¿QUIÉN DEFIENDE TUS DATOS?

BUSCANDO LA TRANSPARENCIA DE LOS INTERMEDIARIOS DE INTERNET EN PARAGUAY

Maricarmen Sequera

ABRIL 2017

TEDIC
TECNOLOGÍA & COMUNIDAD

EFF

Quien Defiende Tus Datos es un proyecto desarrollado por TEDIC
y forma parte de una iniciativa regional en cinco países de América Latina
coordinada por Electronic Frontier Foundation,
una organización internacional sin fines de lucro que desde 1990
defiende la libertad de expresión y la privacidad en el entorno digital.

Consulta esta investigación en:
https://qdtd.tedic.org

Colaboradores: Katitza Rodriguez y Kurt Opsahl de EFF
Edición y diagramación: Luis Alonzo Fulchi
Comunicación: Jazmín Acuña
Diseño: Guada Lobo

Resumen Ejecutivo

Introducción

"¿Quién Defiende Tus Datos?" es un proyecto de TEDIC (Tecnología y Comunidad), la organización de derechos digitales más importante en Paraguay y EFF (Electronic Frontier Foundation), que busca impulsar buenas prácticas entre las proveedoras de Internet para que protejan los derechos humanos y ofrezcan información clara sobre el uso de los datos de las personas que contratan sus servicios de Internet.

Se evalúan las *6 empresas de telecomunicaciones* más importantes del país, que comprenden la gran mayoría del mercado de telefonía fija, móvil y banda ancha. Estas son: Tigo, Personal, Copaco, Vox, Claro y Chaco Comunicaciones.

Para la evaluación de las proveedoras de Internet se ha tenido en cuenta los estándares de derechos humanos y empresas, tales como los *Principios Rectores sobre las Empresas y Derechos Humanos* de la Organización de las Naciones Unidad, la *Guía de Implementación de los Principios Rectores* para el Sector TIC elaborada por la Comisión Europea; la *Guía de Implementación* de la Iniciativa de Internet Global (Global Network Initiative).

También se incorporan los resultados de *"Who has your back?"* el proyecto regional liderado por Electronic Frontier Foundation, con participación de organizaciones como R3D de México, Fundación Karisma de Colombia, Hiperderecho de Perú e InternetLab de Brasil.

Por otro lado, para este informe, se adoptan los estándares de protección de privacidad expuestos en la Constitución de la República del Paraguay, tratados internacionales ratificados por Paraguay y decisiones de la Corte Suprema y la Corte Interamericana de Derechos Humanos.

El reto más importante de las proveedoras de Internet en Paraguay es ampliar el compromiso con la transparencia y respectar los derechos humanos. Es necesario promover la transparencia más allá de la gestión financiera. Este informe sirve como una herramienta que refleja la importancia de rendir cuentas sobre los datos personales quienes contratan estos servicios.

El presente informe continuará periódicamente con evaluaciones realizadas de forma anual. Cada versión revelará la metodología y resultados, garantizando que los mismos estén dentro del alcance y las posibilidades de cumplimiento por parte las empresas evaluadas para que defiendan tus datos.

Criterios de Evaluación

Se utilizaron 6 criterios para evaluar las *prácticas y políticas de privacidad* de cada compañía, basados en los siguientes puntos de vista:

- Compromiso público de proteger la privacidad;
- Adopción de prácticas y políticas en favor de los usuarios;
- Transparencia de las prácticas y políticas.

A continuación se desarrollan cada uno de los criterios:

1. Políticas de privacidad y protección de datos personales

> *La compañía cuenta con una política de privacidad y de protección de datos personales, utilizando un lenguaje claro y libre de tecnicismos. Informa a las personas sobre la recolección, uso, almacenamiento, procesamiento de sus datos personales. En particular, este instrumento debe ser visto como una oportunidad para informar de manera clara a los usuarios respecto de sus derechos y no debería ser visto como un mero formalismo legal. La compañía también cuenta con políticas de privacidad frente a las autoridades gubernamentales. La misma describe cual es el procedimiento legal para entregar a la justicia los datos de sus usuarios en el caso que haya una investigación criminal bajo solicitud del juez competente.*

Al respecto, tanto la *Constitución de la República* en su artículo 33 —Sobre la Intimidad de las personas— como los *Tratados Internacionales* protegen el derecho a la intimidad como uno de los pilares de las democracias modernas. Asimismo organismos internacionales de protección de *Derechos Humanos* han señalado que las empresas deben establecer e implementar condiciones de servicio que sean transparentes, claras, accesibles, así como apegarse a las normas y principios internacionales de Derechos Humanos; incluyendo las condiciones en las que pueden generarse interferencias con el derecho a la

privacidad de los usuarios[1]. Es indispensable que la compañía cuente con políticas que cumplan estos protocolos a la hora de entregar información personal y datos personales a las autoridades.

Por otra parte, los metadatos forman parte de la comunicación y tienen el carácter de inviolabilidad tal como se desprende del artículo 36 de la Constitución Nacional:

> *"No podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley...".*

Las empresas deben almacenar los metadatos de sus usuarios por un mínimo de 6 meses según el artículo 10 de la ley de Comercio Electrónico 4868/2013. En este escenario, es imprescindible que las ISPs describan y den a conocer qué información personal está siendo retenida, así como las medidas para salvaguardar dichos datos ante posibles ataques o riesgos que puedan afectar dicha información.

El art. 10 de la ley 4858/2013 dice:

> *"Los Proveedores de Servicios de Intermediación y los Proveedores de Servicios de Alojamiento de Datos deberán almacenar los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio, por un período mínimo de 6 (seis) meses, en los términos establecidos en este artículo. Para el cumplimiento de lo dispuesto en este artículo, los datos serán almacenados únicamente a los efectos de facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.*
>
> *Los Proveedores de Servicios de Alojamiento de Datos deberán almacenar sólo aquéllos datos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.*

1 CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 112.

> *No podrán utilizar los datos almacenados para fines distintos a los que estén permitidos por la ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos".*

En un caso contencioso[2] reciente en el que se condenó al Brasil por el uso ilegal de escuchas telefónicas en un proceso penal, la Corte Interamericana señaló que el derecho a la privacidad protege tanto al *contenido* de la comunicación electrónica como a otros datos propios del proceso técnico de la comunicación, como ser los *metadatos* o *datos de tráfico*. Esta jurisprudencia vinculante a la jurisdicción nacional paraguaya, sitúa a estos datos en una instancia de protección constitucional y de derechos humanos.

Por otro lado, la ley 4868/2013 de Comercio Electrónico y su decreto reglamentario 1165/14 obliga compulsivamente a informar y proteger los datos de los usuarios:

> *Art 9 de la ley 4868/2013: "Obligación de los Proveedores de Servicios de Intermediación. Los Proveedores de Servicios de Intermediación consistentes en la prestación de servicios de acceso a Internet, estarán obligados, sin perjuicio de las disposiciones vigentes sobre los Servicios de Acceso a Internet y Transmisión de Datos establecidas por la Autoridad Competente, a: a) informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; b) informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en Internet o que puedan resultar nocivos para la niñez y la adolescencia; Esta obligación de información se tendrá por cumplida si el correspondiente Proveedor incluye la información exigida en su página o sitio principal de Internet. a) suspender el acceso a un contenido o servicio cuando un órgano competente, en ejercicio de las competencias que legalmente tenga atribuidas, requiera que se interrumpa la prestación de un servicio o que se retire algún contenido que vulnere lo dispuesto en el Artículo 6°".*

2 Corte I.D.H. Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas) , párr. 114.

> *Art 11 del reglamento 1165/14: "Deber de Informar y Protección de Datos. El proveedor de bienes y servicios por vía electrónica a distancia, debe poner a conocimiento del consumidor o usuario la finalidad y el tratamiento que se le daría sus datos personales, conforme a la Ley vigente relativa a la materia. Así mismo, debe comunicar el destinatario de los datos suministrados y el responsable de custodiar o almacenar la información proporcionada. El proveedor de bienes y servicios empleará sistemas seguros para evitar la pérdida, alteración y acceso de terceros no autorizados a los datos suministrados por el consumidor o usuario."*

La Institución garante y responsable del cumplimiento de la ley de Comercio Electrónico es el Ministerio de Industria y Comercio, que tiene como atribución la coordinación de inspecciones y controles a los distintos proveedores de Internet. Inclusive debe aplicar sanciones por las faltas no previstas específicamente en la ley de *defensa del consumidor* y establecidas en la ley de Comercio Electrónico.

2. Autorización judicial

> *La vigilancia sin consentimiento del afectado conlleva riesgos de abusos por las autoridades, por ello resulta imprescindible la autorización de un juez competente. Para solicitar información personal debe haber una autorización del juez competente tal como lo expresan las normas penales y la Constitución Nacional del Paraguay. La interceptación de la comunicación privada de las personas tiene carácter excepcional con pena de nulidad en el juicio. Este criterio implica verificar si la compañía cuenta con políticas que cumplan los protocolos para entregar la información a la autoridad judicial. Es decir, detalles del expediente penal, número de causa, datos de la persona, el tipo base penal que incurre el investigado, argumentación legal y firma del juez de la causa.*

La Constitucional Nacional en el artículo 36 sobre la inviolabilidad de las comunicaciones obliga a las autoridades del Estado a solicitar información a las compañía *sólo a través de una orden judicial* debidamente justificada.

La siguiente imagen ilustra el mecanismo de solicitud de dicha información:

El debido proceso para una interceptación de información

3. Notificación al usuario

> *La compañía deberá contar con una política de notificación a usuarios afectados por medidas de vigilancia estatal, en el primer momento permitido por la ley. Deberá demostrar que han litigado los impedimentos legales o regulatorios para llevar a cabo la notificación y publicar de forma accesible que ha promovido mecanismos de notificación al usuario al congreso o a otros entes regulatorios.*

Cuando a los usuarios se les dice que su información de cuenta o de conexión a Internet fueron exigidas por las autoridades administrativas o judiciales, hay una expansión de las oportunidades de ejercer efectivamente su derecho de defensa contra los abusos e irregularidades. El fuerte impacto de las notificaciones para garantizar una defensa efectiva en el Estado de Derecho no es una idea nueva. A la luz del principio constitucional del debido proceso, muchas leyes establecen la obligación de notificar a las personas sobre las medidas que afectan a sus derechos.

Por su parte el Código Procesal Penal en su artículo 151 y Resolución de la Corte Suprema de Justicia de Paraguay disponen la obligación de notificar a la persona, cuando el Ministerio Público le ha imputado por un supuesto hecho punible.

Este derecho de *notificación a las personas afectadas* por medidas de vigilancia ha sido reconocido por especialistas en Derechos Humanos en Internet y fue plasmado en un documento llamado *"Necesario y proporcionados"* y dice lo siguiente:

> *"Es imposible que una persona impugne efectivamente la interferencia de un gobierno en su vida privada si no sabe si ha sido víctima. En líneas generales, la falta de transparencia respecto a la aplicación de las leyes que rigen la vigilancia encubierta puede impedir el control democrático significativo de esas leyes"*[3].

Por otro lado, la *Relatoría Especial Sobre Derechos Humanos de la Organización de las Naciones Unidas* expresó su opinión al respecto:

> *"Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accedidas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones"*[4].

Es decir, la notificación podría no poder llevarse a cabo de inmediato en tanto se podría frustrar el éxito de una investigación, pero debería al menos efectuarse cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento no genere un riesgo inminente de peligro a la vida o integridad de alguna persona. Actualmente existe un vacío legal sobre este punto en el Código Procesal Penal respecto a la protección de

3 *"Necesario y proporcionado"*. Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. Versión Mayo 2014. Página 36

4 Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40

los Derechos Humanos en el marco de derecho a la intimidad y un juicio justo. Esto no invalida a la compañía del deber de actuar *de buena fe* para salvaguardar la intimidad de sus usuarios, notificándoles sin poner en peligro el objetivo de la investigación penal.

En casos adversos a la implementación de la política de notificación de la empresa, la compañía deberá combatir judicialmente los impedimentos legales para notificar a usuarios afectados, al menos, luego de que haya transcurrido un tiempo razonable para que no se frustre el objeto de la medida de vigilancia. Otra medida, sería llevar a cabo acciones de incidencia legislativa o regulatoria para la implementación de mecanismos legales de notificación.

En el contexto de las *solicitudes de datos personales*, las proveedoras de Internet adquieren un papel esencial en la protección de las garantías procesales de los usuarios afectados. Es decir, la notificación por la empresa permite al usuario desafiar las solicitudes ilegales: tanto órdenes judiciales sin fundamento, como solicitudes de las autoridades administrativas sin competencia ni justificación. En la situación actual, el usuario depende de los retos realizados por las propias empresas contra las peticiones que consideran abusivo. Si el usuario es notificado, obtiene a la mayor brevedad, la capacidad de defenderse de posibles violaciones de su privacidad.

Con esto en mente, creemos que es importante fomentar la práctica de la notificación al usuario a través del proyecto *"¿Quién defiende tus datos?"* (WHYB). En los casos en que las solicitudes de datos no van acompañadas de la obligación de confidencialidad, la notificación es permitida por la ley paraguaya (dada la ausencia de prescripción legal en contrario). La posibilidad de notificación de usuario puede ser necesaria, no sólo en los casos de solicitudes de datos en procesos civiles, sino también en relación con las solicitudes hechas por otras agencias gubernamentales, tales como el Ministerio de Hacienda o CONATEL. Se fortalece la posibilidad de desafío legal a la presentación de pruebas irrelevantes a los hechos del caso.

En esta edición, hemos decidido esta categoría sería una "prima", porque la notificación no es ni una obligación legal impuesta a las empresas ni una práctica generalizada en el país. Es una medida vista como innovadora y en cierta medida costosa (debido a que requiere personal dedicado a las notificaciones). Por estas razones, su adopción revelaría un compromiso especial con el avance de la protección de los derechos de los usuarios, especialmente digno de ser observado. La *notificación al usuario*, a la primera oportunidad legalmente posible, y preferiblemente antes de la divulgación de los datos, colabora con los principios de defensa legal, y fomenta una cultura de protección de la privacidad.

4. Posicionamiento público en contra de la vigilancia masiva o sin control

> *Es determinante para el respeto y protección de los derechos humanos de los usuarios y generar confianza en torno al ecosistema de Internet, es indispensable el compromiso público y posicionamientos sobre políticas públicas, legislaciones nacionales que afecten la tecnología con perspectiva de Derechos Humanos.*

En este parámetro se analiza si la compañía tiene un posicionamiento institucional público en el que haya reconocido sus responsabilidades de *respeto y protección de derechos humanos*, incluyendo el *derecho a la privacidad*. Para este efecto, se analiza si existe algún posicionamiento que cumpla con las características señaladas por el Principio 16 de los Principios Rectores sobre las Empresas y los Derechos Humanos aprobados por el Consejo de Derechos Humanos de la Organización de las Naciones Unidas a través de la resolución 17/4, de 16 de junio de 2011 a saber:

> *"Compromiso Político*
>
> *16. Para asumir su responsabilidad de respetar los derechos humanos, las empresas deben expresar su compromiso con esta responsabilidad mediante una declaración política que:*
>
> *a) Sea aprobada al más alto nivel directivo de la empresa;*
>
> *b) Se base en un asesoramiento especializado interno y/o externo;*

> *c) Establezca lo que la empresa espera, en relación con los derechos humanos, de su personal, sus socios y otras partes directamente vinculadas con sus operaciones, productos o servicios;*
>
> *d) Se haga pública y se difunda interna y externamente a todo el personal, los socios y otras partes interesadas;*
>
> *e) Quede reflejada en las políticas y los procedimientos operacionales necesarios para inculcar el compromiso asumido a nivel de toda la empresa."*

El posicionamiento político debe ser público y reflejar claramente el compromiso de la empresa de respetar los derechos humanos en el marco de sus actividades empresariales.

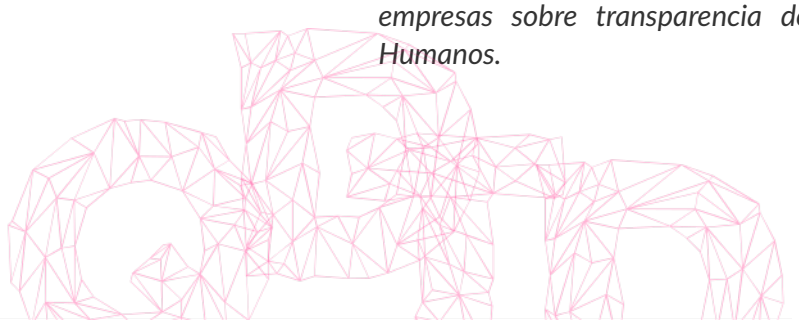
En este criterio se evalúa si la compañía ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad.

También se evalúa, si participa en algún mecanismo sectorial o multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales (Ejemplos: *Global Network Initiative* o *Telecommunications Industry Dialogue*).

Por otro lado, es esencial que la compañía cuente con políticas de participación en las discusiones locales e Internacionales sobre el ecosistema de Internet; los Foros de Gobernanza de Internet (IGF) son espacios de debate público propiciados por Naciones Unidas, donde se discutan de forma abierta los principios compartidos, normas, reglas, procesos de toma de decisión y programas, que modelan la evolución y el uso de Internet.

5. Transparencia

> *El Principio 21 de los Principios Rectores sobre las Empresas y los Derechos Humanos de Naciones Unidas, exige buenas prácticas a las empresas sobre transparencia desde la perspectiva de los Derechos Humanos.*



Los *informes de transparencia* para el sector de las TIC, en relación al impacto que las mismas provocan en la privacidad de los usuarios, han sido elaborados de forma más frecuente en los últimos años[5]. La publicación de un informe de transparencia sobre las *solicitudes de acceso a datos* por parte de autoridades de seguridad y justicia debe proveer suficiente información para evaluar el contenido y el alcance de las medidas de vigilancia por parte de las autoridades.

Los *informes de transparencia* son declaraciones emitidas por empresas que contienen una variedad de estadísticas relacionadas con las solicitudes de datos. Las empresas de Internet de todo el mundo han adoptado la práctica de publicar informes de transparencia activa para informar cómo y cuándo cooperan con el gobierno, en general, porque lo exige la ley, mediante la divulgación de información que puede ser utilizada como prueba en los casos civiles y penales. Esta ya es una buena práctica establecida entre empresas de contenidos como Google, Facebook, Twitter y Microsoft y los proveedoras como Vodafone y Verizon.

Este criterio evalúa la publicación de estadísticas respecto a cuántas solicitudes de información han sido recibidas y cumplidas, así como la inclusión de detalles sobre el tipo de solicitudes, instituciones solicitantes y la motivación y fundamentación de las autoridades. El cumplimiento parcial de este criterio es recompensado con media estrella.

6. Bloqueo de contenidos en Internet

> *La ISP publica los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y además indica los soportes legales/contractuales que justifican dichas acciones. Si la compañía aclara las motivaciones que le llevan a filtrar/retirar/bloquear contenidos o a suspender/cancelar servicios.*

5 Ejemplos de ello son la *Guía de Implementación de los Principios Rectores para el Sector TIC* fue elaborada por la Comisión Europea; la *Guía de Implementación* de la Iniciativa de Internet Global (Global Network Initiative) y el reporte *"Who has your back?"* elaborado por Electronic Frontier Foundation.

En este criterio se analiza las políticas que tiene la ISP sobre bloqueos/filtrados/retirada de contenidos sea por carácter judicial en lo penal y/o civil: pornografía infantil, derecho de autor, derecho al olvido, seguridad nacional, entre otros. Así cómo criterios internos como el principio de *neutralidad en la red*.

En la Declaración Conjunta[6] de 2011 sobre libertad de expresión e Internet, los relatores para la libertad de expresión de la ONU, OSCE, OEA y CADHP, indicaron que:

> *"La interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional".*

Asimismo, afirmaron que:

> *"El bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o ciertos tipos de usos (como las redes sociales) constituye una medida extrema—análoga a la prohibición de un periódico o una emisora de radio o televisión—que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual".*

Y finalmente:

> *"Los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión".*

Por otro lado, según *Internet Society*, el *principio de neutralidad en la red* se conforma como un elemento central del funcionamiento de Internet:

> *"Un elemento clave de la arquitectura de Internet es que los datos de los usuarios se transmitan en forma de paquetes de información estandarizados, sin considerar su contenido, su emisor ni su destinatario. Este enfoque no discriminatorio frente al tráfico de Internet es una*

6 Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

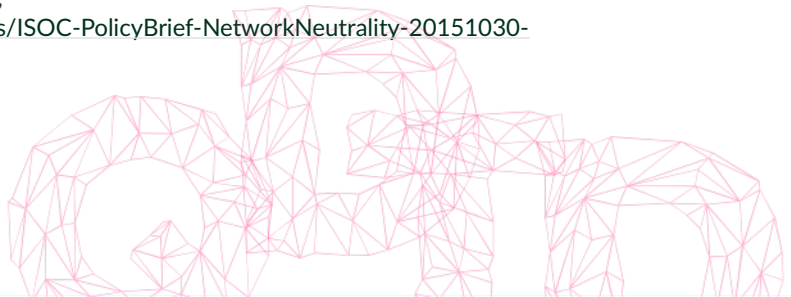
> *premisa central del funcionamiento de Internet. Permite que los datos fluyan fácilmente a través de las redes sin que su paso sea obstaculizado a causa de la naturaleza de los mismos. Básicamente, este enfoque de interconexión abierta es uno de los pilares que sustentan Internet y que han permitido su éxito"*[7].

Este principio se encuentra regulado en Paraguay, en el artículo 26 de la resolución 190/2009 de CONATEL de la siguiente forma:

> *"[...] que los datos de los usuarios se transmitan en forma de paquetes de información estandarizados, sin considerar su contenido, su emisor ni su destinatario".*

Este criterio evalúa si La ISP especifica los procedimientos para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios teniendo en cuenta el debido proceso; lo que supone como mínimo: notificación al usuario, oportunidad de defensa, criterios de proporcionalidad, etc.

7 → "Open Inter-networking: Getting the fundamentals right: access, choice, and transparency," 21 de febrero de 2010, http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choiceand-transparency
→ "Network neutrality—let those packets flow," 30 de marzo de 2015, http://www.internetsociety.org/blog/asia-pacific-bureau/2015/03/network-neutrality-–-let-those-packetsflow
→ "Zero rating: enabling or restricting Internet access?" 24 de septiembre de 2014, http://www.internetsociety.org/blog/asia-pacific-bureau/2014/09/zero-rating-enabling-or-restricting-internetaccess
→ "Neutralidad de la red" 30 de octubre de 2015, https://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030-es.pdf



Metodología

Para esta investigación se analizó documentación sobre cada proveedora de Internet y luego se intentó establecer contacto con cada una de ellas. Se logró socializar los resultados preliminares de evaluación con las empresas Tigo, Personal, Vox y Claro, pero no se tuvo respuesta de Copaco, ni de Chaco Comunicaciones. En estas reuniones se presentó la metodología de evaluación que sería implementada para el año 2017, así como recibir retroalimentación por parte de las propias ISP.

Categoría 1: Política de privacidad y protección de datos personales

Lo que precisamos saber es: ¿La ISP proporciona información clara y completa sobre la recopilación, uso, almacenamiento, procesamiento y protección de datos personales del usuario?

En esta categoría, se evalúan las *políticas y avisos de protección de datos y privacidad* de la compañía, disponible públicamente, sobre el tratamiento de los datos personales que obtiene al prestar el servicio de telecomunicaciones, y no únicamente sobre datos que otorga la persona al contratar el servicio o utilizar el sitio web de la compañía. ¿Se establece de manera precisa qué información de usuario y de sus comunicaciones son obtenidas, almacenadas, así como la temporalidad con la que dichos datos son almacenados?

¿Cuáles son los criterios de evaluación?

> *I) La compañía proporciona información y claras referencias legales sobre la recopilación de datos personales, incluyendo los datos personales que se recogen y en qué situaciones se produce la recogida;*
>
> *II) La compañía proporciona información y claras referencias legales sobre el uso y/o procesamiento de datos personales, incluyendo los fines para los que se utilizan y cómo se produce este;*

III) La compañía proporciona información y claras referencias legales en el almacenamiento de datos personales, incluyendo cuánto tiempo se almacenan los datos así como donde se almacenan y cuando se eliminan, si es que se eliminan;

IV) La compañía proporciona información y claras referencias legales sobre protección de datos personales, incluyendo las prácticas de seguridad que se observan en los procedimientos de retención de datos, si existe política de anonimización de datos y quién/es tendría/n acceso a las bases de datos;

V) La compañía proporciona información y claras referencias legales en el uso de los datos personales por parte de terceros, incluyendo información sobre las circunstancias en que esto iba a pasar y/o la necesidad de autorización del cliente para hacerlo;

VI) Es fácil acceder a esta información en el sitio web de la compañía.

Estándares de desempeño:

POLÍTICA DE PRIVACIDAD	
★	La ISP cumple 5 a 6 criterios
★	La ISP cumple 3 a 4 criterios
★	La ISP cumple 2 criterios
☆	La ISP no cumple ninguno o sólo reúne uno de los criterios

Categoría 2: Autorización judicial

Queremos saber: ¿La ISP se comprometen a divulgar información del cliente, metadatos y contenidos de las comunicaciones únicamente en presencia de una orden judicial?

En esta categoría se evalúa si la compañía exige a las autoridades, la presentación de autorización judicial de manera previa a la entrega de datos sobre el contenido de las comunicaciones o sus metadatos. Si la compañía, en su contrato o cualquier documento oficial a disposición del público deja claro a los usuarios las circunstancias en que las autoridades judiciales o administrativas pueden tener acceso a sus datos.

¿Cuáles son los criterios de evaluación?

> *I) La ISP se compromete a entregar datos sobre el contenido de las comunicaciones de un usuario a las autoridades de justicia siempre que medie la existencia de una orden judicial previa;*
>
> *II) La ISP se compromete a entregar información de la cuenta y registros de conexión a las autoridades de justicia, siempre que medie la existencia de una orden judicial previa.*

Estándares de desempeño:

AUTORIZACIÓN JUDICIAL	
★	La ISP cumple con ambos criterios
★	La ISP cumple con uno de los criterios
☆	La ISP no cumple ninguno de los criterios

Categoría 3: Notificación al usuario

Queremos saber: ¿Las ISP notifican a los usuarios afectados por solicitudes de obtención de datos personales por parte de autoridades o si han promovido el retiro de obstáculos para llevar a cabo la notificación?

Para obtener una estrella en esta categoría, las empresas deben tener una *política de notificación* a usuarios afectados por medidas de *vigilancia estatal* en el primer momento permitido por la ley o, en su caso, demostrar que han combatido legalmente los impedimentos legales o regulatorios para llevar a cabo la notificación o, alternativamente, demostrar que han promovido mecanismos de notificación al usuario al congreso o a otros entes regulatorios.

¿Cuáles es el criterio de evaluación?

> *I) La empresa se compromete a notificar a los usuarios antes de cumplir con las solicitudes de datos de información de cuentas y registros de conexión en los casos no prohibidos por la confidencialidad legal, o para emitir una notificación tan pronto como sea legalmente posible.*

Estándares de desempeño:

NOTIFICACIÓN AL USUARIO	
★	La ISP cumple el criterio
☆	La ISP no cumple el criterio

Categoría 4: Posicionamiento público en contra de la vigilancia masiva o sin control

Precisamos saber: ¿Ha iniciado el ISP un posicionamiento público sobre el respeto y la promoción de los derechos humanos en Internet, en especial contra la vigilancia masiva o vigilancia sin control de las comunicaciones?

En esta categoría se evalúa si las empresas han expresado de manera pública su postura de rechazo a la *vigilancia masiva*, o a la vigilancia sin controles adecuados para impedir vulneraciones a la privacidad de sus usuarios. Si posee una *política institucional* en la que reconoce sus responsabilidad de respeto y protección de los derechos humanos, incluyendo el derecho a la privacidad; y si participa en algún foro o mecanismo para el respeto de derechos humanos en el ámbito de sus responsabilidades empresariales.

Es muy importante conocer las posiciones adoptadas por las empresas en cuanto a privacidad de los usuarios y los derechos de protección de datos. Esta categoría tiene como objetivo evaluar la participación de los ISP en el debate público en relación con las cuentas y las políticas públicas que pueden impactar esos derechos.

También se evalúa si la empresa ha participado, de manera individual o colectiva, en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad.

En esta edición de *"Quién defiende tus datos"*, hemos seguido la contribución de los ISP en los debates públicos más importantes recientemente (desde 2015 hasta 2016) entre los que se cuentan: los debates sobre *Retención de datos de tráfico*, la ley de *Protección de la Niñez de Contenidos Nocivos* y el *Plan Nacional de Ciberseguridad*. Para esta evaluación, hemos considerado sólo las contribuciones hechas por los ISP de forma individual y no por las asociaciones que algunos ISP pueden ser parte –como la Cámara de Proveedoras de Internet del Paraguay.

¿Cuáles son los criterios de evaluación?

I) La empresa ha participado individualmente en cualquier debate público sobre respeto y protección de los Derechos Humanos en Internet (contribuciones realizadas por asociaciones que la empresa pueda ser parte no se consideran); es decir, la compañía ha participado en procesos públicos de incidencia legislativa o ante otros entes regulatorios en defensa del derecho a la privacidad. Ejemplos: el Proyecto de ley de "Obligación de Conservar tráficos de datos en Internet" o Proyecto de ley de "Protección de niños, niñas y adolescentes de contenidos nocivos en Internet" y el Plan de "Ciberseguridad en Paraguay".

II) Participa en algún mecanismo sectorial o multi-sectorial para la promoción, respeto y protección de derechos humanos en el ámbito de sus responsabilidades empresariales (Ejemplos: Global Network Initiative, Telecommunications Industry Dialogue, Pacto Global).

III) La Compañía participa en los Foros de Gobernanza de Internet a nivel local y/o Internacional. Los espacios de debate no vinculante de múltiples partes interesadas de Naciones Unidas por el cual las ISP forman parte del "grupo empresas", actor clave para el ecosistema de Internet.

Estándares de desempeño:

POSICIONAMIENTO CONTRA VIGILANCIA MASIVA	
★	La ISP cumple con todos los criterios
★	La ISP cumple dos criterios
☆	La ISP no cumple ninguno de los criterios

Categoría 5: Transparencia

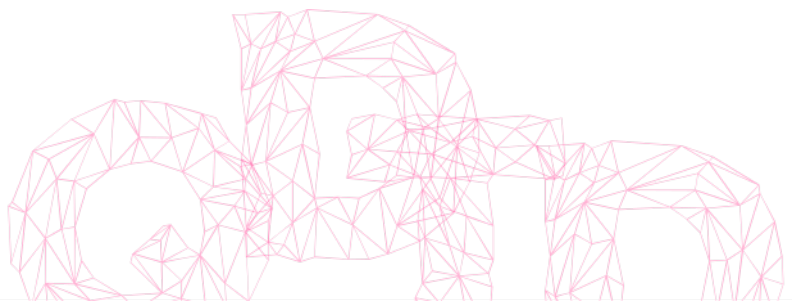
Precisamos saber: ¿La ISP publica informes de transparencia que contienen información sobre cuántas veces los gobiernos han solicitado datos del usuario y la frecuencia con que la empresa proporcionó esos datos a los gobiernos?

Se evaluará si el informe de transparencia evidencia el número de usuarios y usuarias que han sido notificados en el último año con relación al número de solicitudes por parte del Gobierno. El informe de transparencia notifica el origen de las solicitudes para el bloqueo o retiro de contenidos de Internet –incluyendo pornografía infantil, infracción al derecho de autor, cumplimiento de sus propias políticas, etc..

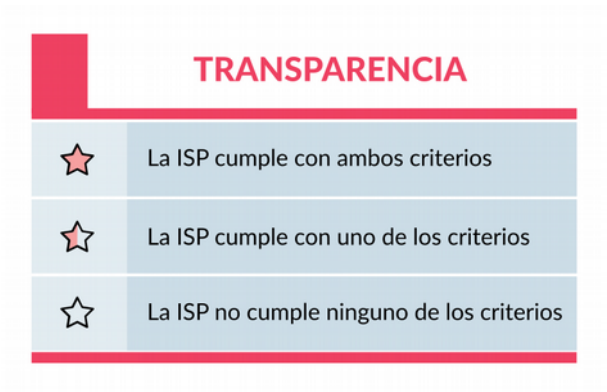
Si bien las ISP en Paraguay no están bajo ninguna obligación de producir informes de *transparencia activa*, esto podría ser una ventana de oportunidad para mostrar que están preocupadas por la construcción de confianza en sus relaciones con los clientes, basadas en la transparencia.

¿Cuáles son los criterios de evaluación?

> *I) La compañía publica informes de transparencia para informar de la colaboración con las autoridades gubernamentales;*
>
> *II) La compañía publica informes de transparencia informando acerca de la colaboración con las autoridades gubernamentales, indicando: (a) la cantidad de solicitudes y divulgaciones clasificados por tipo de datos –si se trata de información de cuenta o de conexión de registros; (b) la cantidad de solicitudes y divulgaciones clasificadas por el cual la autoridad gubernamental hizo la solicitud; (c) la cantidad de solicitudes y divulgaciones clasificados por la motivación alegada por la autoridad gubernamental –presentación de pruebas en materia civil, penal, o los casos administrativos, etc..*



Estándares de desempeño:



Categoría 6: Bloqueo de contenidos en Internet

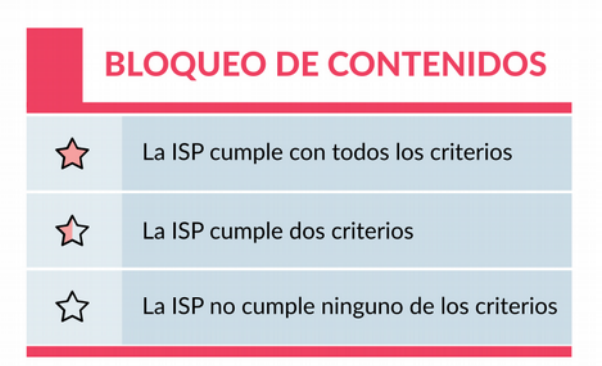
Precisamos saber: ¿la ISP es clara con los y las usuarias sobre las formas en que filtra, retira o bloquea contenidos y cancela o suspende servicios?

Se evalúa si la ISP publica los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios y, además, indica los soportes legales/contractuales que justifican dichas acciones. La compañía aclara las motivaciones que la llevan a tomar esas acciones. La ISP específica los procedimientos para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios teniendo en cuenta el debido proceso; lo que supone como mínimo: notificación al usuario, oportunidad de defensa, criterios de proporcionalidad, etc..

¿Cuáles son los criterios de evaluación?

> *I) La ISP pública los procedimientos que emplea para filtrar/retirar/bloquear contenidos o suspender/cancelar servicios, y advierte sobre las motivaciones y los soportes legales/contractuales que lo justifican;*
>
> *II) La ISP no tiene antecedentes de filtrar/retirar/bloquear contenidos o suspender/cancelar servicios*

Estándares de desempeño:



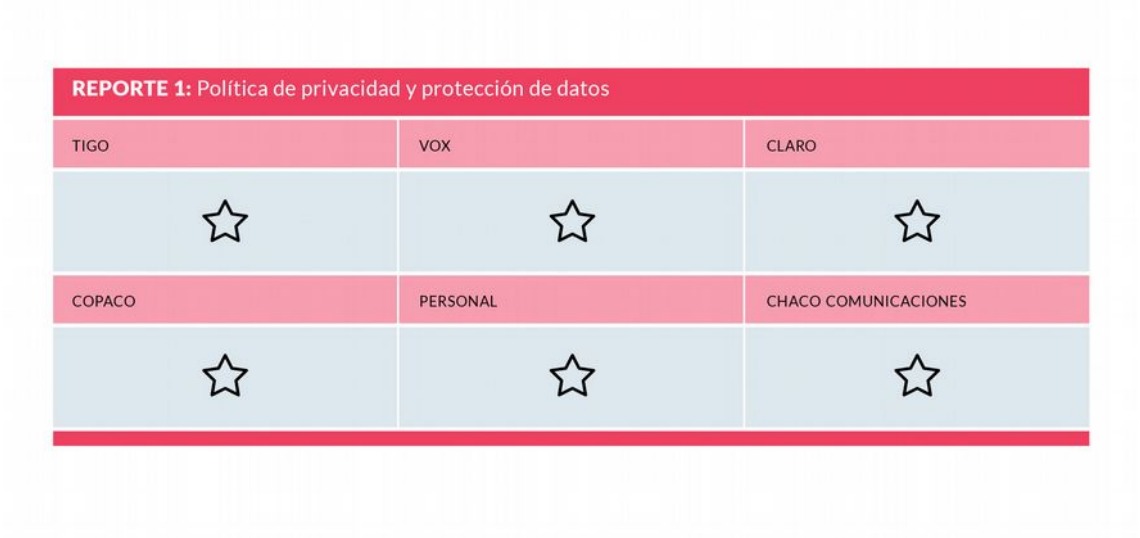
Resultados

Reporte 0:

CUADRO GENERAL COMPARATIVO 2017

CRITERIOS	Política de privacidad y protección de datos	Autorización Judicial	Notificación	Posiciona-miento público en contra de la vigilancia	Informes de transparencia	Bloqueo de contenidos en Internet	Porcentaje de cumplimiento
tigo	☆	★	☆	★	★	★	41,6 %
Personal	☆	★	☆	☆	☆	★	25 %
Claro	☆	★	☆	★	☆	★	33,3 %
VOX	☆	★	☆	★	☆	★	33,3 %
COPACO S.A.	☆	★	☆	☆	☆	★	25%
CHACONET	☆	★	☆	☆	☆	☆	16,6 %

Reporte 1: Política de privacidad y protección de datos



Tigo, Personal, Copaco, Claro, Vox y Chaco Comunicaciones *no tienen una política o aviso de privacidad* disponible en su página principal de Internet por lo que ninguna compañía cumple con el criterio. Algunas cuentan con *Términos y Condiciones* para el uso de la web, como Tigo y Personal; esta información es importante pero no suficiente para la protección del derecho a la intimidad de los que contratan el servicio de telefonía e Internet.

No obstante, en la entrevista realizada con las ISPs Tigo, Personal, Vox y Claro se comprometieron en revisar esta calificación.

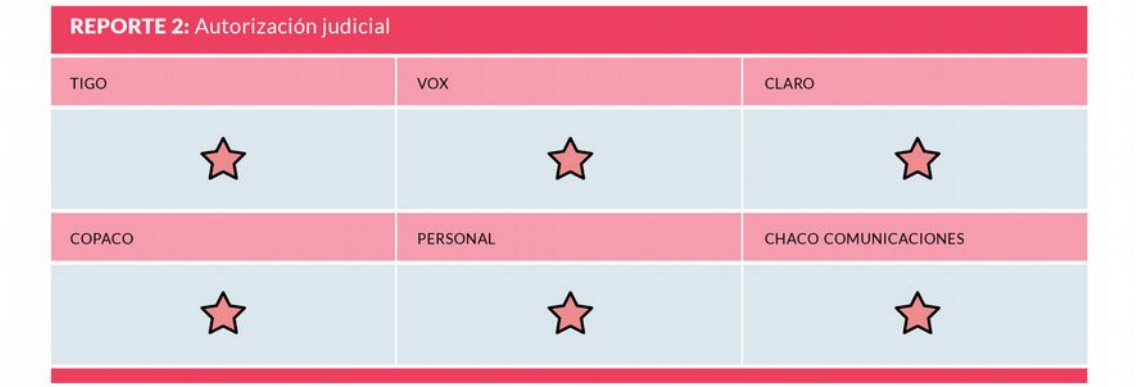
Ninguna ISP indica de manera clara qué información se recaba sobre el usuario y sus comunicaciones, ni por cuánto tiempo se conservan los datos personales.

Recomendación:

> Las ISP deben trabajar en la *transparencia* de tratamiento de datos de sus clientes. La publicación de sus políticas sobre privacidad y datos personales deben ofrecer claridad a sus usuarios.
>
> Estos *avisos de privacidad y tratamiento de datos* forman parte de los estándares de economía digital que promueven los reportes de la OECD – desde este 2017, Paraguay es miembro oficial de esta organización. La

adecuaciones mínimas a estas normas de buenas prácticas visibilizaría a nivel regional y mundial la responsabilidad y compromiso de las empresas locales en la calidad de la conectividad de los habitantes del territorio paraguayo.

Reporte 2: Autorización judicial



La Constitución de la República es clara al exigir que las autoridades designadas por las leyes deben obtener una *autorización judicial* antes de obtener acceso al contenido de las comunicaciones.

Si bien este requisito para la colaboración no se encuentra detallado en ninguna web de las ISP entrevistadas, no existen evidencias que las proveedoras de Internet no hayan entregado información de servicio de Internet sin orden judicial.

Sin embargo es importante destacar que las ISP Tigo, Personal y Claro manifestaron su preocupación por los servicios de telefonía. En ese caso están obligadas a facilitar información de los metadatos de la llamada –conocido como "cruce de llamadas"– por solicitud fiscal. Este mecanismo fue aceptado por la Corte Suprema sin tener en cuenta las sentencias internacionales vinculantes a nuestra jurisdicción nacional que indican la autoridad judicial como único mecanismo posible.

Por otro lado, según ISP entrevistadas, se han dado caso casos en que han rechazado solicitudes de acceso a *datos de llamadas telefónicas* por no cumplir con los requisitos legales, tales como número de expediente, hecho punible,

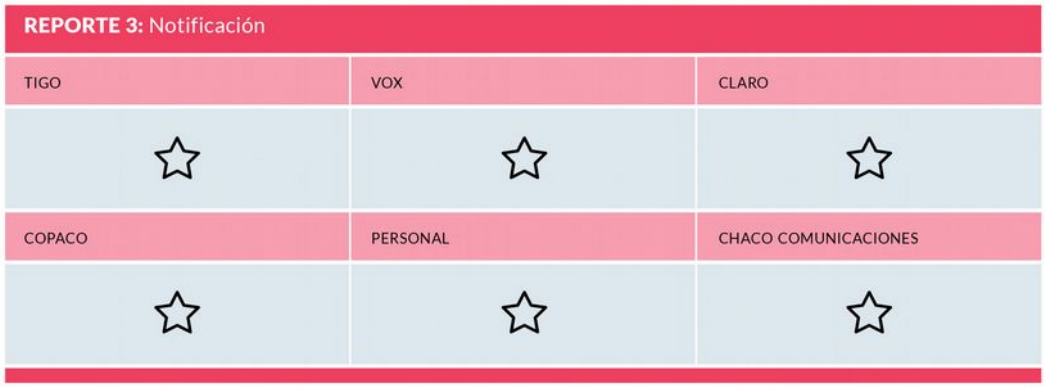
argumentos, etc.. Sin embargo sigue habiendo irregularidades en el acceso y divulgación de los datos de los clientes que contratan servicios de telefonía, sin los requisitos legales. Un ejemplo de ello es el caso del espionaje sobre la periodista de *ABC Color*, por parte de las fuerzas militares, en el que se comprobó que empleados de Personal filtró información, violentando no solo su privacidad sino también afectando la libertad de expresión en un estado democrático.

Por último, para casos de servicios de Internet, según las entrevistas, Tigo, Personal y Claro no conservan los *datos de tráfico* de sus usuarios. Por su parte, Copaco y Vox no solo retienen sino que facilitan información sobre datos/metadatos de sus usuarios a las autoridades de persecución penal. Esto último es preocupante, ya que por un lado, cumplen la ley de Comercio Electrónico, al almacenar la información, pero la violan al entregarla con finalidades diferentes a la prevista en dicha ley.

Recomendación:

> Establecer explícitamente este requisito en el *aviso de privacidad y tratamiento de datos personales* para la colaboración con autoridades de seguridad y justicia que implique la intervención del contenido de comunicaciones privadas.
>
> Asimismo, es deseable que tanto Copaco como Vox incluyan en sus avisos detalles del tratamiento que realizan sobre los metadatos almacenados. Se ha demostrado –por jurisprudencias internacionales vinculantes a nuestro sistema judicial– que los metadatos pueden revelar aspectos sensibles de la vida privada de las personas. Por tanto es indispensable que los titulares de dichos datos tengan acceso a los mismos cuando lo soliciten.

Reporte 3: Notificación



En este criterio encontramos una situación compleja: las ISP entrevistadas *no reconocen* el rol central que juegan en la defensa de la intimidad de sus usuarios. Como no existen avisos de privacidad, no hay información sobre la forma de entrega de la información personal a las instituciones autorizadas por el Estado, ni existen detalles sobre el procedimiento que se debe emplear cuando esto sucede.

Recomendación:

> Es deseable que las ISP tengan una política pública de notificación a usuarios afectados por medidas de vigilancia. Si bien, pueden existir impedimentos legales para efectuar la notificación de manera previa o simultánea a la medida de vigilancia –por ejemplo por poner en riesgo la efectividad de una investigación o comprometer físicamente la integridad de una persona– no se detectó una *política de notificación* para cuando la medida se haya agotado o haya transcurrido un periodo de tiempo razonable después de la conclusión.

Reporte 4: Posicionamiento en contra de la vigilancia masiva

Únicamente la empresa Claro a través de América Móvil, fue detectada con el compromiso público de reconocimiento de sus responsabilidades empresariales en materia de derechos humanos y ha expresado públicamente su rechazo a medidas de vigilancia masiva y sin controles[8].

El caso del espionaje de la periodista de ABC por parte de las fuerzas militares con la complicidad de un empleado de Personal, fue un escenario importante para que todas las ISP se posicionen contra este tipo de abuso, además de llevar el caso en instancias penales. Lamentablemente ninguna ISP hizo público su repudio contra este tipo de acciones inconstitucionales e ilegales, ni suscribieron un compromiso de mejorar sus mecanismos de acceso a la información para generar mayor confianza de sus clientes.

No obstante, existen ISP que participaron en análisis legislativos que afectan la regulación de Internet y los derechos Humanos. Tigo, Personal y Claro se posicionaron en contra de la ley de *"Protección de niños, niñas y adolescentes de*

8 América Móvil Sustainability Report 2015 Pág. 52: http://www.americamovil.com/sites/default/files/2016-09/AMX-IS-2015-espanol.pdf

contenidos nocivos en Internet" durante las consultas públicas de las mesas de trabajo llevadas a cabo por la *Secretaría Nacional de la Niñez y Adolescencia*.

En lo referente a *políticas públicas de seguridad digital*, todas las ISP entrevistadas, salvo Chaco Comunicaciones, han participaron de las mesas de trabajo para el desarrollo del *Plan Nacional de Ciberseguridad*.

Asimismo, la Empresa Tigo tiene una alta representación en instancias Internacionales sobre políticas de derechos humanos como *US Global Compact* capítulo Paraguay y *Telecommunications Industry Dialogue* a través de Millicom.

La ISP que le sigue en este criterio es Claro, que participa de *US Global Impact* a nivel internacional[9].

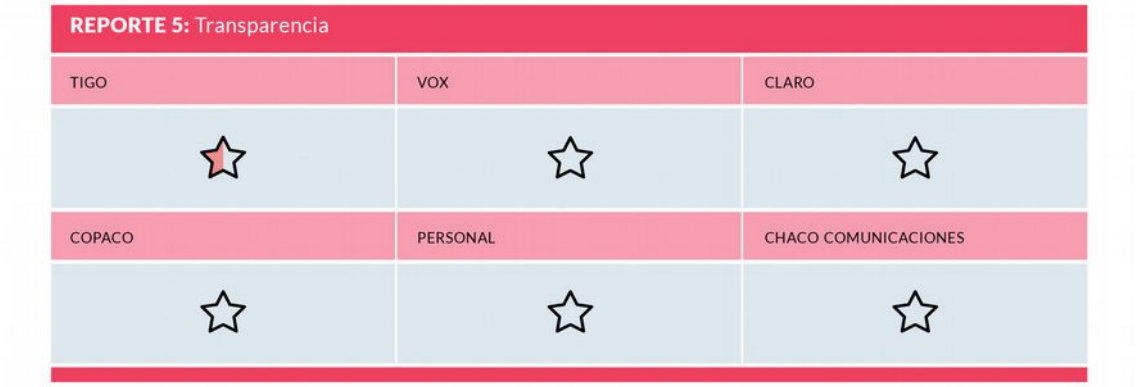
En lo que respecta a la participación en el Foro de Gobernanza de Internet, solo Copaco y Vox han cumplido con este criterio.

Recomendación:

> Es deseable que las ISP formen parte de foros internacional y nacionales sobre los asuntos de Internet (*Foro de Gobernanza de Internet*) y participen en mecanismos para afrontar sus responsabilidades en materia de derechos humanos como *US Global Compact* (*Pacto global* – capítulo nacional o internacional) y *Telecommunications Industry Dialogue*. Asimismo, es clave la participación y opinión pública sobre acontecimientos que involucren a Internet para mejorar la transparencia en el cabildeo político, intereses que afectan a sus usuarios.

9 http://www.americamovil.com/es/acerca-de-nosotros/sustentabilidad

Reporte 5: Transparencia



Unicamente, Tigo a través del informe anual de Millicom denominado *"Requests from law enforcement in South America"*[10] publica un informe de solicitudes de datos y metadatos de los usuarios solicitados por las autoridades judiciales. No obstante este informe sólo se encuentra disponible en inglés y no ofrece suficiente información que permita saber el volumen, origen, motivos y alcance de solicitudes. Tampoco el número e identidad de las autoridades que solicitan a acceder a dichos datos por lo que no se cumple el segundo punto del mismo criterio para completar la estrella.

Lamentablemente las demás ISP evaluadas no publicaron informe individual de transparencia respecto de solicitudes gubernamentales de intervención de comunicaciones y de acceso a datos de usuario y sus comunicaciones.

Recomendación

> El *informe de transparencia* es un elemento positivo para el resguardo de los derechos humanos. Conocer el número global de solicitudes realizadas

10 http://www.millicom.com/media/8404741/Millicom-LED-Report-2016.pdf

por las autoridades de persecución penal, estadísticas respecto a las solicitudes realizas por otras autoridades, identificación de las instituciones solicitantes, tipos de solicitudes y razones que fueron otorgadas para hacer la solicitud, son claves para hacer un seguimiento de la vigilancia estatal de las comunicaciones. Un ejemplo a seguir es TELIA Company[11] de Suecia y Finlandia, que además de clasificar y divulgar los datos de interceptación legal de datos de sus usuarios, también publica informes de sostenibilidad donde expone todos los casos en que ellos defendieron la privacidad y otros derechos humanos de sus usuarios.

Es importante recalcar que empresas intermediarias como Facebook, Google, Twitter divulgan en sus páginas web informes de transparencia donde se especifican las solicitudes de los gobiernos. Un hecho a destacar es que México ha incluido estos informes como una obligación legal.

11 El siguiente informe clasifica la interceptación legal histórica de datos, datos de suscripción y peticiones impugnadas/rechazadas: http://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/ledr_oct2016_final.pdf

Reporte 6: Bloqueo de contenidos en Internet

La única ISP que no cumple los estándares de servicio de acceso a Internet es Chaco Comunicaciones. En la web oficial se publican medidas de bloqueos contra las descargas mediante tecnologías peer-to-peer (p2p).

Las demás ISP no han adoptado medidas contractuales para el bloqueo de acceso a Internet. Cabe mencionar que en el 2010 ocurrió un caso de bloqueo: a una página web que realizó una parodia sobre el periódico nacional *Abc Color*.

Afortunadamente, no se han encontrado evidencias de nuevos bloqueos similares.

Estas ISP no han logrado de obtener todas las estrellas, porque no se encontraron guías o *códigos de conducta* que especifiquen los comportamientos esperados y los no permitidos por dichas empresas y así evitar sanciones a los usuarios.

Recomendación:

> La suspensión preventiva y hasta la interrupción de los servicios de Internet para ciertos casos deben estar estipuladas en una guía o código

para justificar el control, bloqueo y retiro de contenidos por parte de las ISP. Por tanto es indispensable que se describan estos criterios para garantizar a sus usuarios que los procedimientos de bloqueos seguirán una norma legítima y acorde a los estándares internacionales de derechos humanos.

QUIEN DEFIENDE TUS DATOS

www.tedic.org

Este informe fue diagramado
con LibreOffice 5