalles que tengan en cuenta la legislación local de los países en los que operan. Este es el caso de Millicom y Telefónica, cuyos informes de transparencia aportan más información específica de cada país que las directrices LE que están a disposición del público. Ambas empresas divulgan directrices de LE locales, pero solo para algunos países QDTD (véase la sección 1.4).

No hemos podido encontrar directrices de LE para América Móvil, aunque su informe de transparencia contiene alguna información relacionada, y Claro en Chile y Perú publican directrices locales. El anexo legal de Vodafone destaca por proporcionar información exhaustiva sobre la legislación aplicable a las solicitudes de LE en los países en los que opera el ISP, entre los que se incluye España.

Los informes QDTD identificaron y puntuaron las directrices LE locales en Argentina (IPLAN y Telefónica-Movistar), Brasil (Algar, TIM, Oi y Telefónica-Vivo), Chile (todos los ISP investigados), Colombia (Telefónica-Movistar, Millicom-Tigo, ETB y DirecTV), Perú (América Móvil-Claro y Telefónica-Movistar) y España (Vodafone).

Los informes de transparencia y las directrices LE son herramientas cruciales para la rendición de cuentas de los gobiernos y la supervisión pública de la vigilancia de las comunicaciones. Arrojan luz sobre aspectos críticos del modo en que las autoridades gubernamentales acceden a la información de los clientes y la utilizan, así como sobre los controles y salvaguardias que las empresas tienen en cuenta a la hora de responder a las solicitudes.

A lo largo de los años, los informes de la QDTD han animado a los proveedores de servicios de Internet a elevar el nivel de sus compromisos y han presionado a las empresas para que revelen detalles útiles para identificar y abordar tendencias preocupantes. Dos de esas tendencias son el acceso directo de los gobiernos a las redes de las empresas de telecomunicaciones y el uso de solicitudes masivas de datos de usuarios no dirigidas y/o acuerdos de intercambio de datos con fines de investigación criminal, inspección o política pública.

[4] Telefónica explica que las solicitudes de información de usuarios rechazadas lo fueron por las siguientes razones: no cumplen con la legislación local para ese tipo de requerimiento; no contienen todos los elementos necesarios (firmas necesarias, autoridad competente, descripción técnica del requerimiento, etc.), o es técnicamente imposible ejecutar la solicitud.

El informe de transparencia de Millicom menciona que el ISP debe conceder a las autoridades gubernamentales acceso directo a sus redes en Honduras, El Salvador, Colombia y Paraguay. Teniendo en cuenta este y otros informes, Karisma incluyó un parámetro en la edición de Colombia de 2021 para evaluar si las empresas revelan información sobre sus prácticas de acceso directo, como la base legal que autoriza el acceso directo y el papel del ISP. Según el informe de Karisma, Telefónica-Movistar abordó claramente el tema, y tanto América Móvil-Claro como Millicom-Tigo divulgaron información sobre el marco jurídico que supuestamente sustenta el acceso directo en Colombia. Otras seis empresas evaluadas en el informe de Colombia de 2021 guardaron silencio sobre esta práctica. Los retos para informar adecuadamente sobre el acceso directo se mantuvieron en la última edición de Colombia. Esta vez, solo Movistar y Tigo recibieron créditos en esta categoría.

A su vez, la pandemia de COVID-19 atrajo una mayor atención sobre las peticiones masivas de datos de personas usuarias por parte de los gobiernos y/o los acuerdos de intercambio de datos en los que participan empresas de telecomunicaciones. También ha reforzado los debates sobre la sensibilidad de los datos de localización. Véase la sección 1.3 de este informe comparativo para más información sobre cómo afectó la pandemia a los criterios de QDTD. Sin embargo, los informes de InternetLab para Brasil han evaluado la información que los ISP proporcionan sobre la divulgación de datos de geolocalización a las autoridades desde la edición de 2019. Más recientemente, el informe de Brasil de 2021 descubrió que solo la mitad de las empresas evaluadas mencionan la recopilación o el procesamiento de datos de localización. De ellas, solo TIM y América Móvil-Claro proporcionan más detalles sobre las circunstancias en las que comparten los datos de localización de las personas usuarias a las autoridades y por qué teniendo en cuenta la legislación brasileña aplicada a este tipo de datos.

En cuanto al intercambio de datos con entidades gubernamentales, el informe de Colombia de 2021 destacó que la falta de transparencia y de notificación a las personas usuarias dificulta el seguimiento del uso indebido de los datos personales. Además, las empresas estatales (ya sean totalmente públicas o con participación estatal) deberían ser más claras sobre si comparten información personal de sus clientes con fines políticos o de otro tipo, y cómo lo hacen. Karisma subraya el caso del operador de telecomunicaciones ETB, que es uno de los propietarios de la *Agencia de Analítica de Datos de Bogotá* (AGATA). El objeto social de AGATA es contribuir a las iniciativas relacionadas con la ciudad inteligente de Bogotá y ofrecer servicios al sector privado. Según su página web, las entidades que formaron AGATA proporcionan datos que la agencia utiliza para ofrecer soluciones digitales. ETB no detalla información sobre esta colaboración.

Por último, los ISP siguen revelando muy poco sobre sus prácticas y acuerdos de intercambio de datos con sus socios comerciales, algo que algunos informes QDTD han empezado a rastrear. Para tener una visión más holística de las prácticas empresariales relacionadas con las solicitudes de datos de las autoridades públicas, la publicación de las evaluaciones de impacto sobre la protección de datos (EIPD) de los ISP mejoraría definitivamente la transparencia y la supervisión pública de la vigilancia gubernamental y empresarial. Desde el informe de Brasil de 2020, InternetLab ha comprobado si las empresas publican las EIPD, pero hasta ahora ninguna empresa evaluada lo ha hecho.

- ⇨ Para más información sobre los problemas de transparencia y proporcionalidad del acceso a los datos por parte de las fuerzas de seguridad, véanse las **secciones 2.1 y 2.3**.
- ⇨ Véase más información sobre lo que dicen las empresas acerca de su intercambio de datos con socios comerciales en **la sección 3.1**.

Autorización judicial

Esta categoría de evaluación comprueba si el ISP se compromete públicamente a solicitar una orden judicial antes de entregar los datos de la persona usuaria a las autoridades. Lograr tal compromiso depende de lo que exija o permita el marco jurídico nacional de cada país que realiza la investigación de QDTD. La metodología de cada informe se adapta para reflejar el margen de maniobra de los ISP dentro del marco jurídico de cada país a la hora de adoptar interpretaciones protectoras cuando responden a solicitudes de las fuerzas de seguridad. Aunque la necesidad de una orden judicial previa es casi unánime entre los países del QDTD para la interceptación de las comunicaciones, excepto en Colombia, el acceso de los gobiernos a los metadatos suele gozar de un menor nivel de protección en la región. Cuando la ley otorga la misma protección a los metadatos, como en Brasil, o no hace distinciones para socavar las salvaguardias de los metadatos, como en Chile o Argentina, los informes del QDTD solicitan el compromiso de los ISP de exigir una orden judicial antes de entregar tanto el contenido de las comunicaciones como los metadatos. Cuando la legislación nacional autoriza claramente a las autoridades policiales a acceder a los metadatos sin autorización judicial previa, como en Panamá, los informes QDTD reformulan la petición y, en su lugar, solicitan información sobre el compromiso de las empresas de rechazar las solicitudes gubernamentales ilegales.

En general, los informes de QDTD encontraron compromisos más sólidos para exigir una orden judicial previa para las solicitudes gubernamentales de metadatos en Brasil, Chile, Perú (especialmente Telefónica-Movistar) y España (especialmente Vodafone).

⇨ Véase más información sobre la importancia de lograr mayores salvaguardias para el acceso de los gobiernos a los metadatos en América Latina en la **sección 2.2**.

Notificación a la persona usuaria

Tal vez el parámetro de evaluación más difícil en los informes QDTD sea preguntar a los ISP si notifican a las personas usuarias cuando el gobierno solicita sus datos, ya que muchas empresas que operan en América Latina se resisten a esta práctica. Argumentan que las solicitudes de información de los usuarios por parte de las autoridades policiales están sujetas a deberes de secreto, y les resulta difícil saber cuándo terminan sus obligaciones de secreto, a pesar de que esta categoría de proyecto pide el compromiso de los ISP de notificar a las personas usuarias en la primera oportunidad permitida por la ley. Sin embargo, a la luz de las dudas de los ISP, muchos informes QDTD dan créditos cuando las empresas demuestran esfuerzos concretos hacia la transparencia. Pueden obtener créditos por comprometerse con las autoridades o a través de otras vías a poner en marcha un procedimiento de notificación en casos penales, por comprometerse a notificar a los usuarios las solicitudes de datos en otros tipos de casos (por ejemplo, civiles, laborales y de familia), o simplemente por divulgar políticas claras sobre la notificación a la persona usuaria.

Con el tiempo, los informes QDTD desempeñaron un papel relevante a la hora de conseguir que los ISP adoptaran políticas de notificación. Los aliados del proyecto identificaron declaraciones de las empresas en las que se reservaban la posibilidad de notificar a la persona usuaria sobre las solicitudes de sus datos en Argentina (AT&T-DirecTV, Telefónica-Movistar), Chile (WOM, VTR, América Móvil-Claro, GTD), Colombia (AT&T-DirecTV) y Panamá (Más Móvil). En Chile y Perú, América Móvil-Claro

se ha comprometido a notificar a la persona usuaria en casos civiles, laborales y de familia. WOM ha hecho lo mismo en Chile.

⇨ Véase más información sobre el papel clave que desempeña la notificación al usuario de las solicitudes gubernamentales en la salvaguarda de los derechos humanos en **el apartado 2.4**.

Compromiso con la privacidad de la persona usuaria en los tribunales, el Congreso y los debates políticos

Esta categoría trata de medir los compromisos de las empresas más allá de lo que declaran en sus políticas, analizando si los ISP han adoptado una postura a favor de la privacidad de la persona usuaria ante los tribunales, el Congreso, los organismos administrativos o en el contexto de otros debates políticos. Sin embargo, se trata de una categoría difícil de medir y depende en gran medida de que las empresas se comprometan con los aliados de QDTD a proporcionar enlaces y documentos que muestren sus prácticas. Las empresas de telecomunicaciones no suelen informar sistemáticamente sobre los casos legales que inician para impugnar demandas arbitrarias de datos ni sobre sus posiciones en debates legislativos o políticos específicos sobre privacidad. AT&T publica información sobre sus posturas y actividades en relación con la protección y la seguridad en Internet, pero el contenido de su sitio web, salvo contadas excepciones, solo aborda debates globales o acontecimientos relacionados con Estados Unidos. El sitio web corporativo de Telefónica también incluye entradas sobre cuestiones regulatorias y de políticas públicas. Sin embargo, no hay mucha información específica sobre los países latinoamericanos.

Para evaluar esta categoría, la investigación de QDTD generalmente implica comprobar los medios de comunicación, las redes sociales de los ISP y su participación en actos públicos. Los litigios de las empresas también son más fáciles de localizar e identificar en los países en los se encuentran mecanismos más ágiles y sencillos para la búsqueda de jurisprudencia en diversos tribunales nacionales, lo que varía significativamente entre los países QDTD. En los informes QDTD, Claro Chile destaca en esta categoría de proyectos por crear una sección específica en su sitio web para detallar las interacciones con las autoridades públicas. En Brasil, Oi incluye en el informe de sostenibilidad de la empresa información sobre los recursos judiciales que inició contra las solicitudes de datos del gobierno. El informe de transparencia global de Millicom también ofrece alguna información sobre su compromiso con las autoridades locales para reforzar la privacidad y las garantías procesales. Cuando sea posible, la empresa podría proporcionar recursos más concretos relacionados con tales esfuerzos.

Las empresas se encuentran en una posición crítica para evaluar y poner freno a las solicitudes abusivas de los gobiernos, especialmente cuando no hay notificación previa a los usuarios y las personas objeto de las mismas solo pueden buscar remedio después de que se haya producido la medida de vigilancia intrusiva. Los informes de QDTD subrayan casos relevantes en los que los ISP defendieron la privacidad de los usuarios y usuarias. He aquí algunos ejemplos:

- En Brasil, los informes de InternetLab destacan el recurso de inconstitucionalidad presentado por la Asociación Nacional de Empresas de Telefonía Móvil (ACEL) contra una disposición de la Ley de Organizaciones Criminales del país que permite la divulgación de metadatos telefónicos sin orden judicial previa. Más recientemente, el proveedor de telecomunicaciones Oi impugnó una orden judicial que otorgaba a la policía la facultad de acceder

durante seis meses a todos los datos almacenados relacionados con la telefonía, incluida la información de identificación de los abonados, los registros de llamadas y SMS y los datos de localización. En el último informe, Claro, Oi, TIM, Vivo y Brisanet impugnaron directamente las solicitudes de datos hechas por autoridades de investigación porque carecían de una orden judicial, mostraban una base jurídica insuficiente o iban más allá de las obligaciones legales de las empresas de almacenar datos.
- En Perú, Hiperderecho informó sobre la negativa de Claro a cumplir con una solicitud de la autoridad tributaria del país SUNAT para revelar la base de datos completa de clientes de prepago y postpago con fines de auditoría.
- En cuanto a los debates legislativos, Derechos Digitales señaló una comunicación que Claro Chile envió a los legisladores en relación con la reforma de la Ley de Protección de Datos de Chile. El ISP expresó su preocupación por las solicitudes de información de usuarios que recibe de organismos públicos, sugiriendo que las normas de tratamiento de datos personales para las empresas también deberían aplicarse a los organismos estatales, incluyendo controles preventivos y oficiales de cumplimiento.

Por último, los informes de QDTD suelen dar créditos a las empresas de esta categoría si se unen a iniciativas de múltiples partes interesadas para la protección de las personas usuarias y la promoción de los derechos humanos. Cabe señalar que importantes empresas de telecomunicaciones de la región, como Telefónica y Millicom, han abandonado recientemente la Global Network Initiative (GNI), un proyecto de establecimiento de normas de libre expresión entre cuyos miembros hay empresas, inversores y organizaciones sin ánimo de lucro de distintas regiones. Aunque Telefónica y Millicom siguen formando parte del Diálogo de la Industria de las Telecomunicaciones, un grupo de operadores y vendedores de telecomunicaciones que promueven la libre expresión y la privacidad, esta iniciativa está formada por empresas cuyos representantes suelen proceder de sus sedes europeas y no tienen necesariamente en cuenta los retos particulares de América Latina.

Seguridad digital

Esta categoría de evaluación se midió por primera vez en el informe de 2017 de Karisma para Colombia. En ese momento, América Móvil-Claro, Telefónica-Movistar, AT&T-DirecTV y EMCALI no utilizaban cifrado (protocolo HTTPS) en sus sitios web, mientras que Millicom-Tigo, ETB y Telebucaramanga ya lo hacían. A través del cifrado, el HTTPS protege la transmisión de los datos personales que las personas introducen en las webs y apps de los ISP cuando consultan sus cuentas, interactúan con la empresa o adquieren servicios. El primer informe de IPANDETEC para Panamá en 2019 encontró que Claro no utilizaba el protocolo de seguridad en el canal virtual de atención al cliente del ISP. Las siguientes ediciones en Perú, Colombia y Panamá mostraron que todas las empresas evaluadas ahora utilizan el protocolo de seguridad. En Perú, Hiperderecho indica que todos los ISP destacados también ofrecen a las personas usuarias métodos de seguridad adicionales, como la autenticación de dos factores para acceder a sus cuentas en los canales de comunicación de los ISP. Sin embargo, todavía hay muchas lagunas cuando observamos la postura pública de las empresas de telecomunicaciones con respecto a las violaciones de datos o qué información publican las empresas sobre sus protocolos y medidas de ciberseguridad. Dependiendo del país, algunas de las principales empresas de telecomunicaciones, como Millicom-Tigo, Telefónica-Movistar y América Móvil-Claro, ofrecen orientación sobre seguridad digital. En cuanto a los protocolos y compromisos relativos a las violaciones de datos personales, los informes de QDTD en Brasil, Colombia y Panamá muestran que los ISP facilitan información en

distintos grados y, en Brasil, ofrecen respuestas públicas deficientes a las denuncias de violaciones de datos.

⇨ Véase más información sobre protocolos y compromisos relacionados con la violación de datos en **la Sección 3.3**.

1.3. La pandemia de COVID-19 reflejada en los informes QDTD

La emergencia sanitaria y social mundial suscitada por la pandemia de COVID-19 impulsó a los gobiernos a hacer frente a la propagación masiva del virus. Las precipitadas respuestas basadas en la tecnología suscitaron muchas y serias preocupaciones entre los expertos y los defensores de la sociedad civil que trabajan en la intersección entre tecnología y derechos humanos. Los informes de QDTD publicados durante este periodo han reflejado algunas de estas cuestiones en sus parámetros. Por ejemplo, las normativas de emergencia que amenazaban la neutralidad de la red en Colombia llevaron a Karisma a incluir criterios relacionados en su informe de 2021.

En el frente de la privacidad, el acceso de los gobiernos a los datos de los usuarios para las políticas de control de COVID-19 se destacó entre las ediciones de QDTD.

El informe de Brasil de 2020 comprobó qué empresas adoptaron una postura pública para defender la privacidad y la protección de datos frente a las presiones del gobierno para acceder a los datos de telecomunicaciones durante la pandemia. InternetLab subrayó que Oi se comprometió públicamente a exigir a la agencia nacional de estadística del país, IBGE, que firmara un término de responsabilidad antes de darle acceso a los datos de los usuarios, debido a una normativa que posteriormente anuló el Supremo Tribunal Federal de Brasil. El informe también señalaba que los proveedores de telecomunicaciones han firmado acuerdos de intercambio de datos con estados y municipios. Aunque funcionarios del gobierno revelaron a la prensa la existencia de tales acuerdos, su contenido no estaba disponible públicamente. Vivo y Tim se comprometieron públicamente a que solo se compartirían con el gobierno datos anónimos y agregados, a través de mapas de calor y tablas dinámicas. Y después de que un tribunal de São Paulo dictaminara que este acuerdo debía ser público, muchos proveedores de telecomunicaciones publicaron las políticas pertinentes en sus sitios web, entre ellos TIM, Telefónica-Vivo, América Móvil-Claro y Oi. Sin embargo, las políticas de las empresas no especificaban las prácticas y técnicas de seguridad adoptadas para garantizar el anonimato de los datos compartidos. Además, los ISP deberían haber publicado sus políticas de forma proactiva e inmediata, y no tras la presión pública.

Esto también es lo que busca fomentar el informe de Chile en ediciones más recientes. Desde 2021, los informes QDTD de Derechos Digitales detectan qué proveedores hicieron públicos sus acuerdos de intercambio de datos con instituciones públicas y privadas. Considerando tanto la pandemia del COVID-19 como las demandas de las fuerzas de seguridad en el contexto de las protestas sociales en todo el país en 2019, los informes de Chile comenzaron a verificar qué proveedores se comprometen públicamente a entregar información sensible de las personas usuarias, como datos de localización, a las autoridades solo si las solicitudes se refieren a personas específicas y vienen con autorización judicial previa. Los informes de transparencia también deben indicar si las solicitudes se dirigen a individuos o a grupos de personas (por ejemplo, búsquedas en torres de telefonía móvil). Cuando se trata de compartir datos con fines de política

pública, los ISP deben comprometerse a compartir con las autoridades gubernamentales únicamente datos de localización anonimizados y agregados.

Los resultados de los informes de Chile muestran avances significativos. Para 2022, Telefónica-Movistar y Entel han publicado detalles sobre sus acuerdos de intercambio de datos para hacer frente a la pandemia. América Móvil-Claro, VTR y WOM empezaron a informar sobre las solicitudes colectivas que los ISP recibieron de las autoridades. Todas las empresas investigadas, excepto Telefónica-Movistar y GTD, se comprometieron a exigir una orden judicial y la indicación, o individualización, de las personas afectadas en las solicitudes gubernamentales que impliquen información sensible. Y todos los ISP, excepto GTD y VTR, refrendaron el compromiso de compartir únicamente datos de localización anonimizados y agregados con fines de política pública.

Por último, el informe 2022 de Eticas creó una puntuación particular para indicar si los ISP hicieron pública alguna medida específica de protección de datos relacionada con la pandemia. De las seis empresas de telecomunicaciones evaluadas, solo Vodafone recibió crédito por publicar una política específica de protección de datos sobre su colaboración con las autoridades gubernamentales en las acciones de control de la COVID-19. La política de Vodafone se compromete a salvaguardias importantes, como compartir únicamente datos agregados y anónimos y respetar los principios de proporcionalidad y limitación de la finalidad. Aunque el informe menciona que el ISP ha puesto en marcha medidas de seguridad adecuadas, no proporciona ningún otro detalle sobre cuáles son estas medidas. Aun así, Vodafone va un paso más allá que otras empresas de telecomunicaciones en España al haber puesto a disposición una política específica para las acciones relacionadas con COVID.

1.4. Comparación regional de las principales empresas reportadas

Esta sección esboza una comparación regional de las principales empresas de telecomunicaciones con operaciones en América Latina y España incluidas en los informes QDTD de al menos dos países diferentes. Se han producido cambios relevantes en la afiliación y distribución geográfica de las empresas a lo largo de los años del proyecto. Esto es especialmente cierto en el caso de América Central, donde publicamos ediciones para Panamá y Nicaragua. Por lo tanto, la distribución de mercado de cada empresa en los informes QDTD que indicamos a continuación considera la última edición de cada país.

Salvo en el caso de los informes de transparencia, la comparación de esta sección no tiene en cuenta las políticas o directrices mundiales.

Telefónica/Movistar/Vivo

Operaciones en Argentina, Brasil, Chile, Colombia, México, Perú y España

Políticas de protección de datos/ privacidad	"Centros de Privacidad y/o Transparencia" en todos los países investigados: Argentina, Brasil, Chile, Colombia, México, Perú y España.
Informes de transparencia	Informe global con información detallada de todos los países (publicado recientemente en portugués). Disponible en todos los sitios web locales.
Autorización judicial previa	○ Contenido/Interceptación: Argentina, Brasil, Chile, México, Perú, España ○ Metadatos: Brasil, Perú
Notificación a la persona usuaria	○ Declaración general reservándose la posibilidad: Argentina (2019) ○ Denegación de notificación a la persona usuaria: Chile, Perú
Directrices LE	Argentina, Brasil, Chile, Colombia, México, Perú. Las directrices LE publicadas en los sitios web de Argentina y México son menos informativas que las disponibles en las páginas web de las demás filiales.

América Móvil/Claro/NET

Operaciones en Argentina, Brasil, Chile, Colombia, Nicaragua, Panamá, Paraguay y Perú.

Políticas de protección de datos/ privacidad	○ "Portal de privacidad y/o protección de datos": Brasil, Chile ○ Política estándar que cubre la prestación de servicios de telecomunicaciones: Argentina, Colombia, Paraguay, Perú ○ Política estándar que cubre únicamente los canales de comunicación: Nicaragua ○ Confuso en cuanto a su ámbito de aplicación: Panamá
Informes de transparencia	○ Informe local con datos agregados de solicitudes gubernamentales: Chile, Perú. En Brasil, Claro proporciona datos en el informe de sostenibilidad del ISP ○ Informe global con datos agregados de solicitudes gubernamentales: Publicado a partir de 2021, ofrece datos agregados *por región*. Abarca todos los países. Regiones divididas en: América del Norte y el Caribe, América Central, Cono Sur y Región Andina. No está disponible en sitios web locales.
Autorización judicial previa	○ Contenido/Interceptación: Argentina, Brasil, Chile, Perú. ○ Metadatos: Brasil, Chile, Perú.
Notificación a la persona usuaria	○ Declaración general reservándose la posibilidad: Chile ○ Compromiso de notificación en casos no penales: Chile, Perú ○ Denegación de notificación a la persona usuaria: Panamá
Directrices LE	○ Directrices para la aplicación de la ley: Chile, Perú ○ Informe global: El informe de transparencia 2021 de América Móvil incluye alguna información

	sobre el procedimiento seguido y la legislación aplicable.

Millicom/Tigo

Operaciones en Colombia, Nicaragua, Paraguay y Panamá

Políticas de protección de datos/ privacidad	○ No hay Centro o Portal de Privacidad, salvo algo similar en Colombia. ○ Confuso en cuanto a su ámbito de aplicación: Nicaragua, Panamá, Paraguay
Informes de transparencia	○ Informe local con datos agregados de solicitudes gubernamentales: Colombia ○ Informe global con datos agregados de solicitudes gubernamentales: Proporciona datos agregados *por región*, abarcando todos los países. Las regiones se dividen en: América del Sur, América Central. No está disponible en sitios web locales.
Autorización judicial previa	○ Contenido/Interceptación: Paraguay, Panamá ○ Metadatos: Ninguno
Notificación a la persona usuaria	○ Declaración general reservándose la posibilidad: Ninguna ○ Compromiso de notificación en casos no penales: Ninguno
Directrices LE	○ Colombia

Otros ISP con presencia en más de un país[5]

AT&T/DirecTV (Argentina, Colombia, México), Liberty Latin America (VTR Chile, +Móvil Panamá), Entel (Chile, Perú), Telecom Group (Personal Argentina y Paraguay)

Políticas de protección de datos/ privacidad	○ "Portal de Privacidad y/o Protección de Datos" (obs: AT&T solo tiene un Centro de Privacidad en su web global) Entel Chile ○ Política estándar que cubre la prestación de servicios de telecomunicaciones: AT&T México, DirectTV (Argentina), DirecTV (Colombia), VTR Chile, +Móvil Panamá, Entel Perú, Personal Argentina ○ Política estándar que cubre únicamente las vías de comunicación: Personal Paraguay
Informes de transparencia	○ Informe local con datos agregados de solicitudes gubernamentales: VTR Chile, Entel Chile ○ Informe global con datos agregados de solicitudes gubernamentales: AT&T México, DirecTV (Argentina y Colombia). El informe de AT&T proporciona muy pocos datos sobre los países latinoamericanos, excepto México.
Autorización judicial previa	○ Contenido/Interceptación: AT&T México, VTR Chile, Entel Chile, Personal Argentina ○ Metadatos: AT&T México, VTR Chile, Entel Chile, Personal Argentina
Notificación a la persona usuaria	○ Declaración general reservándose el derecho o la posibilidad: DirectTV Colombia y Argentina, VTR Chile, +Móvil Panamá ○ Explicación sobre la limitación y compromiso de evaluar las circunstancias: Entel Chile ○ Compromiso de notificación en casos no penales: ninguno

[5] AT&T y Liberty Latin America prestan servicios en otros países del proyecto, pero a continuación enumeramos solo los países en los que figuran los ISP en sus últimos informes publicados.

	○ Denegación de notificación a la persona usuaria: ninguna
Directrices policiales	○ Informe local: VTR Chile, Entel Chile

Los informes QDTD también han desempeñado un papel importante al impulsar a las empresas no dominantes a superar a los grandes líderes del mercado en sus compromisos con la transparencia y la privacidad de las personas usuarias. WOM y VTR en Chile son buenos ejemplos. Además, Somos Conexión en España, TIM en Brasil e IPLAN en Argentina han demostrado que el compromiso con los informes QDTD se traduce en una mayor protección de las personas usuarias y en una mejor calificación de las ediciones del proyecto.

2. La aplicación de las normas de derechos humanos a la vigilancia de las comunicaciones: Acceso de los Gobiernos a los datos e impugnación de las buenas prácticas de los proveedores de servicios de Internet

Las normas internacionales de derechos humanos constituyen el marco universal en el que debe evaluarse cualquier injerencia en el derecho a la intimidad. Los organismos universales y regionales de derechos humanos, los tribunales internacionales y los expertos y defensores de la sociedad civil han desarrollado una labor fundamental y continua basada en las normas internacionales de derechos humanos sobre cómo proteger el derecho a la privacidad en la era digital.[6] Los instrumentos internacionales de derechos humanos dejan claro que todas las restricciones al derecho a la intimidad, incluido el derecho a no sufrir injerencias arbitrarias en las comunicaciones, deben seguir una prueba de tres partes: las restricciones deben estar prescritas de forma clara y accesible por la ley, ser adecuadas y necesarias para alcanzar un objetivo legítimo en una sociedad democrática, y ser proporcionadas al objetivo perseguido.

[6] Electronic Frontier Foundation y ARTICLE19, Necessary & Proportionate Global Legal Analysis, (mayo de 2014). https://necessaryandproportionate.org/global-legal-analysis/; Resolución de la Asamblea General de la ONU sobre el derecho a la intimidad en la era digital, UN Doc A/RES/75/176 (16 de diciembre de 2020); Resolución de la Asamblea General de la ONU sobre terrorismo y derechos humanos, UN Doc A/RES/74/147 (18 de diciembre de 2019); Resolución del Consejo de Derechos Humanos de la ONU sobre el derecho a la intimidad en la era digital, UN Doc A/HRC/RES/42/15 (7 de octubre de 2019); Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance.

Los informes QDTD ayudan a arrojar luz sobre las amenazas que se ciernen sobre la aplicación de las normas de derechos humanos a la vigilancia gubernamental. Estas amenazas ponen en peligro los principios de necesidad y proporcionalidad, así como las garantías procesales y las medidas de supervisión necesarias para impedir el acceso arbitrario de los gobiernos a los datos y defender los principios de las sociedades democráticas.

Aunque las empresas tienen la responsabilidad de respetar la privacidad y mitigar los riesgos para los derechos humanos en sus actividades,[7] también debemos abordar los retos derivados de la legislación local, las prácticas de aplicación de la ley basadas en interpretaciones de las normas nacionales y los preocupantes patrones presentes en la jurisprudencia. En las siguientes secciones se describen brevemente estas amenazas y retos en tendencia, y se analiza cómo socavan los principios y salvaguardias de los derechos humanos.

2.1. Autorizado por la ley, necesario y proporcionado

La OACDH hizo hincapié en que todos los tipos de actividades relacionadas con la vigilancia estatal deben llevarse a cabo sobre la base de la ley. Dichas leyes deben ser suficientemente precisas y describir la categoría de personas que pueden ser objeto de vigilancia. El Alto Comisionado señaló que "la vigilancia debe basarse en sospechas razonables, y toda decisión que la autorice debe ser suficientemente específica". Los informes de QDTD señalan al menos dos puntos importantes de atención en relación con la prueba de tres partes que deben superar las restricciones a la privacidad para ser legítimas según el derecho internacional de los derechos humanos. Los exponemos a continuación.

Solicitudes de datos de usuarios indeterminados o acuerdos de intercambio de datos con fines de investigación penal, inspección o política pública

El acceso de las autoridades gubernamentales a grandes porciones de información de usuarios indeterminados en poder de los ISP suscita preocupación, tanto si los datos se van a utilizar con fines policiales como de políticas públicas. El intenso recurso a medidas de vigilancia en la lucha contra la pandemia del COVID-19 acercó estas dos líneas de preocupación, aunque la forma de evaluar y abordar cada una tiene sus particularidades.

La prueba de las tres partes para restringir los derechos a la privacidad y protección de los datos es de nuevo la línea de base para cualquier política gubernamental que implique el tratamiento de datos que afecten a personas y/o grupos. Esta línea de base debe incluir sólidas normas de no discriminación[8] y de protección de datos, con salvaguardias como la minimización de datos, la limitación de la finalidad y el

[7] Principios Rectores de las Naciones Unidas sobre las empresas y los derechos humanos: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011, https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

[8] La Declaración y el Programa de Acción de Viena señalan: "La administración de justicia, incluidos los organismos encargados de hacer cumplir la ley, [...] en plena conformidad con las normas aplicables contenidas en los instrumentos internacionales de derechos humanos, [es] esencial para la realización plena y no discriminatoria de los derechos humanos e indispensable para el proceso de democracia y desarrollo sostenible"(traducción propia). Declaración y Programa de Acción de Viena, Conferencia Mundial de Derechos Humanos de Viena, 1993, https://www.ohchr.org/en/instruments-mechanisms/instruments/vienna-declaration-and-programme-action.

consentimiento. También debe incluir medidas concretas y eficaces para garantizar la seguridad, la transparencia y la rendición de cuentas, o el control comunitario, sobre si las políticas intensivas en datos son legítimas, necesarias y eficientes. La línea de base también debe considerar *si* estas políticas deben concebirse, aplicarse o mantenerse, y *cómo*.

Dicho esto, nos centraremos en la cuestión de las solicitudes no dirigidas (o de blancos indeterminados) con fines policiales.

Las autoridades gubernamentales recurren cada vez más a las bases de datos de Internet y de las empresas tecnológicas para realizar búsquedas masivas y sin sospechosos específicos en el contexto de investigaciones penales. Desde las búsquedas en torres de telefonía móvil ("tower dumps") hasta las búsquedas por geovallas y palabras clave, esas solicitudes, a menudo respaldadas por una orden judicial, invierten la lógica de investigar a sospechosos concretos basándose en una sospecha razonable que justifique la restricción del derecho a la intimidad. Por el contrario, las búsquedas *inversas* parten de un conjunto masivo de datos relacionados con las comunicaciones vinculados a determinadas zonas geográficas o palabras clave, durante un periodo concreto, para establecer un grupo de posibles sospechosos.

Estas búsquedas pueden incluir la información privada de millones de personas sin relación con un delito y someterlas a nuevos controles sin justificación razonable. Las búsquedas inversas de localización pueden sacar a la luz información sensible, como la ubicación del propietario de un dispositivo, enfriando la libertad de expresión y poniendo en peligro la intimidad y otros derechos humanos. Por ejemplo, los fiscales chilenos pidieron a las empresas de telecomunicaciones que entregaran todos los números de teléfono móvil que se hubieran conectado a torres de telefonía cerca de cinco estaciones de metro de Santiago, donde los incendios marcaron el inicio de la revuelta social y las protestas del país en 2019. Al obtener estos números de teléfono, sería posible identificar a los propietarios de dispositivos ubicados en la zona de protestas y luego tratar de inferir, basándose solo en su ubicación, si participaron en las protestas. Las autoridades policiales de Estados Unidos también han utilizado órdenes de geovalla para investigar desórdenes durante manifestaciones de *Black Lives Matter*.

Además de cuestiones de legalidad (como si la legislación nacional autoriza claramente este tipo de búsqueda) e idoneidad (considerar que esta técnica puede sesgar la investigación, invertir la carga de la prueba y dar lugar a un uso abusivo), las búsquedas inversas plantean serios problemas de proporcionalidad. Buscar en el pajar para posiblemente encontrar la aguja se alinea con lo que los organismos de derechos humanos entienden por vigilancia masiva y su carácter desproporcionado. Como subraya el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), "la vigilancia masiva de comunicaciones en ningún caso puede ser proporcionada". En esta misma línea, el Alto Comisionado de la ONU recomendó a los Estados que aclaren que la autorización de medidas de vigilancia requiere una sospecha razonable de que un individuo concreto ha cometido o está cometiendo un delito penal o participa en actos que suponen una amenaza específica para la seguridad nacional.

Las búsquedas inversas, por tanto, merecen una cuidadosa atención por parte de los tribunales y organismos de derechos humanos, ya que retuercen las garantías procesales y no cumplen las normas de necesidad y proporcionalidad. Los proveedores de servicios de Internet deben impugnar las solicitudes indiscriminadas de datos y comunicaciones de las personas usuarias. A su vez, los tribunales nacionales deberían defender las

normas internacionales de derechos humanos y las salvaguardias constitucionales poniendo fin a los registros sin sospecha razonable.

Acceso directo

El acceso directo a las redes de las empresas de telecomunicaciones para interceptar comunicaciones u obtener datos relacionados con las comunicaciones es otra práctica problemática de vigilancia gubernamental que se refleja en los informes de QDTD, en particular en las ediciones de Colombia de 2021 y 2022 (véase la sección 1.2). El informe de transparencia global de Millicom destaca que los requisitos de acceso directo en Honduras, El Salvador y Colombia impiden a los proveedores de servicios de Internet saber siquiera con qué frecuencia o durante qué periodos se produce la interceptación. Millicom informa de que en Colombia, la empresa está sujeta a fuertes sanciones, incluidas multas, si las autoridades descubren que obtuvo información sobre la interceptación mediante acceso directo que tiene lugar en su sistema. Como resultado, Millicom no posee información sobre con qué frecuencia y durante qué periodos de tiempo se interceptan las comunicaciones en sus redes móviles. El ISP afirma que también existe un requisito de acceso directo en Paraguay, pero los procedimientos allí permiten a la empresa ver las órdenes judiciales necesarias para que las autoridades gubernamentales inicien la interceptación.

El Diálogo de la Industria de las Telecomunicaciones subrayó que los acuerdos de acceso directo pueden dejar a las empresas sin ningún control operativo o técnico de su tecnología y de los datos de sus clientes. Tales acuerdos restringen la capacidad de los proveedores de servicios para examinar, cuestionar e informar sobre el acceso de los gobiernos a los datos. En este sentido, el GNI señaló que las prácticas de acceso directo son problemáticas al menos en tres aspectos: no suelen estar sujetas a los mismos procedimientos legales que median y supervisan las solicitudes de las fuerzas de seguridad; las autoridades tienden a aplicar el acceso directo mediante herramientas que van más allá de las soluciones estandarizadas de interceptación legal; y las prácticas de acceso directo a menudo no se reconocen públicamente ni se informa de ellas. Otro aspecto crucial que señala el GNI es que "a diferencia de las solicitudes de aplicación de la ley, que tienden a basarse en objetivos concretos, los acuerdos de acceso directo suelen extraer datos en bloque".

La OACDH y el Tribunal Europeo de Derechos Humanos declararon que las prácticas de acceso directo son motivo de grave preocupación, ya que son especialmente propensas a los abusos y tienden a eludir las principales garantías procesales. En cuanto a los países cubiertos por los informes QDTD, ni siquiera está clara la base jurídica que autoriza los procedimientos de acceso directo. Por lo que sabemos, no hay nada en la legislación de Paraguay que obligue explícita y públicamente a las empresas de telecomunicaciones a proporcionar acceso directo. En Colombia, Karisma informa que las autoridades se han basado en disposiciones del Decreto 1704 de 2012 para interceptar comunicaciones sin la intervención de la empresa de telecomunicaciones. Hay al menos dos cuestiones que podemos subrayar aquí. Primero, la norma es un decreto, y no una ley formal. En segundo lugar, el lenguaje del decreto no es claro en cuanto a si dispensa , o incluso prohíbe, que la empresa participe en el procedimiento de interceptación y tenga conocimiento de que la medida se está llevando a cabo en su propia infraestructura.

Debido al gran riesgo que entraña esta práctica para la vigilancia sin restricciones, los acuerdos de acceso directo deben condenarse. Son solicitudes intrínsecamente desproporcionadas y no están sujetas a ninguna supervisión ni a otras salvaguardias

sólidas. Las empresas deben seguir arrojando luz sobre estos requisitos y concienciando sobre los riesgos inherentes al acceso directo.

2.2. Control judicial

Al promover normas para la protección de la privacidad en la era digital, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos afirmó que:

> *Las medidas de vigilancia, incluidas las peticiones de datos sobre comunicaciones a las empresas y el intercambio de inteligencia, deben ser autorizadas, examinadas y supervisadas por órganos independientes en todas las etapas [...]. El órgano independiente que autoriza las medidas de vigilancia concretas, preferiblemente una autoridad judicial, debe asegurarse de que existen pruebas claras de una amenaza lo suficientemente importante y de que la propuesta de vigilancia tiene un fin específico y es estrictamente necesaria y proporcional, y autorizar (o rechazar) ex ante las medidas de vigilancia.*

Los organismos de derechos humanos y los expertos han afirmado en repetidas ocasiones que las autoridades judiciales independientes son las más adecuadas para autorizar las medidas de vigilancia de las comunicaciones, y que la autorización debe ser *previa*, antes de que tenga lugar la medida de vigilancia. El Tribunal de Justicia de la UE sostuvo que la fiscalía, "cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior", no puede considerarse una autoridad administrativa *independiente* para autorizar el acceso a los datos de las comunicaciones en las investigaciones penales.

No obstante, la legislación local o la jurisprudencia nacional consolidada en los países latinoamericanos imponen retos, o incluso obstáculos, a la iniciativa de los proveedores de servicios de Internet de exigir una orden judicial antes de entregar los datos de las comunicaciones a las autoridades (véase la sección 1.2). En Colombia, la interceptación de comunicaciones privadas solo está sujeta a un control judicial posterior. La Fiscalía General de la Nación está facultada para ordenar la interceptación y proceder a ella antes de que un juez evalúe la validez de la medida.

En Panamá, la Ley 51/2009 autoriza a los fiscales a solicitar una cantidad considerable de metadatos de comunicaciones a los proveedores de telefonía y a los proveedores de servicios de Internet sin más revisión judicial posterior. En Perú, cambios recientes en el Decreto Legislativo 1182 autorizaron a la unidad especializada de investigación policial a solicitar a los operadores de telecomunicaciones acceso a datos de localización de teléfonos móviles o dispositivos electrónicos en tiempo real sin orden judicial previa, más allá de los casos de emergencia en los que exista un riesgo o peligro inminente para la vida humana y la integridad física. Antes de ese cambio, el DL 1182 limitaba esta facultad a los casos en que se estuviera cometiendo un delito (casos de "flagrante delito"). Ahora también abarca las investigaciones preliminares de una importante gama de delitos, como la minería ilegal y los delitos contra la administración pública. El marco legal de Panamá y Perú, sin embargo, exige una orden judicial previa para interceptar el contenido de comunicaciones privadas.

A pesar de que los organismos de derechos humanos y los tribunales internacionales entienden cada vez mejor que los metadatos de las comunicaciones pueden ser tan reveladores e intrusivos como el contenido de las comunicaciones, las leyes nacionales de América Latina siguen tratando los metadatos como menos dignos de protección. Los

"metadatos", como la identificación de las partes que participan en la comunicación, las direcciones IP, las ubicaciones, la hora y la duración de las comunicaciones y los identificadores de dispositivos, pueden revelar las actividades de las personas, dónde viven, sus relaciones, hábitos y otros detalles de sus vidas y rutinas cotidianas. A menudo, los tribunales nacionales tampoco actualizan la protección de los derechos fundamentales para adaptarla a los cambios tecnológicos.

En Paraguay, una sentencia de la Corte Suprema de Justicia de 2010 obstaculiza la aplicación de salvaguardias más estrictas para el acceso de las fuerzas de seguridad a los datos de las comunicaciones. La sentencia 674/2010 sostuvo que la protección constitucional de las comunicaciones en Paraguay solo cubre el contenido de las comunicaciones, por lo que los fiscales pueden solicitar registros de llamadas, información de identificación del abonado telefónico y datos de localización sin una orden judicial previa. Las autoridades policiales de Paraguay se basan en esta sentencia para exigir el acceso a los metadatos sin autorización judicial, a pesar de que la Ley 642/95 de Telecomunicaciones del país establece que tanto el *contenido* como la *existencia de las* comunicaciones no pueden divulgarse salvo por orden judicial. Aproximadamente un año antes de la sentencia de Paraguay, la Corte Interamericana de Derechos Humanos (Corte IDH) reconoció que la protección de la privacidad de las comunicaciones en la Convención Americana sobre Derechos Humanos se aplica tanto al contenido como a los metadatos:

> *[E]l artículo 11 se aplica a las conversaciones telefónicas con independientemente de su contenido, e incluso puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido [...], como cualquier otro elemento del proceso comunicativo mismo; por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada [...]. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación.*

La Corte IDH afirmó que la "fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente". Por ello, "el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada." Las legislaciones internas y los tribunales de los países latinoamericanos deben responder al llamado de la Corte IDH para actualizar adecuadamente la protección otorgada a la privacidad y a la protección de datos. Cabe destacar que en muchos países latinoamericanos la Convención Americana sobre Derechos Humanos tiene el mismo o incluso mayor rango que las propias constituciones nacionales de los países. Por lo tanto, las empresas, entre otras, pueden explorar el litigio estratégico para reforzar las salvaguardias de la privacidad ante las débiles normas locales. Por otro lado, los legisladores y los tribunales no deberían esperar para aumentar las protecciones contra las capacidades de vigilancia cada vez más omnipresentes e intrusivas.

2.3. Transparencia

Las leyes secretas no son leyes. Según las normas internacionales de derechos humanos, una ley solo es una base legítima y válida para autorizar la restricción de la privacidad y

otros derechos si es públicamente accesible. Como subrayó la OACDH al abordar el derecho a la privacidad en la era digital, "las normas y las interpretaciones secretas del derecho no cumplen los requisitos necesarios para considerarse 'ley'." El Relator Especial para la Libertad de Expresión de la CIDH señaló que los Estados deben revelar los procedimientos de vigilancia gubernamental. La información mínima que debe hacerse pública incluye los procedimientos para autorizar la vigilancia, seleccionar objetivos y manejar los datos recopilados, así como los protocolos para compartir, almacenar y destruir los datos.

Sin embargo, la mayoría de las veces los protocolos de vigilancia de las fuerzas de seguridad se consideran secretos. Por ejemplo, mientras que los protocolos peruanos para las escuchas telefónicas por parte de las empresas de telecomunicaciones son públicos, las directrices sobre el intercambio de datos por parte de los ISP con la policía, que aplican el DL 1882, se han declarado "información reservada". En Chile, el Ministerio Público ha desarrollado, y los ISP han aceptado, un protocolo para la interceptación de comunicaciones y otras solicitudes de datos que es secreto para el público en general. Las técnicas de vigilancia del gobierno deben estar sujetas al escrutinio público y a una supervisión independiente para garantizar que los procedimientos respetan los derechos humanos y que existen los controles adecuados. Las directrices públicas de los ISP en materia de aplicación de la ley ayudan a arrojar luz sobre dichos procedimientos, pero la normativa que siguen también debería ser de acceso público.

Además, en virtud del principio de transparencia, los Estados deben publicar información agregada sobre las solicitudes de datos a los proveedores de servicios. Del mismo modo, los Estados no deben interferir en los esfuerzos de las empresas por publicar las estadísticas de las solicitudes gubernamentales de datos de los usuarios. El secreto de las medidas de vigilancia específicas y en curso no debe impedir la publicación de datos agregados sobre las demandas de vigilancia de los gobiernos.

2.4. Notificación a la persona usuaria y derecho de recurso

Notificar a la persona usuaria cuando los gobiernos solicitan su información a los proveedores de servicios es esencial para frenar las solicitudes indebidas y proteger los derechos a la vida privada y al debido proceso. La notificación a las personas les permite prepararse para una defensa legal e impugnar solicitudes potencialmente arbitrarias. Antes de la revolución de la comunicación electrónica, la policía que buscaba información de las personas tenía que llamar a su puerta y mostrar una orden judicial. La persona registrada podía observar si la policía registraba o incautaba su correspondencia escrita y, si consideraba que la intrusión era indebida, pedir la intervención de un tribunal.

La vigilancia electrónica, en cambio, es mucho más subrepticia. Los datos de una persona pueden ser interceptados o adquiridos directamente de los proveedores de telecomunicaciones o de Internet y la persona no es consciente de ello a menos o hasta que los datos se utilicen como prueba que dé lugar a cargos penales. Como resultado, es menos probable que las personas descubran la violación de su derecho a la privacidad. Los tribunales internacionales han reconocido la importancia de notificar a las personas

sometidas a vigilancia. El Tribunal Europeo de Derechos Humanos ha sostenido que la notificación es:

> *[...] indisolublemente ligada a la eficacia de los recursos y, por tanto, a la existencia de garantías efectivas contra el abuso de las facultades de control, ya que, en principio, hay pocas posibilidades de recurso por parte del interesado a menos que éste sea informado de las medidas adoptadas sin su conocimiento y, por tanto, pueda impugnar su justificación a posteriori."*

Del mismo modo, el Tribunal de Justicia de la UE ha subrayado que "las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados deben notificarlo a las personas afectadas [...] tan pronto como dicha notificación ya no pueda poner en peligro las investigaciones que llevan a cabo dichas autoridades". El Alto Comisionado de las Naciones Unidas para los Derechos Humanos también reconoció que los usuarios que hayan sido objeto de vigilancia deben ser notificados después de la medida.

Aunque la obligación de notificar recae principalmente en el Estado, el compromiso voluntario de los ISP de informar a los usuarios sobre las solicitudes de datos gubernamentales, cuando la ley no se lo prohíbe, es un elemento clave para crear una cultura de transparencia y protección de las garantías esenciales de la privacidad. Los países parte del proyecto QDTD tienen leyes que establecen que los procedimientos de interceptación de comunicaciones son por defecto secretos. Pero algunos, como Chile y Perú, tienen obligaciones claras de notificar a la persona usuaria en las condiciones establecidas por la ley.

El secreto sobre la interceptación de las comunicaciones previsto por la ley debe estar limitado en el tiempo y no extenderse automáticamente a otras medidas de vigilancia, como el acceso a los datos almacenados de las comunicaciones. Cuando la ley no lo establezca claramente, el retraso en la notificación a las personas afectadas debe justificarse ante un tribunal y estar vinculado a un peligro real para la investigación o a un daño a una persona. Las autoridades estatales y las empresas no deben interpretar las salvaguardias legales que preservan la confidencialidad de los datos retenidos o capturados por los ISP y entregados a las autoridades para justificar el bloqueo de la notificación a las personas afectadas. La edición 2021 de IPANDETEC muestra los fallos de tal interpretación, utilizada por las empresas en el último informe de Panamá. Mientras que los datos recogidos a través de la vigilancia están restringidos para ser revelados a terceros no autorizados, cuando estos datos se refieren a la persona usuaria, su recopilación y contenido no deben mantenerse en secreto para esta persona. Los derechos tradicionales de acceso, rectificación, cancelación y oposición (ARCO) en los marcos de protección de datos latinoamericanos, especialmente cuando están respaldados por un derecho constitucional, refuerzan el derecho de la persona a saber que su información personal se ha compartido con las autoridades gubernamentales también en el contexto de la aplicación de la ley.

2.5. Compromiso político y evaluaciones de impacto

Los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos (Principios Rectores de la ONU) proporcionan un enfoque basado en principios para que todas las empresas prevengan, mitiguen y remedien los impactos adversos sobre los derechos humanos relacionados con sus actividades. Los principios operativos destacan que las empresas tienen la responsabilidad de respetar los derechos humanos, lo que

incluye asumir un compromiso en sus políticas de respetar los derechos humanos, llevar a cabo la debida diligencia en materia de derechos humanos y proporcionar o cooperar en la reparación de abusos en los casos en que la empresa haya causado o contribuido a causar impactos adversos sobre los derechos humanos.

Teniendo esto en cuenta, el último informe de la ADC para Argentina evaluó qué proveedores de servicios de Internet tienen compromisos claros de política pública para respetar los derechos humanos. De las seis empresas evaluadas, solo IPLAN y Telefónica-Movistar recibieron crédito por haber hecho alguna declaración pública al respecto. Las políticas de Movistar son mucho más completas que las de IPLAN. Además, Movistar también ha ideado y publicado un Modelo de Gobierno de la Protección de Datos Personales, basado principalmente en el cumplimiento del RGPD de la UE. El informe de ADC también identificó qué empresas de telecomunicaciones llevan a cabo evaluaciones de impacto sobre la privacidad y la protección de datos, y si divulgan los resultados de las evaluaciones y/o las medidas de mitigación relacionadas que adoptaron. Telefónica-Movistar fue la única empresa que informó sobre cómo realiza periódicamente evaluaciones de impacto como parte de su debida diligencia en materia de derechos humanos.

Sin embargo, Vivo, filial brasileña de Telefónica, no ha redactado ni publicado una evaluación de impacto sobre la protección de datos (EIPD) para sus operaciones en Brasil, al menos hasta la publicación del informe 2022 de InternetLab. La empresa no ha sido la única. Los investigadores de InternetLab no encontraron EIPD disponibles para ninguna de las empresas evaluadas, aunque el ISP Oi informó haber realizado su primera evaluación en 2021. La Autoridad de Protección de Datos de Brasil recomienda que los controladores de datos realicen EIPD en cualquier contexto en el que las operaciones de procesamiento de datos personales puedan crear un alto riesgo para garantizar los principios de protección de datos y las libertades civiles y derechos fundamentales del interesado. También recomienda a los responsables del tratamiento que hagan públicas las EIPD, de acuerdo con los principios de protección de datos de la legislación brasileña. En este sentido, las empresas de telecomunicaciones deben asumir el compromiso de evaluar y dar respuestas a los impactos adversos de sus actividades empresariales -así como informar sobre los resultados y las medidas adoptadas- dentro de su responsabilidad de respetar los derechos humanos. En consecuencia, la asociación brasileña de proveedores de telecomunicaciones Conexis publicó un Código de Buenas Prácticas en Protección de Datos que detalla los pasos que deben seguir las empresas de telecomunicaciones al realizar sus EIPD. La transparencia y la participación de las partes interesadas, incluidas las personas usuarias, son cruciales para garantizar que los impactos adversos se identifican, analizan y mitigan adecuadamente de forma continua.

Los marcos de protección de datos desempeñan un papel relevante en los criterios que los aliados evalúan en los informes QDTD. La siguiente sección profundiza en las políticas y prácticas de las empresas en relación con los principios y garantías de protección de datos.

3. Marcos de protección de datos: Avances y deficiencias

Varios países latinoamericanos han promulgado leyes de protección de datos. Chile y Argentina aprobaron por primera vez sus marcos de protección de datos hace más de dos décadas, y ahora están debatiendo actualizaciones de la legislación. En una reciente oleada inspirada en el GDPR de la UE, países como Brasil, Panamá y Ecuador aprobaron finalmente leyes integrales de protección de datos. Otros, como Paraguay, tienen proyectos de ley pendientes en el Congreso y aún carecen de un régimen integral que regule el tratamiento de datos personales.

En muchas jurisdicciones de la región, la legislación sobre protección de datos no se aplica a los servicios de inteligencia ni a las fuerzas del orden. En consecuencia, las salvaguardias fundamentales previstas en la normativa de protección de datos no se incluyen en las normas que deben seguir estos organismos cuando procesan información personal. Esta es una laguna que las jurisdicciones latinoamericanas deben abordar para proteger adecuadamente la privacidad de los datos y la miríada de derechos que defiende. Sin embargo, estas lagunas no disminuyen la responsabilidad de los ISP de cumplir con sus obligaciones ante las leyes de protección de datos, incluso cuando responden a las solicitudes de las fuerzas de seguridad para obtener datos de los usuarios.

Mientras que la sección anterior se centraba en la colaboración de las empresas con las autoridades gubernamentales, la siguiente sección considerará los principios y salvaguardias de la protección de datos para destacar los avances que los ISP han hecho con respecto a los informes QDTD y los puntos débiles que aún tienen que superar.

3.1. Políticas de protección de datos

La transparencia está directamente relacionada con la garantía de un tratamiento justo de los datos personales. Comprobar si los proveedores de servicios de internet facilitan de antemano información fácilmente accesible y comprensible sobre qué datos recogen de los usuarios, y por qué y cómo se procesan dichos datos, ha sido un parámetro compartido en todos los informes QDTD desde las primeras ediciones.

Como se señaló en la sección 1.2, la presencia de leyes de protección de datos en algunos de los países investigados no significaba necesariamente que estas políticas estuvieran fácilmente disponibles y fueran fáciles de localizar en sus primeras ediciones. En Colombia, solo un ISP recibió crédito completo en esta categoría en el informe de Karisma de 2015. En Chile, no más de dos empresas lo hicieron en el informe de Derechos Digitales de 2017. Los últimos informes de IPANDETEC muestran cómo encontrar políticas de protección de datos en los sitios web locales de los ISP que cubren la prestación de servicios de internet y telecomunicaciones por parte de las empresas sigue siendo un reto en Panamá y Nicarágua.

A lo largo de los años, los informes QDTD han aumentado el detalle de la información que las organizaciones aliadas buscan en los contratos y las políticas de protección de datos de los ISP. Por el lado positivo, las puntuaciones generales en esta categoría han mejorado en todas las ediciones, incluso con requisitos más estrictos, a medida que se generalizaba la publicación de estas políticas entre los proveedores de servicios. Sin

embargo, en muchos casos las empresas siguen sin proporcionar información básica sobre el tratamiento de los datos personales de los usuarios. A continuación presentamos algunos puntos destacados.

Finalidad del tratamiento

Cabe destacar el contraste entre las primeras y las últimas ediciones en lo que respecta a la divulgación por parte de los ISP de la finalidad del tratamiento de datos personales. Por ejemplo, mientras que solo un ISP brasileño lo hizo en el informe de InternetLab de 2016, todos los ISP investigados en la edición de 2022 recibieron al menos un crédito parcial por revelar esa información. Sin embargo, los avances pueden ser más lentos en contextos locales específicos. En la edición 2022 de TEDIC para Paraguay, por ejemplo, tres de cada cinco empresas seguían sin explicar los fines del procesamiento de los datos de los usuarios. De hecho, Personal y VOX-Hola Paraguay ni siquiera tenían políticas de protección de datos fácilmente accesibles en sus sitios web. Además, el nivel de detalle, y si las empresas van más allá de descripciones vagas de los fines, como "prestar servicios" o "mejorar la experiencia del usuario" es muy variable entre los países del QDTD.

Incluso los informes de lugares con un fuerte trasfondo de protección de datos subrayaron las formulaciones genéricas de finalidad, como la edición de 2018 de Eticas para España. Por su parte, América Móvil-Claro se destaca en algunos países con informes QDTD por proporcionar una interesante tabla (Chile) o una página web detallada (Brasil) que combina los tipos de datos recopilados y los fines relacionados. Sin embargo, la empresa proporciona información completa pero organizada de manera menos amigable en Argentina y Panamá, y una descripción mucho menos exhaustiva en Paraguay. En Brasil, la empresa Oi organizó su política de protección de datos con gráficos y ayudas visuales para facilitar la comprensión de la información, incluidos detalles sobre el tratamiento de datos de no clientes.

Por último, el tratamiento de datos personales con fines publicitarios y de personalización de ofertas comerciales se informa con bastante frecuencia como finalidad autorizada en las políticas de los ISP, aunque va más allá de lo necesario para la prestación habitual de servicios de Internet y telecomunicaciones. Por ello, las empresas deberían ofrecer una oportunidad separada para el consentimiento o, como mínimo, dejar claro a los usuarios cómo pueden optar por la exclusión voluntaria de los fines publicitarios.

Información sobre el almacenamiento de datos personales

Otra información básica que las empresas deberían facilitar de manera sencilla en su política de protección de datos se refiere a si almacenan o conservan los datos de las personas usuarias y durante cuánto tiempo. Las empresas comprometidas con la transparencia y la minimización de datos deberían ser claras sobre qué tipo de datos de las personas conservan en sus bases de datos y los respectivos tiempos de almacenamiento teniendo en cuenta las obligaciones legales y los fines del tratamiento. Aunque aquí también vemos mejoras con respecto a las ediciones QDTD, llama la atención que los ISP sigan necesitando un empujón para revelar adecuadamente esa información. Por ejemplo, todas las empresas que aparecen en los últimos informes de Paraguay y Panamá no lo hicieron. En cuanto a Panamá, IPANDETEC explica que las políticas de Más Móvil y Digicel mencionan que retienen los datos de las personas usuarias, pero no especifican la duración de la retención. Cuatro de los nueve ISP evaluados en Colombia, la mitad de ellos en Chile, y la mayoría en Perú, España y Brasil,

informaron al menos parcialmente sobre la retención o almacenamiento de datos de sus usuarios y usuarias. Los aliados de QDTD en Chile y Brasil también han comprobado si las empresas revelan en qué circunstancias o cómo eliminan estos datos, una información aún más difícil de encontrar en las políticas de las empresas.

Intercambio de datos con terceros

Muchos informes QDTD evalúan si los ISP proporcionan información sobre el intercambio de datos de las personas usuarias con terceros. A menudo, las políticas de las empresas incluyen amplias menciones a la posibilidad de compartir datos con autoridades gubernamentales, a veces especificándolas, y socios comerciales.

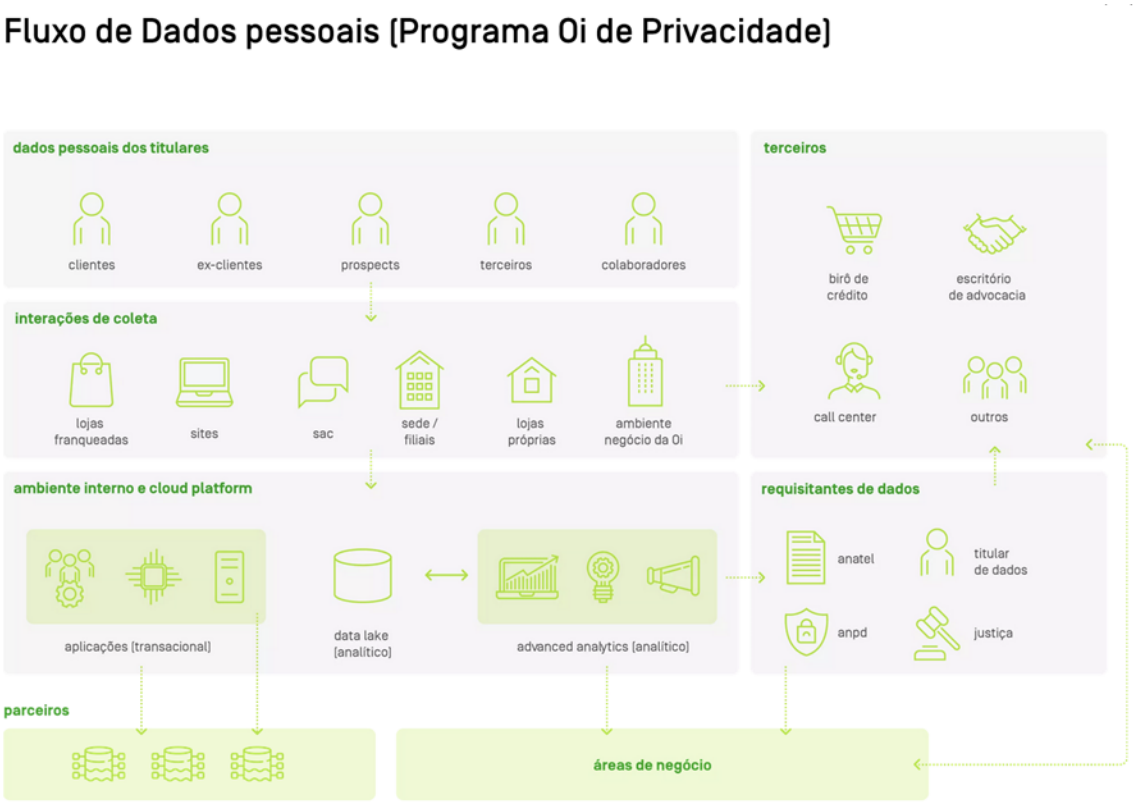
El informe de Paraguay de 2022 destaca también lo contrario: las empresas declaran no compartir los datos de los usuarios sin consentimiento, salvo cuando lo exija la ley o un juez. Copaco establece que no venderá, cederá o distribuirá la información personal que recopile sin el consentimiento del usuario, a menos que sea requerido por un juez con una orden judicial. La propia política no incluye ninguna norma y consentimiento previo en ese sentido. Sin embargo, TEDIC subraya que la política puesta a disposición en la web de Copaco se refiere únicamente a los datos que el ISP recoge del uso de sus apps, y no cubre su prestación general de servicios de internet y telecomunicaciones.

Un compromiso similar se encuentra en la política de Personal. Sin embargo, como señala TEDIC, la misma política establece que la información personal de sus clientes es utilizada por Club *Personal* para proporcionar y mejorar las prestaciones y ofertas de servicios móviles, y puede utilizarse con fines de marketing promocional y/o estadísticos. No hay más información sobre lo que significa Club *Personal* y si está formado por otras empresas o socios. En el informe de Chile 2022, Derechos Digitales se ensaña con VTR por una cláusula en la política del ISP que establece que el usuario, al momento de contratar los servicios de VTR, autoriza tácitamente a terceros a acceder a sus datos de contacto, así como datos sobre los servicios contratados y/o su comportamiento de pago.

Este tipo de cláusulas subrepticias que pretenden apuntalar "autorizaciones" generales y tácitas para compartir datos de las personas usuarias con terceros atentan contra los principios de un tratamiento de datos personales leal y socavan el consentimiento y la autodeterminación del titular de datos como elementos clave de la protección de datos. Las empresas deben abandonar los métodos engañosos, y este tipo de cláusulas no deben considerarse válidas. Si es necesario compartir datos con terceros debido a la complejidad de las operaciones de las empresas, en relación con el almacenamiento de datos, el servicio al cliente, entre otros, esto debe quedar más claro y no mezclarse con otros fines que no sean esenciales para la prestación de servicios, como la publicidad.

Por último, el informe de Brasil de 2022 aumentó los detalles comprobados en las políticas de las empresas sobre este tema. InternetLab evaluó si los ISP informan sobre qué tipo de colaboradores o terceros tienen acceso a los datos de las personas usuarias, y los fines para los que los comparten. Los investigadores también comprobaron si los ISP se comprometen a evaluar el cumplimiento de las normas de protección de datos por parte de terceros. La mitad de las empresas cumplían todos los parámetros, es decir, Claro/NET, Oi y TIM. Claro/NET desglosa la lista de con quién comparte los datos de las personas usuarias y por qué (véase el título *Compartilhamento de dados*). A petición de la persona usuaria, Claro/NET también detalla el nombre de cada tercero con el que la empresa comparte datos. TIM y Oi proporcionan una lista resumida de las categorías de terceros. TIM los detalla según la finalidad de la compartición, de la siguiente manera:

"servicios de tecnología ", "análisis de desempeño", "estudios de mercado" y "para salvaguardar y proteger los derechos de TIM". Oi revela el tipo de terceros: "socios comerciales y de ventas", "oficinas y/o agencias de facturación", "bufetes de abogados", "servicios de centros de llamadas" y autoridades gubernamentales. Es interesante señalar , el gráfico que el ISP ha puesto a disposición que describe el flujo de datos personales (abajo, en portugués):



Transferencias internacionales de datos

En relación con esto, algunos informes QDTD verifican si las empresas mencionan en sus contratos o políticas si realizan transferencias internacionales de datos personales. Esto es importante porque la jurisdicción en la que se almacenan o procesan los datos afecta al régimen legal de normas y protecciones aplicadas al uso y acceso de los datos de las personas usuarias por parte de las autoridades gubernamentales y los particulares. Las leyes de protección de datos de muchos países incluyen normas relativas a la transferencia internacional de datos personales. Estas normas pretenden garantizar un nivel adecuado de protección del derecho de las personas a la protección de datos en el país receptor. Dicha protección incluye salvaguardias apropiadas y recursos legales efectivos para hacer valer los derechos de protección de datos. Básicamente, el régimen jurídico de normas y protecciones aplicado al uso y acceso a los datos de las personas por parte de las autoridades gubernamentales y de los particulares en el país receptor debe ajustarse a las normas de protección de datos del país de origen de los datos.

Las políticas de las empresas que proporcionan información sobre si se producen estas transferencias internacionales, cuándo y por qué es el paso inicial para evaluar si

protegen debidamente los derechos de las personas usuarias independientemente de las fronteras. Los resultados de los informes QDTD son dispares, aunque la mayoría de las empresas evaluadas en los últimos estudios de Brasil, Chile y España mencionan que comparten o pueden compartir datos de los usuarios en el extranjero.

Al menos en el informe de Brasil, estas menciones están relacionadas en su mayor parte con el uso de servicios en la nube para almacenar datos de las personas usuarias. TIM da otros ejemplos, como la prestación de servicios de itinerancia internacional o "cuando contrata a cualquier proveedor relevante para que el ISP preste sus servicios que necesite procesar datos personales de los usuarios en el extranjero", lo cual es una explicación muy genérica en cuanto a tipos de proveedores y circunstancias en las que se necesita una transferencia internacional. TIM también aclara que los proveedores de servicios en la nube pueden cambiar en cualquier momento el lugar donde alojan los datos de los usuarios, pero el ISP trata de limitar contractualmente estas transferencias para que se produzcan de forma segura y a países con leyes que garanticen niveles adecuados de seguridad y protección de datos. Los principales servidores de terceros utilizados por TIM están ubicados en Brasil, en el Espacio Económico Europeo (EEE) y en California, en los Estados Unidos.

A su vez, Algar no especifica en qué casos puede transferir datos personales al extranjero (más allá de enumerar las hipótesis de transferencias internacionales de datos establecidas en la ley de protección de datos de Brasil), ni dónde se encuentran los servidores extranjeros utilizados por la empresa. Sin embargo, Algar declara que el Encargado del Tratamiento de Datos de la empresa debe evaluar cualquier intercambio internacional de datos para comprobar si el país de destino tiene un nivel adecuado de protección de datos en comparación con el ordenamiento jurídico de Brasil. La transferencia también puede producirse cuando el controlador receptor sigue mecanismos como cláusulas contractuales estándar y normas corporativas globales.

En España, el informe 2022 de Eticas comprobó no solo si las empresas proporcionaban información general sobre las transferencias internacionales de datos, sino también si pedían el consentimiento explícito de la persona usuaria o si les ofrecían la posibilidad de no participar en dichas transferencias. Solo cuatro ISP de las 15 empresas evaluadas, incluidos proveedores de telecomunicaciones, sitios web de venta y alquiler de viviendas y aplicaciones para la venta de artículos de segunda mano, obtuvieron pleno crédito en este parámetro.

3.2. Derechos del titular

Otra parte importante de las políticas de las empresas está relacionada con la información a las personas usuarias sobre sus derechos y los mecanismos que la empresa pone en marcha para que se los puedan ejercer. Independientemente de las diferencias entre los marcos jurídicos de protección de datos, un conjunto tradicional de derechos de los titulares de datos en la región comprende los a menudo denominados derechos ARCO (acceso, rectificación, cancelación y oposición). Algunos informes QDTD han evaluado la información que los ISP proporcionan a las personas usuarias en ese frente, y un par de ellos han comprobado la respuesta de los ISP a las solicitudes de los usuarios para acceder a sus datos personales. Aquí resumimos las principales conclusiones.

Información

Desde su primera edición para Argentina en 2018, ADC ha estado verificando si los ISP identifican los derechos del titular de datos en sus políticas. En su momento, Telecentro no lo hizo e IPLAN y Telecom (Arnet) mencionaron los derechos ARCO, pero solo vagamente, enunciando los derechos sin mayor explicación. Lo que es peor, Telecom (Arnet) exigía a quienes solicitaban acceso a datos personales que enviaran físicamente por correo una carta con firma notarial. Además de añadir burocracia, el requisito va en contra de un principio de la ley de protección de datos de Argentina según el cual no se debe cobrar a los usuarios por acceder a sus datos personales. En el informe 2022 de la ADC, todas las empresas evaluadas informan sobre los derechos de los titulares de datos. Pero sigue habiendo altibajos. Esta vez, Arlink es la empresa que exige una carta notarial de la persona usuaria para que pueda tener acceso a sus datos personales. Claro ofrece un formulario, al que no se puede acceder fácilmente a través del sitio web local de la empresa y que, según ADC, requiere una cantidad excesiva de datos personales en comparación con lo estipulado en la ley de protección de datos de Argentina. Por otro lado, IPLAN ofrece una explicación detallada sobre cómo las personas usuarias pueden ejercer sus derechos ARCO y proporciona un formulario estándar que las personas pueden enviar por correo postal o electrónico para acceder a sus datos personales. El formulario incluye grabaciones de cámaras de vigilancia que IPLAN utiliza en sus instalaciones.

La primera vez que InternetLab evaluó este parámetro fue en la edición de Brasil de 2019. A diferencia de Argentina, en ese entonces solo Telefónica-Vivo recibió crédito completo por detallar los derechos ARCO y las formas en que las personas usuarias podían contactar a Vivo para ejercerlos. Los resultados han mejorado significativamente en la edición de 2022. Cinco de los seis ISP evaluados cumplieron totalmente con este parámetro, mientras que Brisanet lo hizo parcialmente. Esto se debe a que Brisanet informa de cómo las personas usuarias pueden dirigirse a la empresa para reclamar sus derechos, pero la descripción que ofrece sobre esos derechos es incompleta e incluso engañosa. InternetLab destaca una cláusula del contrato de banda ancha del ISP que renuncia a las garantías de privacidad de los usuarios para los datos disponibles públicamente, lo que hace caso omiso de las protecciones otorgadas por la legislación brasileña.

Finalmente, IPANDETEC incluyó este parámetro en el último informe de Panamá. Sólo la mitad de las empresas explicaron los derechos ARCO y los medios para ejercerlos-Claro y Más Móvil. Sin embargo, mientras Claro ofrece varios canales que las personas usuarias pueden utilizar para ello (es decir, la cuenta de WhatsApp de Claro, el centro de llamadas o el correo electrónico), quienes deseen solicitar acceso a sus datos personales a Más Móvil deben dirigirse personalmente a la sede del ISP. Si bien es fundamental que las empresas verifiquen la autenticidad de quien solicita el acceso a los datos personales, las personas no deberían incurrir en gastos ni desplazamientos para ejercer este derecho. En cuanto a las otras dos empresas evaluadas, Digicel no menciona los derechos ARCO y proporciona como punto de contacto un correo electrónico no específico para Panamá y un número de teléfono de los EE.UU. Por su parte, Tigo Panamá describe cómo las personas usuarias pueden ejercer sus derechos de acceso y rectificación, pero la política disponible en el sitio web local del ISP se limitaba a los datos de las personas usuarias recopilados a través de las aplicaciones y sitios web de la empresa.

Cumplimiento del derecho de la persona usuaria a acceder a sus datos personales

Este parámetro se evaluó por primera vez en la edición de México de 2016. Los investigadores de R3D verificaron si las empresas de telecomunicaciones móviles respondían adecuadamente a las solicitudes de acceso a datos. Es decir, si ante una solicitud de una persona usuaria, el proveedor móvil le entregó sus datos personales, incluyendo metadatos de comunicaciones, como registros de llamadas y datos de localización, en formato electrónico y dentro del plazo de 20 días establecido en la ley de protección de datos de México. Las tres empresas mencionadas fallaron. AT&T, Telefónica-Movistar y América Móvil-Telcel dejaron a los investigadores de R3D sin respuesta a su petición, incluso después de que la organización solicitara al *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México* que confirmara que los metadatos de comunicaciones son datos personales y que las empresas de telecomunicaciones tenían la obligación de entregarlos a quienes presentaran solicitudes de acceso a los datos.

Más recientemente, InternetLab empezó a comprobar si los ISP brasileños responden puntualmente a las solicitudes de las personas usuarias para confirmar si la empresa procesa sus datos personales o para obtener acceso a dichos datos, siguiendo las normas establecidas en la ley de protección de datos de Brasil. De las seis empresas, solo Claro/NET y TIM cumplían plenamente este parámetro en el informe de InternetLab de 2022. Sin embargo, los datos facilitados por estas empresas se limitaban a la información de identificación de abonados y no incluían todos los metadatos de las comunicaciones de los usuarios que las empresas de telecomunicaciones procesan habitualmente. Algar contestó a tiempo, pero para afirmar que el ISP no procesaba ningún dato personal de la cuenta solicitante, lo que probablemente no sea correcto, ya que la solicitud procedía de un cliente de Algar. Los investigadores de InternetLab no pudieron obtener ninguna respuesta de Oi, y ni siquiera pudieron presentar la solicitud para Vivo debido a problemas técnicos en la aplicación de la empresa.

Por último, Brisanet no proporcionó ningún canal en línea para que los no clientes confirmaran si la empresa procesa sus datos. Los no clientes pueden ver sus datos personales tratados por un operador de telecomunicaciones, por ejemplo, cuando llaman o reciben llamadas de los clientes de ese operador. Tienen el mismo derecho que los clientes a confirmar si la empresa ha tratado sus datos personales y a acceder a ellos. Pero Brisanet exige a los no clientes que envíen una carta física a la sede de la empresa con copias compulsadas de su DNI y su firma. Aunque las medidas de comprobación son pertinentes para verificar si los datos solicitados corresponden a la persona que hace la petición, la empresa debería ofrecer una alternativa en línea y menos burocrática para todas las personas usuarias, no solo para sus clientes.

3.3. Violación de datos: Protocolos y acciones

La forma en que las empresas previenen y enfrentan las violaciones de datos personales es también un componente crítico de las preocupaciones sobre la privacidad y protección de datos. Algunos informes de QDTD lo han analizado con más detalle.

Desde la edición de Colombia de 2017, Karisma evaluó qué ISP proporcionaban información sobre cómo mitigan las violaciones de datos. En aquel entonces, solo Millicom-Tigo y Telebucaramanga obtuvieron buenos resultados en este parámetro

entre los siete ISP destacados. Como subrayó Karisma, los malos resultados obtenidos por América Móvil-Claro y Telefónica-Movistar levantaron una bandera roja para la mayoría de las personas usuarias colombianas que confiaban en estas empresas para proteger sus datos personales. La situación solo mejoró ligeramente en la edición de 2022 de Karisma. Telefónica-Movistar y Millicom-Tigo cuentan con un protocolo y documentación para mitigar las violaciones de datos. Skynet divulga en general qué medidas de seguridad despliega, pero no qué medidas de contingencia aplica el ISP en caso de brechas de seguridad. ETB también facilita información general sobre las medidas de seguridad y cómo hace frente a los incidentes de seguridad, pero no describe medidas de mitigación concretas. Las otras cinco empresas evaluadas no recibieron ningún crédito en esta categoría.

IPANDETEC evaluó por primera vez este parámetro en el informe de Panamá de 2021. Ninguna empresa, a excepción de Millicom-Tigo, tenía información de acceso público que indicara que adoptan un protocolo para informar a las personas usuarias sobre violaciones de datos, a pesar de que la regulación de protección de datos de Panamá establece un deber de notificación en estos casos (en particular el Decreto Ejecutivo 235/2021).

Sin embargo, ni siquiera Tigo proporcionó esa información en el sitio web del ISP para Panamá, sino solo en una página web de Millicom, en inglés, sobre ciberseguridad. Y lo que es más, la página web es algo críptica a la hora de revelar los protocolos de seguridad de la empresa. En ella se afirma que "Millicom ha implantado un marco de riesgos que se basa en una combinación del Marco de Ciberseguridad (CSF) del NIST, así como en la norma ISO/IEC 27001:2013". Al saber que dichos marcos de riesgo implican las mejores prácticas para mitigar y abordar las violaciones de datos, lo que incluye la comunicación interna y pública sobre el incidente de seguridad, los investigadores de IPANDETEC concluyeron que informar a las personas afectadas es parte de los protocolos que adopta Tigo Panamá. Sin embargo, el extracto que mencionamos está lejos de ser informativo para las personas en general.

En Brasil, el informe 2021 de InternetLab comprobó qué ISP adoptaron una postura pública a favor de la seguridad de las personas usuarias proporcionando información concreta sobre estrategias de mitigación de riesgos y prevención de incidentes. Sólo Brisanet no recibió crédito en este parámetro. Entre lo más destacado figuraba un nuevo documento de TIM titulado "Política de seguridad de la información y ciberseguridad", que, entre otras cosas, ofrecía un canal de comunicación específico para casos de seguridad. Pero no todo fueron buenas noticias. Aunque Claro, Oi y TIM obtuvieron una buena puntuación por sus declaraciones públicas relativas a la mitigación de los riesgos cibernéticos, InternetLab señaló que todos ellos no proporcionaron respuestas sólidas a las acusaciones de violación de datos (Claro en 2020, y Oi y TIM en 2021).

Los ISP solo dieron "respuestas genéricas". InternetLab subrayó que "no se dieron explicaciones sólidas sobre el caso, ni se defendió concretamente ninguna norma o técnica que pudiera abordar las acusaciones [de violación de datos]." Telefónica-Vivo también se enfrentó a acusaciones de violación de datos en 2020, y recibió notificaciones de las autoridades de consumo y telecomunicaciones. Según InternetLab, la empresa envió respuestas públicas a las autoridades, afirmando haber evaluado sus sistemas internos y no haber encontrado incidentes de seguridad. Las respuestas no mencionaban ninguna mejora en las medidas de seguridad de Vivo.

3.4. Reconocimiento facial

El uso del reconocimiento facial está aumentando entre los proveedores de servicios móviles, especialmente para las líneas de prepago, como método de verificación para activar los servicios de telecomunicaciones. El reconocimiento facial representa una amenaza inherente a la privacidad, la justicia social, la libre expresión y la seguridad de la información. Las propuestas gubernamentales que exigen a las personas usuarias proporcionar datos biométricos para utilizar los servicios de telefonía móvil suscitaron una gran resistencia de la sociedad civil en México y Paraguay, que han conseguido suspender su aplicación y aprobación legislativa definitiva, respectivamente.

Los informes QDTD empezaron a estudiar más de cerca el uso de esta tecnología por parte de los ISP con la última edición de Brasil. Desgraciadamente, hubo poco compromiso por parte de las empresas. InternetLab no encontró ningún documento público o declaración en contra del uso obligatorio del reconocimiento facial como método de verificación para activar los servicios de telecomunicaciones. Sin embargo, el informe destaca positivamente que Oi no utiliza esta tecnología para registrar a sus usuarios y usuarias. Oi también ha compartido con los investigadores de InternetLab declaraciones emitidas por la empresa que subrayan la importancia de llevar a cabo evaluaciones de impacto cuando los organismos públicos contratan a proveedores de servicios de tecnología de reconocimiento facial.

4. Conclusiones y recomendaciones

La visión general de los logros, retos y tendencias a lo largo de la serie de informes QDTD subraya un importante conjunto de conclusiones.

4.1 Políticas y prácticas de protección de datos

A pesar de los grandes avances, la presencia de leyes de protección de datos en vigor sigue sin corresponderse necesariamente con políticas de privacidad y protección de datos de las empresas que sean exhaustivas y fáciles de encontrar y comprender. Y lo que es peor, no conduce necesariamente a que los ISP pongan a disposición políticas de privacidad y protección de datos que se apliquen a la prestación de servicios de telecomunicaciones en lugar de solo a la recopilación de datos a través de la utilización de sus sitios web y aplicaciones. Este es un desafío particularmente en los mercados más pequeños, como Panamá, Nicaragua y Paraguay, a los que las principales empresas de telecomunicaciones parecen no dar prioridad, al menos en los aspectos que evalúan los informes QDTD. En el caso de Paraguay, aún no existe una legislación integral de protección de datos. De hecho, los obstáculos de aplicación de los marcos de protección de datos en la región no disminuyen la importancia de contar con dichas leyes. En este sentido, surgen tres preocupaciones principales: Los países latinoamericanos que aún carecen de leyes integrales de protección de datos o se basan en leyes obsoletas, la exclusión de las fuerzas del orden y los organismos de inteligencia del ámbito de aplicación de varias leyes de protección de datos de la región, y las legislaciones que no garantizan poderes de supervisión y una estructura eficaces a las autoridades de protección de datos.

En cuanto a las políticas de las empresas evaluadas recientemente en los informes de QDTD, los proveedores de telecomunicaciones siguen sin ofrecer detalles suficientes sobre la información básica acerca de cómo procesan los datos de las personas usuarias. Entre otras lagunas, muchas de sus políticas solo muestran declaraciones genéricas sobre los fines del tratamiento de los datos personales, guardan silencio o dicen muy poco sobre sus protocolos de violación de datos, y carecen de información significativa sobre los plazos de almacenamiento de datos y los procedimientos de supresión de datos, así como sobre el intercambio de datos con terceros (incluso cuando implican transferencias internacionales de datos). Además, existe la problemática práctica de los proveedores de servicios de Internet de mencionar que comparten datos de las personas usuarias con terceros como si esto pudiera funcionar como una autorización general y encubierta para la transferencia de datos a socios comerciales sin que las personas usuarias tengan la oportunidad específica de saberlo o de dar su consentimiento. Aunque las empresas de telecomunicaciones suelen informar mejor a las personas usuarias sobre sus derechos y los medios para ejercerlos, siguen sin garantizar que ellas puedan acceder a sus datos de forma efectiva y práctica.

4.2 Informes de transparencia y directrices para la aplicación de la ley

Los informes de transparencia son tanto una mejor práctica consolidada del sector como un reto persistente. La mayoría o la mitad de los ISP de países como España, Panamá, Paraguay, Perú y Colombia siguen sin revelar información estadística detallada sobre las solicitudes gubernamentales de datos de personas usuarias. Los informes globales de América Móvil y Millicom no proporcionan información estadística por países. Ambas empresas tienen pocas filiales que publiquen informes de transparencia locales, específicos para cada país. El informe de AT&T muestra un desequilibrio significativo en lo que revela sobre los países en los que opera. Comparte mucha más información sobre las demandas gubernamentales en los EE.UU., aunque también proporciona algunos detalles sobre las solicitudes de las fuerzas de seguridad en México. Para el resto de países, la información que proporciona AT&T es mínima. Telefónica es el ISP que mejor equilibra los datos que publica para todos los países en los que presta servicios, mientras que Millicom se destaca por sus informes cualitativos. Con pocas excepciones, los informes de transparencia global no están fácilmente disponibles en los sitios web locales de las empresas de telecomunicaciones.

Asimismo, existe una tendencia cada vez mayor a consolidar la divulgación de las directrices de LE como mejor práctica. Sin embargo, el tipo y el detalle de la información divulgada varían mucho entre los ISP y las sucursales locales de los ISP. De hecho, encontrar directrices de LE locales, específicas de cada país, sigue siendo un reto importante. Los aliados de QDTD no pudieron encontrar ninguna o identificaron muy pocas en Panamá, Paraguay y España. En Perú, solo las grandes empresas publican directrices locales sobre LE. Las directrices globales resumidas no son suficientes para conocer los pasos que dan las empresas ante las solicitudes de datos gubernamentales, ya que no proporcionan información significativa a nivel de país sobre los procedimientos y salvaguardias que deben seguir las autoridades locales.

4.3 Autorización judicial y notificación a la persona usuaria

El margen permitido para unas salvaguardias más sólidas en cada marco jurídico nacional sobre privacidad repercute directamente en los compromisos de las empresas de telecomunicaciones de exigir una orden judicial antes de entregar los datos de los usuarios y usuarias a las autoridades y de notificar a las personas afectadas sobre las demandas gubernamentales de datos. Las leyes nacionales que autorizan a los fiscales o a la policía a acceder a los metadatos sin una orden judicial previa, más allá de las circunstancias de emergencia, no protegen adecuadamente los derechos de privacidad y protección de datos de las personas usuarias. Además, la legislación nacional que establece disposiciones de confidencialidad casi ilimitadas con respecto al acceso gubernamental a datos supone un obstáculo muy preocupante para los compromisos de las empresas de notificar a la persona usuaria acerca de las solicitudes de datos hechas por autoridades gubernamentales. Esto dificulta el ejercicio del derecho a la reparación y nuestra capacidad social para controlar los abusos en la vigilancia gubernamental.

4.4 Compromisos con la privacidad

Salvo contadas excepciones, se trata en general de una categoría difícil de medir en los informes de QDTD, ya que depende en gran medida del acceso público a la jurisprudencia de los tribunales inferiores de los países (como en Brasil) y/o del compromiso de los ISP con los investigadores de QDTD. Las empresas de telecomunicaciones no publican sistemáticamente sus actuaciones ante los tribunales, el Congreso o los debates sobre regulaciones y políticas públicas. Aunque los principales ISP mundiales publican sus posiciones generales sobre debates regulatorios en los sitios web corporativos de sus empresas matrices, no solemos encontrar contenidos similares en las páginas web de sus filiales locales. Es destacable, por tanto, que Claro Chile haya creado una sección específica en su página web para informar sobre sus interacciones con las autoridades públicas, y que Oi en Brasil incluya información sobre sus impugnaciones judiciales a peticiones gubernamentales en el informe de sostenibilidad de la empresa. Cuando los informes QDTD consiguen señalar las acciones de los ISP contra normativas arbitrarias o solicitudes gubernamentales desproporcionadas, o su postura pública a favor de las salvaguardias de la privacidad, los ejemplos que destacan demuestran el papel crucial que desempeñan los ISP a la hora de limitar los abusos de la vigilancia.

Esto refuerza la importancia de que las empresas de telecomunicaciones lleven a cabo evaluaciones de impacto sobre la protección de datos y ejerzan la debida diligencia en materia de derechos humanos, en una visión holística de sus prácticas comerciales y su colaboración con las autoridades gubernamentales. Lamentablemente, aún les queda mucho camino por recorrer en ambos frentes. Aunque algunas grandes empresas mundiales han desarrollado procedimientos internos para cumplir estos requisitos, convertirlos en una práctica consolidada entre los proveedores de servicios de Internet sigue siendo un reto. Las empresas más pequeñas también deberían asumirlo como un

diferencial positivo a su favor. Por último, es preocupante que las empresas de telecomunicaciones con mayor presencia en América Latina, o sus representantes en la región, estén en general al margen de las iniciativas multisectoriales o industriales pertinentes para fomentar el cumplimiento de los derechos humanos por parte de las empresas.

4.5 Tendencias emergentes preocupantes

A lo largo de los años, los informes QDTD han añadido nuevos parámetros para reflejar y responder a la aparición de tendencias preocupantes. Como ya hemos comentado en las secciones 1.2, 1.3, 2.1 y 3.4, entre esas tendencias preocupantes se incluyen los mandatos gubernamentales para acceder directamente a las redes de los proveedores de telecomunicaciones, a menudo sin el conocimiento de la empresa, para obtener los datos de las comunicaciones de las personas usuarias. También incluyen las solicitudes masivas no dirigidas de las fuerzas de seguridad (como las búsquedas inversas en datos de localización), y las solicitudes indiscriminadas de datos relacionadas con políticas públicas sin las salvaguardias adecuadas (por ejemplo, las acciones durante el brote de la pandemia de COVID). Por último, destacamos el creciente uso del reconocimiento facial obligatorio y la recopilación de datos biométricos para activar servicios de telecomunicaciones, especialmente líneas móviles de prepago.

A la vista de estas conclusiones y partiendo de la base detallada establecida por los Principios Necesarios y Proporcionados sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, recomendamos:

Empresas

- Publicar información completa, fácil de usar y detallada por país sobre sus políticas y prácticas de privacidad y protección de datos teniendo en cuenta la prestación de sus servicios de manera general, en lugar de revelar únicamente las prácticas y políticas de tratamiento de datos recopilados en sus sitios web y aplicaciones móviles. Las políticas exhaustivas de privacidad y protección de datos incluyen información significativa sobre cómo almacenan los datos de las personas usuarias (incluido el tipo de datos almacenados, durante cuánto tiempo y qué ocurre después de este periodo), sus prácticas de intercambio de datos con terceros (incluido un desglose de los terceros implicados, los fines del intercambio y el compromiso de evaluar el cumplimiento de las salvaguardias de protección de datos por parte de terceros), las transferencias internacionales de datos y sus fines, y las medidas de seguridad y los protocolos de violación de datos de la empresa, así como información significativa sobre los derechos de los titulares de datos (incluida la forma en que las personas pueden ejercer efectivamente tales derechos).

- Hacer que sus políticas estén disponibles en las lenguas habladas en el país donde prestan servicios, como las lenguas nativas. Proporcionar canales de atención al cliente capaces de ofrecer asistencia en esas lenguas en la mayor medida posible.

- Garantizar el correcto ejercicio de los derechos de los titulares de datos en relación con todos los datos personales que trate la empresa, incluido el derecho de acceso a los datos personales, independientemente de que la persona usuaria sea o no una de sus clientes. La responsabilidad de la empresa de comprobar la autenticidad de la persona que realiza la solicitud no debe suponer una carga para las personas con obstáculos burocráticos o de desplazamiento. La respuesta a una solicitud de acceso a datos personales debe abarcar todos los datos relacionados con esa persona, incluidos los metadatos de las comunicaciones y los datos inferidos (en caso de elaboración de perfiles de usuario, por ejemplo).

- Disponer de políticas, procedimientos y estructura para hacer frente de forma eficaz y transparente a las violaciones de datos. Informar sistemáticamente sobre las acciones de la empresa para garantizar la seguridad y la privacidad al almacenar y procesar de cualquier otro modo los datos de las personas usuarias.

- Abandonar métodos engañosos como la inclusión de cláusulas subrepticias en sus políticas con el fin de "autorizar" ampliamente el intercambio de datos con terceros. Si el intercambio de datos es necesario para las operaciones habituales de las empresas, en relación con el almacenamiento de datos, el servicio al cliente, entre otros, estos fines deben quedar claros en las políticas de las empresas, y no mezclarse con otros fines que no sean esenciales para la prestación de servicios, como la publicidad. En tales casos, los proveedores de servicios de Internet deben ofrecer una oportunidad separada para el consentimiento o, como mínimo, dejar claro a las personas usuarias cómo pueden optar por no participar.

- Informar públicamente y, en la medida de lo posible, ser transparentes sobre los acuerdos de intercambio de datos con fines de investigación penal, inspección o política pública. Arrojar luz sobre los requisitos de acceso directo y concienciar sobre sus riesgos inherentes.

- Publicar informes estadísticos de transparencia detallados sobre todos los accesos gubernamentales a los datos de sus clientes. Como mínimo, desglosar los datos agregados por país, tipo de datos (interceptación de contenidos, metadatos e información de identificación de abonados), número de solicitudes aprobadas y rechazadas, y número de accesos de personas usuarias afectadas. Los informes locales de transparencia en los estudios de QDTD muestran que los ISP también pueden proporcionar otros datos agregados importantes, como el número de solicitudes de localización en tiempo real, el número o la proporción de solicitudes dirigidas o individualizadas *frente a las* solicitudes masivas, las razones para rechazar las solicitudes gubernamentales y un desglose de las demandas por autoridad solicitante en combinación con el tipo de datos solicitados.

- No considerar las disposiciones legales sobre el secreto de las comunicaciones privadas y la confidencialidad de las medidas de investigación *per se* como una prohibición para publicar informes de transparencia con datos agregados específicos de cada país sobre las solicitudes gubernamentales. Cuando las

autoridades gubernamentales adopten una interpretación de este tipo, explorar vías para colaborar con ellas con el fin de superar interpretaciones estrictas de la ley o considerar formas de impugnar ante los tribunales una limitación tan desproporcionada de la transparencia.

- Publicar directrices para los organismos gubernamentales que buscan datos de las personas usuarias. Es importante que el público sepa cómo la policía y otros organismos públicos obtienen los datos de los clientes de los proveedores de servicios. Para garantizar el acceso público a esta información, los proveedores deben publicar de forma transparente las directrices que proporcionan a las agencias gubernamentales. Ya sea en su informe de transparencia o en las directrices LE, las empresas deberían incluir y definir qué entienden por metadatos, aclarando qué tipo de datos de las personas usuarias se incluyen en esas categorías notificadas. También deberían detallar, para cada país, el marco legal aplicable para el acceso gubernamental a los datos y las autoridades competentes para solicitar cada categoría de datos de usuario.

- Adoptar las interpretaciones más protectoras de los marcos jurídicos nacionales para exigir una orden judicial antes de entregar los datos de las personas usuarias a las autoridades, excepto en casos de emergencia cuando exista un riesgo inminente de peligro para la vida humana (véanse los Principios 6 y 7). Impugnar las solicitudes gubernamentales arbitrarias o desproporcionadas de datos de personas usuarias, incluidas las solicitudes masivas no individualizadas, como las búsquedas inversas de localización.

- Notificar a las personas usuarias sobre las solicitudes de datos hechas por autoridades gubernamentales en la primera oportunidad que permita la ley, incluso en casos no penales (véase el Principio 8). Colaborar con las autoridades gubernamentales para estudiar la mejor manera de aplicar la notificación a las personas afectadas de acuerdo con los marcos jurídicos nacionales. No interpretar de forma amplia el secreto sobre los procedimientos de interceptación de comunicaciones para que cubra automáticamente otras medidas de vigilancia, como el acceso a los datos de comunicaciones almacenados. Además, la confidencialidad de los datos de las personas usuarias no debe justificar las limitaciones impuestas a la empresa para notificar a las personas al que se refieren los datos, ya que dicha confidencialidad sirve para proteger a las personas usuarias, no para cegarles ante las solicitudes de terceros a sus datos.

- Evaluar las oportunidades de litigio estratégico para reforzar las salvaguardias de la privacidad presentes en las normas constitucionales y de derechos humanos frente a las débiles normas locales. En la medida de lo posible, participar en los debates políticos y legislativos locales en defensa de unas salvaguardias sólidas de la privacidad y la protección de datos. Divulgar información específica de cada país sobre litigios y esfuerzos y acciones a favor de la privacidad y la protección de datos de las personas usuarias.

- Adoptar compromisos políticos claros, exhaustivos y sólidos para respetar los derechos humanos en el suministro de sus productos y servicios. Realizar evaluaciones de impacto sobre la protección de datos y los derechos humanos de forma continua, publicando sus resultados e informando sobre las medidas de mitigación que haya adoptado la empresa.

- Comprometerse con iniciativas multisectoriales e industriales comprometidas con la defensa de la privacidad, la protección de datos y la libertad de expresión en la prestación de servicios de telecomunicaciones y acceso a Internet. Garantizar la participación de representantes de empresas que puedan abordar adecuadamente el contexto latinoamericano y sus retos particulares.

Entendemos que muchas de estas recomendaciones pueden suponer un reto para los ISP más pequeños. Aunque el respeto de los derechos humanos y la prevención y mitigación de los daños deben integrarse regularmente en las prácticas y planes empresariales de cualquier proveedor de servicios de Internet, las instituciones de derechos humanos, las autoridades de protección de datos, las asociaciones del sector y las organizaciones de la sociedad civil pueden desempeñar un papel a la hora de proporcionar orientación y comentarios sobre cómo las empresas pueden lograrlo de la manera más eficaz posible.[9] Además, todos estos actores hacen parte de un ecosistema más amplio cualificado para abogar, tanto a nivel local como regional, por unas sólidas salvaguardias de la privacidad y la protección de datos en la prestación de servicios de telecomunicaciones e Internet.

Estados

Cualquier limitación impuesta a los derechos humanos debe estar prescrita por la ley, y ésta debe ser lo suficientemente accesible, clara y precisa como para que las personas tengan conocimiento previo de su aplicación y puedan preverla. La limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y la opción menos intrusiva disponible. Cualquier limitación del derecho a la vida privada no debe privar de sentido a la esencia del derecho y debe ser coherente con otros derechos humanos, incluida la prohibición de discriminación. Cuando la limitación no cumple estos criterios, la limitación sería ilegal y/o la injerencia en el derecho a la intimidad sería arbitraria. El deber de los Estados de respetar y garantizar el derecho a la privacidad implica la adopción adecuada de salvaguardias procesales y la supervisión efectiva de los poderes de vigilancia del gobierno. Hemos detallado dichas salvaguardias a lo largo de los Principios Necesarios y Proporcionados. Las recomendaciones que figuran a continuación articulan este conjunto de principios con las conclusiones de los informes QDTD. En este sentido, los Estados deberían

- Establecer marcos jurídicos de protección de datos completos y eficaces. Garantizar a las autoridades de protección de datos unas competencias y una estructura de supervisión sólidas e independientes. Los marcos jurídicos de protección de datos y el mandato de las autoridades de supervisión deben

[9] Por ejemplo, el proyecto B-Tech de la OACDH proporciona orientación y recursos para aplicar los Principios Rectores de las Naciones Unidas sobre las empresas y los derechos humanos en el espacio tecnológico. Disponible en: https://www.ohchr.org/en/business-and-human-rights/b-tech-project

aplicarse tanto a las partes privadas como a las estatales, incluidas las fuerzas de seguridad y los servicios de inteligencia.

- Publicar informes de transparencia sobre las demandas gubernamentales para acceder a la información de los clientes. El Relator Especial de la ONU para la Libertad de Expresión ha pedido a los Estados que divulguen información general sobre el número de solicitudes de interceptación y vigilancia que han sido aprobadas y rechazadas. Dicha divulgación debe incluir un desglose de las demandas por proveedor de servicios, autoridad de investigación, tipo y propósito de la investigación, número de personas o cuentas afectadas, y período cubierto. Los Estados no deben interferir con los proveedores de servicios en sus esfuerzos por publicar estadísticas de solicitudes de datos gubernamentales y los procedimientos que aplican al evaluar y cumplir con dichas solicitudes (véase el Principio 9).

- Ser cauteloso con los acuerdos de intercambio de datos con el gobierno con fines de política pública o de inspección (véase el apartado 2.1). Empréndalos solo cuando sea necesario y proporcionado para la consecución de un objetivo legítimo en una sociedad democrática, y sobre la base de un fundamento jurídico coherente y democráticamente aprobado. La base de cualquier política gubernamental que implique el tratamiento de datos que afecte a personas y/o grupos debe incluir normas sólidas de no discriminación y protección de datos, con salvaguardias como la minimización de datos, la limitación de la finalidad y el consentimiento. También debe incluir medidas concretas y efectivas para garantizar la seguridad, la transparencia y la rendición de cuentas, y el control de la comunidad, y que las políticas intensivas en datos sean legítimas, necesarias y eficientes. Esto incluye una participación cívica significativa sobre *si* estas políticas deben concebirse, aplicarse o mantenerse y *cómo*.

- Revisar la legislación para garantizar que establece sólidas salvaguardias de privacidad para el acceso de los gobiernos a los datos, teniendo en cuenta el panorama tecnológico actual y las potentísimas capacidades de vigilancia que permite. La legislación nacional debe restringir específicamente los poderes de investigación en su alcance y duración a la investigación y el enjuiciamiento penal específicos. Debería exigir una autorización judicial previa por parte de una autoridad judicial imparcial e independiente antes de que las fuerzas del orden accedan a los datos de los usuarios. La revisión judicial posterior solo debería aplicarse en casos de emergencia, cuando exista un riesgo inminente de peligro para la vida humana. Los Estados no deben basarse en categorizaciones artificiales de los datos (por ejemplo, "datos de abonado" o "metadatos") para renunciar a la autorización judicial previa o para justificar cualquier injerencia desproporcionada en la privacidad. Las injerencias en la vida privada de las personas usuarias también deben basarse en evidencias sólidas. Los Estados deben garantizar mecanismos de reparación eficaces y una supervisión judicial rigurosa por parte de un organismo regulador independiente.

- Establecer y/o aplicar de forma efectiva la obligación legal de un Estado de notificar a todos los individuos afectados por medidas de vigilancia

gubernamental. Dicha notificación debe producirse con tiempo e información suficientes para permitirles impugnar la decisión o buscar otros recursos. El retraso en la notificación solo está justificado cuando pueda poner en peligro la investigación o el enjuiciamiento, o suponer un riesgo inminente de peligro para la vida humana. La autoridad judicial competente debe autorizar dicha demora en cada caso y asegurarse de que se notifica a la persona afectada tan pronto como desaparezca el riesgo (véase el Principio 8). Cualquier medida que impida a un proveedor de servicios notificar voluntariamente a los usuarios debe ser excepcional, de duración limitada y estar sujeta a criterios estrictos con razones claras y convincentes para imponer tales restricciones. De lo contrario, privados del conocimiento de una medida intrusiva, los individuos objeto de la misma se quedan con muy pocos o ningún recurso para luchar o buscar reparación contra la vigilancia ilegal o arbitraria.

- Abandonar la condenable práctica de adoptar normas, protocolos e interpretaciones secretas de la ley en el contexto del acceso de los gobiernos a los datos. Los gobiernos que lleven a cabo actividades de vigilancia deben asegurarse de que lo hacen de conformidad con un marco jurídico nacional que cumpla las normas exigidas por el derecho internacional de los derechos humanos. Como tal, cualquier legislación que regule la vigilancia debe ser clara, precisa y accesible al público.[10]

- Poner fin a los mandatos de vigilancia desproporcionados. Los gobiernos no deben exigir a los proveedores de servicios de Internet y a los operadores de telecomunicaciones que concedan acceso directo a sus redes o servidores. Las búsquedas indiscriminadas y sin sospechosos de los datos de las comunicaciones tampoco cumplen las normas necesarias y proporcionadas (véase el apartado 2.1). Los tribunales y los legisladores nacionales no deben apoyar ni consentir estas prácticas. Por el contrario, la jurisprudencia y la legislación nacionales deben defender las normas internacionales de derechos humanos y las normas constitucionales garantizando salvaguardias suficientes para restringir la vigilancia gubernamental arbitraria y desproporcionada.

- Abandonar el reconocimiento facial y otros mandatos de recogida de datos biométricos para que las personas puedan activar y beneficiarse de los servicios de telecomunicaciones.

[10] Véase la Resolución del Consejo de Derechos Humanos de las Naciones Unidas sobre el derecho a la privacidad en la era digital, UN Doc A/HRC/RES/48/4 (7 de octubre de 2021). Véase también Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, El derecho a la privacidad en la era digital, UN Doc A/HRC/27/37 (30 de junio de 2014), párrafo 29; e Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, UN Doc A/HRC/41/35 (28 de mayo de 2019), párrafo 50.