



POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES EN LAS EMPRESAS DE TELECOMUNICACIONES

Estudio de casos de Argentina, Brasil, Chile y México

VOLUMEN II

Área de Privacidad



Diciembre 2016

<https://adcdigital.org.ar>

Este trabajo fue realizado como parte de un proyecto financiado por la Ford Foundation, el mismo es publicado bajo una licencia Creative Commons Atribución - No Comercial - Compartir Igual. Para ver una copia de esta licencia, visite <https://creativecommons.org/licenses/by-nc-sa/2.5/>.



El documento *Políticas de protección de datos personales en las empresas de telecomunicaciones: Estudio de casos de Argentina, Brasil, Chile y México* es de difusión pública y no tiene fines comerciales.

Índice

i	Introducción	5
ii	Argentina ¹	7
i	Empresas privadas de telecomunicaciones en Argentina	12
iii	Brasil ²	17
i	Introduction	17
ii	Telecommunication Companies' Data Protection Practices . .	18
i	Questions answered exclusively by InternetLab	18
ii	Pending questions: Companies' answers	20
iv	Chile ³	27
i	Mercado de ISP en Chile	28
ii	Conexiones y Penetración del Internet	28
iii	Velocidad del servicio	29
iv	Mercado de Acceso a Internet: Aspectos generales	30
v	Estructura de mercado	30
vi	Empresas participantes	32
vii	Participación de mercado	33
viii	Análisis de contratos	38
ix	Análisis de entrevistas	40
x	Hallazgos en el análisis de caso ISP chilenas	45
xi	Conclusiones	48

¹ El presente trabajo fue realizado por **Jeannette Torrez**, investigadora de las Areas de Libertad de Expresión y Privacidad de la Asociación por los Derechos Civiles.

² InternetLab members involved in this project: **Fabiane Midori Sousa Nakagawa** and **Jacqueline de Souza Abreu**. Collaborator: **Francisco Carvalho de Brito Cruz**, Director of InternetLab.

³ Colaboraron en la elaboración de este informe: **Valentina Hernández** y **Pablo Viollier**, ambos investigador de Derechos Digitales, así como **Rodrigo Vargas**, **Constanza Alarcón** y **Bastián Riveros**, pasantes del equipo de investigación de Derechos Digitales.

v	México ⁴	49
i	Evaluación de proveedoras de servicios de telecomunicaciones	50
vi	Hallazgos principales. Conclusiones y recomendaciones finales	56

⁴ El presente capítulo fue realizado por el equipo de la **Red en Defensa de los Derechos Digitales** (R3D), México.

Políticas de protección de datos personales en las empresas de telecomunicaciones

Estudio de casos de Argentina, Brasil, Chile y México[¶]

I Introducción

Para una mejor comprensión del estado de la protección de datos personales en América Latina, es necesario complementar el estudio del marco normativo analizado en el informe “El sistema de Protección de Datos Personales en Argentina y América Latina” publicado por ADC, con un relevamiento de las prácticas que realizan aquellas entidades que -por la naturaleza y envergadura de sus tareas o funciones- tienen en sus manos el manejo de grandes bases de datos personales. En ese sentido, el sector empresarial se nos presenta como un actor que en el desarrollo de sus actividades accede a y utiliza una cantidad considerable de información de las personas. Así, el estudio de las prácticas y políticas empresariales resulta de suma importancia para analizar el efectivo cumplimiento de la legislación en vigencia.

Dentro del sector privado, nuestra atención se focalizó en el mercado de las telecomunicaciones, debido a que estas empresas son responsables del almacenamiento y el procesamiento de un gran volumen de datos personales. Como resultado de este poder, las “telcos” están en una posición que puede volverlas propensas a adoptar comportamientos que pongan en riesgo el resguardo de los derechos de los titulares de los datos. Por citar un par de ejemplos, podemos pensar en el uso de datos para fines distintos a los que fueron invocados para su recolección (la comercialización de estos datos a terceros es una instancia clara de lo recién afirmado) o en la comunicación de datos personales a las autoridades para fines de seguridad o de investigación.

Por lo tanto, resulta imprescindible que las empresas incorporen prácticas respetuosas de la normativa sobre protección de datos personales y la autodeterminación informativa.

[¶]El presente informe fue compilado por **Valeria Milanés**, Directora de las áreas de Privacidad y Libertad de Expresión de la Asociación por los Derechos Civiles, y **Eduardo Ferreyra**, abogado e investigador de las áreas de Privacidad y Libertad de Expresión de la ADC. Encargado de diseño: **Leandro Ucciferri**, abogado e investigador de las áreas de Privacidad y Libertad de Expresión de la ADC.

Con esa convicción en mente, desde ADC iniciamos una investigación que se desarrolló durante parte de 2015 y 2016 buscando desentrañar las políticas implementadas por las empresas de telecomunicaciones en los países elegidos como casos de estudio, para intentar detectar las tendencias en la región.

Una vez más, contamos con el invaluable aporte de organizaciones de sociedad civil de la región, que tuvieron a su cargo la investigación en sus respectivos países. De tal suerte, ADC llevó adelante la investigación en Argentina, [InternetLab](#) hizo lo propio en Brasil, [Derechos Digitales](#) lo hizo en Chile y [Red en Defensa de los Derechos Digitales](#) llevó adelante la investigación en México.

Se acordó la selección de al menos dos empresas en cada país y se decidió comenzar la investigación con una entrevista preliminar, que incluyó las mismas preguntas para todas las empresas. Según el resultado de las entrevistas, se evaluaría la adopción de otras actividades. El cuestionario abordó una amplia gama de cuestiones vinculadas al uso de datos y se encuentra reproducido en los capítulos correspondientes a cada país.

Sin embargo, el resultado, si bien esperado, no fue demasiado alentador. En Argentina fueron contactadas más de 17 compañías, incluyendo a los principales operadores como Telefónica, Telecom y Claro. Sólo la empresa IFX Networks contestó el cuestionario.

En Brasil fueron contactadas las empresas Vivo (de Telefónica) y TIM (de Telecom Italia). Sólo TIM contestó en forma parcial el cuestionario.

Por su parte en Chile fueron seleccionadas las empresas Movistar y VTR, ambas empresas accedieron a contestar parcialmente el cuestionario.

En México fueron contactadas las empresas Telcel, Movistar y At&T, sin embargo, ninguna se avino a contestar el cuestionario.

Se compartirán a continuación, en capítulos separados, las experiencias y hallazgos de cada uno de los países. El denominador común fue la reticencia persistente de las empresas en brindar información y la falta de respuesta a las preguntas por parte de las empresas se intentó suplir mediante el análisis de los Términos y Condiciones, Políticas de Privacidad y demás documentación publicada en los sitios web.

En algunos de los casos de estudio se consideró necesario efectuar un breve análisis del mercado de telecomunicaciones del país, dado que las notorias características de fuerte concentración en el sector, además de ser otro de los denominadores comunes de la región, parecen también tener alguna suerte de incidencia en la postura reticente de las compañías.

Por último, se incluyó en el capítulo final una reseña de los hallazgos principales con conclusiones y recomendaciones para la adopción de buenas prácticas empresariales, que no intentan, de ninguna manera, ser un posicionamiento acabado, sino más bien propuestas básicas y disparadoras para

próximos diálogos que deberían tener lugar entre el sector privado, la sociedad civil y otros actores relevantes.

Se anticipa que el capítulo 3, correspondiente a la experiencia de Brasil, se encuentra redactado en inglés y portugués.

II Argentina¹

Desde las áreas de Libertad de Expresión y Privacidad de la Asociación por los Derechos Civiles hemos realizado un trabajo de seguimiento durante el año 2016 para establecer instancias de comunicación con el sector de las empresas de telecomunicaciones en Argentina. El objetivo de estas instancias de diálogo con los sectores mencionados se debían a un interés en generar información valiosa para los ciudadanos en relación al tratamiento de datos personales de los usuarios de las empresas de telecomunicaciones. Desde la ADC consideramos fundamental la articulación de canales de diálogo abiertos con múltiples sectores, debido a que nos basamos en la experiencia internacional que avala un modelo de múltiples partes interesadas² para la construcción de mejores decisiones.

No obstante, identificamos que en Argentina existe por delante un extenso camino a recorrer en materia de diálogo entre el sector privado y las organizaciones de sociedad civil de acuerdo a nuestra experiencia de trabajo durante el 2016.

A partir de marzo 2016, desde la ADC nos hemos acercado tanto a las principales empresas de telecomunicaciones de la Argentina como a las pequeñas y medianas. Además, de intentar lo mismo con organizaciones que nuclean a estas empresas como la Cámara de Informática y Comunicaciones de la República Argentina³ y la Asociación Interamericana de Empresas de Telecomunicaciones.⁴ Respecto a CICOMRA, nos comunicamos por e-mail en una primera oportunidad y luego con la comisión legal de la misma, pero no obtuvimos respuesta. En el caso de ASIET, también el contacto fue establecido via e-mail, y nos fue respondido que las preguntas serían contestadas pero desafortunadamente no fue recibido más contacto de su parte.

Con el fin de obtener colaboración por parte de las empresas en la respuesta a un cuestionario definido, desde la ADC realizamos un plan de acción.

¹ El presente trabajo fue realizado por **Jeannette Torrez**, investigadora de las Areas de Libertad de Expresión y Privacidad de la Asociación por los Derechos Civiles.

² El modelo de múltiples partes interesadas o *multistakeholderism* considera la participación de todos los actores involucrados en un sistema para la discusión y toma de decisiones. La **ICANN** y el **Internet Governance Forum** son ejemplos de relevancia global en la adopción de este modelo.

³ La **Cámara de Informática y Comunicaciones de la República Argentina (CICOMRA)** agrupa a empresas industriales, comerciales y de servicios del sector de la Informática y las Comunicaciones de la Argentina y entre sus socios se encuentran Telefónica, Claro, Telecom, etc.

⁴ **ASIET (Asociación Interamericana de Empresas de Telecomunicaciones)** está conformada por empresas (públicas y privadas) del sector de las telecomunicaciones que operan en los países del continente americano.

En la primera etapa, enviamos un mail a los correos institucionales de las empresas, los cuales en muchos casos eran difíciles de hallar. Si bien los sitios web de las empresas de telecomunicaciones habilitan vías de contacto “visibles” para el reclamo o contratación de servicios, esta situación cambia cuando se buscan vías de contacto a responsables de la empresa para responder a otros temas y especialmente referidos a Datos Personales. Cuando nos referimos a cuestiones ligadas a este tema, la falta de visibilidad para que un usuario o usuaria pueda encontrar de manera sencilla una vía de comunicación se torna un problema, sobre todo si contemplamos lo expresado por la Ley 25.326, cuando establece la designación de un responsable identificable para las bases de datos y en definitiva para hacer valer el derecho de acceso a los datos personales.

El objetivo del envío de los e-mails a las empresas era presentarnos desde la ADC, como organización e intentar pactar una entrevista presencial, y en caso que esa posibilidad no existiera, proceder a enviar el cuestionario para ser respondido y enviado vía correo electrónico.

Luego de enviar los correos electrónicos a: [Telefónica](#), [Telecom](#), [Cablevisión Fibertel](#), [Nextel](#) y [Claro](#) recibimos respuesta por parte Telecom y Nextel, las cuales preguntaron acerca del motivo de las preguntas e incluso una persona de Nextel se comunicó telefónicamente con las oficinas de ADC para obtener mayores detalles acerca del proyecto de investigación. En el caso de Nextel no hubo más respuesta y en el caso de Telecom, la persona que nos contactó explicó que Telecom requería conocer los antecedentes de la ADC como organización y que debía recibir autorización por parte de la empresa para responder.

Por parte de Claro, respondieron que analizarían el pedido mas no volvieron a responder. Y en el caso de Fibertel, respondieron consultando el “alcance” de las preguntas, a las cuales contestaron asegurando el cumplimiento de la Ley 25.326 y expresando que desde la empresa tienen “por política mantener con carácter de confidencial al contenido de los circuitos, normas y procedimientos internos que rigen su operatoria en general y, especialmente, las relativas a la recolección, mantenimiento y remoción de datos personales que obran en las bases que utiliza”. En el caso de Telefónica no hubo respuesta alguna.

Luego de aquella experiencia inicial, procedimos a contactar a otras empresas y cooperativas pequeñas y medianas del resto del país, incluso aquellas destinadas a telefonía IP, a través de correo electrónico, las empresas elegidas fueron: [Telecentro](#), [Gigared](#), [Aginet](#), [Fecosur](#), [Cooperativa Telefónica de Grand Bourg](#), [Cooperativa Telefónica de Vivienda y otros Servicios Públicos Del Viso Ltda. \(TELVISIO\)](#), [IFX Networks](#), [IP Tel](#), [Jumpnet](#), y [Cotelcam](#). Además, contactamos a la [Cámara Argentina de Telefonía IP](#). De las empresas y cámara mencionadas, solo recibimos respuesta de IFX Networks quienes fueron los únicos que respondieron la encuesta vía mail de manera completa.

De forma paralela, procedimos a enviar cartas a Telefónica, Telecom, Telecentro y Nextel -y al tampoco recibir respuesta a Gigared-, a las sedes principales de las mismas ubicadas en la Ciudad de Buenos Aires, además del envío de mails de recordatorio para nuestro pedido. En el caso de la

empresa Nextel, debimos llevar la carta dos veces, debido a que la primera no nos fue recibida por negativa del personal de seguridad.

A pesar de no recibir aprobación para la respuesta del cuestionario, un representante de una de las empresas de telecomunicaciones de mayor tamaño de nuestro país, accedió a participar de un workshop organizado por la ADC en la Facultad de Derecho de la Universidad de Buenos Aires acerca del estado y el futuro de los datos personales en Argentina. Debido a las reglas de Chatham House⁵ utilizadas en el encuentro, no es posible precisar la identidad de la persona asistente, ni de la empresa que representaba. Sin embargo, podemos detallar cómo fue el intercambio durante la mesa de trabajo. La visión de la persona que representaba esta empresa señalaba que siempre había existido una buena relación con la Dirección Nacional de Datos Personales, lo cual puede deberse a las limitadas tareas de control del organismo durante los años que lleva operativo. Menciona además, que en la empresa habían tenido inconvenientes tecnológicos en relación al Registro No Llame⁶ debido a que la baja de usuarios no podía hacerse de forma automatizada, sino manual.

Por otro lado, de manera informal, la persona representante dio aviso que aún se encontraba esperando la autorización para poder responder la encuesta.

Como conclusión a esta experiencia, sostenemos que es necesaria la profundización de procesos que apunten a generar mayor transparencia a instituciones no solo estatales sino también a aquellas del sector privado. La rendición de cuentas de las instituciones estatales promovida por numerosas iniciativas de Gobierno Abierto, es crucial para un monitoreo ciudadano en temas críticos que afectan a la sociedad, pero este aspecto debe ser complementado con informes de transparencia provistos por empresas del sector privado, las cuales también tratan cuestiones de interés fundamentales para los ciudadanos. Si solo nos atenemos a lo que compete a este proyecto, es decir a la Protección de Datos Personales, podemos ver la ausencia de reportes de transparencia en esta materia.

A pesar de la importante existencia de instancias de elaboración de informes concernientes rendición de cuentas para el fisco, las empresas parecieran no sentir la misma obligación respecto a los datos personales. Por ejemplo, Telecom y Telefónica de Argentina, dos de las empresas que concentran la mayor parte de mercado en telecomunicaciones, no lo hacen aunque sí elaboran políticas propias de Términos y Condiciones, dedicando en ambos casos, una sección para referirse Políticas de Privacidad y/o Datos Personales. Si bien esta separación entre los Términos y Condiciones y Datos Personales parece promisorio respecto al cumplimiento de la Ley 25.326, este escenario se difumina al efectivamente acceder a la sección en cuestión debido a ausencia de informes que indiquen:

1. si los usuarios han solicitado acceder a sus datos;

⁵ La regla Chatham House dispone que las personas que asisten a un seminario pueden discutir los resultados del seminario en el mundo exterior, pero no pueden discutir quien asistió o identificar lo que dijo un individuo específico.

⁶ El **Registro No Llame** (2014) es una iniciativa de la Dirección Nacional de Datos Personales que permite a los usuarios de empresas telefónicas evitar recibir llamadas de ofrecimiento de productos por parte de empresas.

2. si las solicitudes de los usuarios fueron permitidas;
3. si las solicitudes fueron denegadas y bajo qué motivos.

En los casos de Telefónica y Telecom, como se enunció previamente, en la sección de legales se encuentran los apartados de protección de datos personales, aunque cabe mencionar que un usuario con poca o nula información respecto a los derechos que tiene como ciudadano o usuario, difícilmente pueda hallar en el sitio de manera sencilla alguna referencia a los derechos de protección de datos personales que posee. Esto genera un marcado contraste con la información de marketing y ofrecimiento de productos que son ofrecidos visiblemente en ambos sitios.

El sitio web de Telefónica destaca dos pequeños apartados correspondientes a la ley de Protección de Datos Personales, en el primero⁷ señalan las disposiciones de acceso a los datos y de retiro y bloqueo.⁸

En la siguiente sección⁹ dedicada a la Protección de Datos Personales explicitan de manera clara y en lenguaje sencillo sus políticas de empresa que respetan la Ley 25.326. Si bien es muy valioso que la empresa elabore y exponga sus condiciones como empresa en esta materia y de manera sencilla, existen algunos problemas para verificar que se cumplan los principios que proponen.

El principio 1, el cual encomienda proteger los datos con estándares de seguridad y confidencialidad no especifica cuáles son esos estándares, si son internacionales, bajo qué pautas de calidad se rigen, si se actualizan, si los elabora y audita la misma empresa o no, etc.

El principio 3 “que permite el acceso a la información únicamente a personas autorizadas por nuestra empresa (sean dependientes o no), las que estarán debidamente capacitadas en el manejo apropiado de la misma y serán pasibles de sanciones en caso de incumplimiento” no da mayores detalles de quienes serán las personas encargadas del acceso a los datos ni quien será la persona responsable como lo indica la ley 25.326. Tampoco se brinda información acerca de si la capacitación de las personas autorizadas es académica o dentro de la misma empresa y si dicha capacitación tiene aval de la Dirección Nacional de Protección de Datos. Además, tampoco se explican qué tipo de incumplimientos serán sancionados ni si acaso existen gradientes en los incumplimientos o diferencias para incumplimientos reiterados.

El principio 5 el cual exige “a aquellos que nos provean algún servicio que se adecuen a nuestros estándares de seguridad y confidencialidad” posee las mismas deficiencias del principio 1 al no explicar cuáles son los estándares.

Una ausencia grave en los principios de la empresa es la falta de compromiso con sus usuarios en

⁷ <http://www.telefonica.com.ar/legales/generales/datos-personales>

⁸ Disposición 10/2008 y Disposición 04/2009

⁹ <http://www.telefonica.com.ar/legales/generales/proteccion-de-datos>

darles conocimiento en caso que sus datos hayan sido solicitados por personas o instituciones ajenas a la titularidad de los datos.

Es llamativo que la empresa exprese un compromiso con el cumplimiento de la Ley 25.326 y además, según sus principios internos ofrezca a sus usuarios acceder, rectificar y suprimir sus datos pero, no genere opciones visibles o de vías online como lo hacen con la contratación de servicios y productos, para el efectivo ejercicio de estos derechos.

Por su parte, Telecom presenta similares dificultades para visibilizar a sus usuarios los derechos que otorga la Ley 25.326. La empresa presenta una sección de Protección de Datos Personales acotada, en la cual a través de un link, que dirige a un archivo de descarga en formato PDF,¹⁰ se advierte a los usuarios que la empresa “cumple con los requisitos” de la Ley 25.326 y que se encuentra como responsable registrado ante la Dirección Nacional de Protección de Datos Personales (DNPDP). Informan acerca del derecho de acceso a los datos personales y mencionan a la DNPDP como la entidad encargada de atender denuncias. Como característica positiva, facilita un link hacia el sitio web de la DNPDP, en el cual es posible buscar las bases de datos personales registradas por Telecom -y de cualquier empresa con bases de datos registrada-, las cuales están diferenciadas por categorías, a saber:

- ◆ Base de clientes
- ◆ Base de clientes con fines publicitarios
- ◆ Call Center
- ◆ Proveedores
- ◆ Recursos Humanos
- ◆ Video vigilancia

Además, hay descripciones de los fines de las bases de datos y también figura el nombre, apellido, teléfono y dirección de correo electrónico de contacto de los responsables de cada base de datos. Esta información es de gran valor para hacer efectivo el acceso a la justicia en relación a los derechos que otorga la Ley 25.326 y sería también deseable que esta información pudiera ser accedida y visibilizada desde el sitio web de la empresa, ya que si bien es correcto que se encuentre en el sitio de la DNPDP, el hallazgo de estos datos es accesible luego de una búsqueda dirigida.

Por su lado, la empresa Telefónica, también cuenta con bases de datos registradas y accesibles en el archivo de la DNPDP, las cuales son:

¹⁰http://institucional.telecom.com.ar/pdf/Proteccion_de_datos_personales.pdf

- ◆ Clientes
- ◆ Recursos Humanos
- ◆ Marketing

En las mismas, se describen acotadamente en qué consisten los registros, pero no informan quienes son las personas responsables y en consecuencia, no hay nombre, ni apellido ni dirección de correo electrónico de contacto para hacer ejercicio del derecho de acceso. Solo se brinda un mismo número de teléfono para las dos de las tres bases de datos.¹¹

Por otro lado, de acuerdo a las respuestas obtenidas por la empresa de telefonía IP IFX Networks, se constata la ausencia de elaboración de informes de transparencia en relación a Datos Personales y algo llamativo que mencionan desde la empresa, es que no reciben peticiones del Poder Judicial para dar información de sus usuarios pero sí de las IP.

i Empresas privadas de telecomunicaciones en Argentina

Con el objetivo de entender la inserción del mercado de empresas privadas en la Argentina, a continuación describiremos brevemente la historia reciente de este sector que tiene como origen las privatizaciones en los inicios de la década de 1990.

Las privatizaciones de las empresas del Estado argentino al igual que otra serie de medidas ejecutadas en paralelo, tuvieron un profundo efecto en la estructura económica del país, y el caso de la empresa ENTEL no fue una excepción, sino el comienzo de un nuevo régimen de política pública y mercado.¹²

Luego de la última dictadura militar, Argentina arrastraba un fuerte endeudamiento externo, traído en gran parte para garantizar ciclos financieros y que predisponían a la economía a una necesidad constante de entradas de capitales foráneos. En este sentido, las políticas económicas aplicadas en Argentina estaban orientadas a generar confianza en el mercado financiero y a los inversionistas extranjeros, lo cual se logró, registrándose una fuerte entrada de divisas que se mantuvo hasta 1995. Ingresaron al mercado doméstico una gran cantidad de capitales debido al atractivo de las tasas de interés, la confianza en que no se devaluaría el peso argentino, los incentivos institucionales para la compra de empresas del Estado y las condiciones de desregulación del mercado que permitían no solo la entrada de los capitales, sino también la salida de los mismos con excedentes.

Esta situación de desregulación de términos económicos e institucionales marcó un patrón para los siguientes años en aplicación de política pública e influyeron decisivamente en lo relacionado a

¹¹ Hasta el momento y luego de reiterar el llamado en varias ocasiones, no hemos podido ser atendidos.

¹² <http://mepriv.mecon.gov.ar/entel/ResHist-entel.htm>

privatizaciones de empresas del Estado, con consecuencias de gran tenor en el sector telecomunicaciones. La combinación de estos instrumentos, entre muchos de sus efectos, provocó la erosión de las reservas de divisas, pero al registrarse grandes ingresos de dólares por inversión extranjera, exportaciones, privatizaciones y préstamos, la situación se mantuvo por algunos años. En esta línea, muchos capitales extranjeros generaron utilidades en la Argentina, y debido a que la tendencia fue la no reinversión en el mercado local de las ganancias, conducta aplicada también por las empresas privatizadas, se produjeron la fuga de las mismas al exterior, garantizadas por la desregulación del sistema financiero. El efecto de esta situación fue la profundización de indicadores negativos para la economía argentina, acentuados por el giro de remesas de utilidades de las multinacionales y empresas privatizadas, a sus casas matrices, lo cual perjudicó las reservas del Banco Central y agudizaron la ya altísima vulnerabilidad de la economía a las fluctuaciones de la economía exterior y la liquidez internacional.

En este sentido, una de las transformaciones económicas que se produjeron en la década de los 90, fue la reducción del tamaño del PBI global, en el cual el sector industrial perdió importancia frente al sector servicios que empezaba mostrar signos de crecimiento, explicado por la importancia de empresas con posiciones oligopólicas beneficiadas por las privatizaciones, entre las cuales se destacan aquellas del sector telecomunicaciones.

Fue ENTEL la primera gran empresa del Estado en ser privatizada, la cual inauguró una serie de estrategias comunes a las siguientes privatizaciones como:

- ◆ Campaña desde los medios de comunicación en pos de generar consenso para ver en la privatización la única alternativa posible de mejorar el servicio de telefonía (y luego del gas, luz y transporte) debido a que se favorecería la competencia entre empresas;
- ◆ abrupto aumento de precios y drástico ajuste de personal durante el proceso de privatización, lo cual despojaba a las empresas de toda responsabilidad ya que los despidos y aumentos de tarifa eran asumidos por el Estado;
- ◆ venta de ENTEL por un precio sensiblemente menor al que correspondía.

Por otro lado, además de las irregularidades que ocurrieron durante el proceso de la privatización, el sector de los empleados telefónicos fue afectado en particular y de manera más aguda que otros gremios, generando situaciones de presión inusitada en los mismos. Una de las particularidades del mercado de telecomunicaciones que la diferencian del resto de los servicios públicos privatizados, se relaciona con que la liberalización y desregulación de ese mercado requería de una intervención estatal intensa para garantizar la competencia que se decía buscar.

Sin embargo, debido a inconsistencias regulatorias se generaron obstáculos para la regulación de precios así como para garantizar la entrada de nuevos operadores, lo que en definitiva ha suscitado

consecuencias negativas para los usuarios (y su pérdida de ejercicio de poder como consumidores) además de una gran concentración en el espectro de las telecomunicaciones. Y debido a la dinámica del sector ICT, a medida que fueron evolucionando las condiciones tecnológicas, se fueron formando entornos que favorecieron posicionamientos privilegiados para las empresas ganadoras de la privatización. De manera que hoy en día existe uno de los mercados más concentrados de América Latina en el espectro de las TIC y con los precios más altos de la región.

Aunque en términos generales no hay obstáculos onerosos para ingresar al mercado de las proveedoras de internet, un estudio del especialista en telecomunicaciones Martín Becerra¹³ muestra que para el año 2013 más del 85 por ciento del mercado de banda ancha se concentró en tres empresas: Telefónica, Telecom y Grupo Clarín y de forma similar, el mercado de telefonía móvil también muestra las mismas características en términos de concentración en manos de unas pocas empresas, a saber, Movistar, Claro y Personal.¹⁴

Tabla de Registro de contacto con Empresas de Telecomunicaciones

Empresa de Telecomunicación	Envío de 1º mail	Respuesta	Fecha de respuesta	Recontacto	Envío de carta	Respuesta definitiva
Telefónica	25/04/2016	no	no		27/04/2016	
Telecom	30/03/2016	si	4/04/2016	25/04/2016	27/04/2016	
Nextel	30/03/2016	si	30/03/2016	25/04/2016	27/04/2016	
Telecentro	27/04/2016	no	no		28/04/2016	
Gigared	14/04/2016	no	no		28/04/2016	
Claro	27/04/2016	si	27/04/2016			
Teleread	14/04/2016	no	no			
Aginet	4/05/2016	no	no			
Fecosur	4/05/2016	no	no			
Cooperativa Telefónica de Grand Bourg	4/05/2016	no	no			
Cooperativa Telefónica, de Vivienda y otros Servicios Públicos Del Viso Ltda (TELVISO)	4/05/2016	no	no			
ARNET	2/05/2016	no	no			
Cotelcam	4/05/2016	no	no			
Fibertel/Cablevisión	31/03/2016	si	n/a	04/05/2016		
IFX Networks	4/05/2016	si	5/05/2016			11/05/2016 Respondieron el cuestionario
IP Tel	4/05/2016	no	no			
Jumpnet	4/05/2016	no	no			
Cámara u Organización						
CICOMRA	14/04/2016	no	no	17/05/2016		
ASIT	25/04/2016	si	25/04/2016			
Catip	4/05/2016	no	no			

Guía de preguntas para empresas de telecomunicaciones

1. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

¹³ Martín Becerra, De la concentración a la convergencia, Buenos Aires: Paidós, 2015. Martín Becerra, "Argentina Digital, convergencia y concentración", Blog de Martín Becerra, Diciembre 21, 2014, disponible en: <http://bit.ly/1LIOi8Y>

¹⁴ Pablo Gutiérrez, "Argentina: El Gobierno anunció la quita de subsidios a empresas de telefonía móvil," Noviembre 2011, <http://bit.ly/1SySITK>; Sebastián Premici, "Servicio. . ." Página12, Octubre, 2011, <http://bit.ly/1H5zk9w>

2. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
3. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
4. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
5. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
6. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
7. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
8. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

9. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
10. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
11. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
12. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?
13. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa ¿Está publicada su política de protección de datos ? ¿Dónde? ¿Cómo se accede a dicha política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

Modelo de carta presentada a empresas de telecomunicaciones

27 de abril de 2016, Ciudad de Buenos Aires

De nuestra mayor consideración,

Quienes suscribimos, Eduardo Ferreyra y Jeannette Torrez, ambos investigadores de la Asociación por los Derechos Civiles (ADC), nos dirigimos a Ud. con el objeto de solicitar una entrevista con algún representante de su empresa, para recabar información acerca de la política de protección

de datos personales de la misma. Dicha entrevista nos servirá como insumo para un proyecto de investigación sobre datos personales en América Latina, que está realizando nuestra organización.

Esta petición fue realizada vía e-mail el día xxxx del corriente año. Si bien recibimos respuesta, aún no ha sido fijado día y horario para la entrevista y es por ello que acudimos a realizar la petición por este medio. Para mayor información enviamos la guía de preguntas a realizarse. En caso que por incompatibilidad de horarios se dificultara fijar un encuentro para realizar la entrevista, solicitamos envíen las respuestas a la guía de preguntas por correo o bien vía mail a jtorrez@adc.org.ar o a eferreya@adc.org.ar

Sin otro particular, lo saluda atentamente.

Eduardo Ferreyra

Jeannette Torrez

III Brasil¹⁵

i Introduction

The following report addresses Brazilian telecommunications companies' data protection practices. It was prepared by Internetlab in May and June of 2016 for the Asociación por los Derechos Civiles (ADC) and is structured according to the questionnaire provided by ADC. Answers in part II.1. were provided based on previous research conducted by InternetLab. In part II.2. were included answers to questions directed at telecom companies, which InternetLab sent to two telecom companies. The companies chosen to be part of this research were Vivo (Telefonica) and TIM (Telecom Italia), which are two of the biggest telecom companies in Brazil. According to the Brazilian's Regulatory Telecommunication Agency (ANATEL), Vivo has 28,57% and TIM has 25,88% of the mobile broadband market share, for instance.¹⁶ The other two comparable companies are Claro and Oi, with 25,28% and 18,6% of the market share, respectively. InternetLab reached out to Vivo and Tim and sent the questionnaire on May 4th (Vivo was previously contacted at April 14th, with a noticed that the questionnaire would be sent). The project was briefly explained and the companies were asked about the possibility of engagement by answering the questionnaire. We explicitly informed that the answers did not need to go into detail and that they were free to adopt institutional positions. It is also important to stress that, since InternetLab had launched the project "Who Defends Your Data"¹⁷ (Quem Defende Seus Dados? – QDSD) on the previous week, it was agreed that the

¹⁵ InternetLab members involved in this project: **Fabiane Midori Sousa Nakagawa** and **Jacqueline de Souza Abreu**. Collaborator: **Francisco Carvalho de Brito Cruz**, Director of InternetLab.

¹⁶ Information available in: <http://www.anatel.gov.br/dados/>

¹⁷ Quem Defende Seus Dados? – Lançamento. Available in: <http://www.internetlab.org.br/pt/noticias/quemdefende-seus-dados/>

questions would not be sent out before that date, so the companies would not think that ADC's project was related to the "Who Defends Your Data" research. When contacted, both companies expressed that they would prefer to answer the questionnaire in a written statement. TIM was the only company that positively responded to the solicitation and sent the questionnaire on June 6th. InternetLab contacted once more on May 16th, but obtained no response. The timid engagement and transparency were also hurdles experienced by InternetLab while conducting the "Who Defends Your Data" research. This project is the Brazilian version of the Electronic Frontier Foundation's "Who Has Your Back", published in the U.S since 2011, which has been expanded to countries in Latin America. It promotes transparency and best practices in the field of privacy and data protection by companies that provide Internet access, making Internet users aware of policies that affect the protection of their privacy and personal data, especially against government requests. TIM and Vivo differentiated themselves from other telecom companies as the only ones willing to engage with the project. Even so, they remained cautious and selective in their participation, what can be interpreted as a concern with taking any step that could potentially impair their reputation with clients and their relationship with the government and law enforcement agencies. Their engagement with the questionnaire must be considered against this backdrop.

As informed in the earlier version of this report, which described Brazil's legislative framework, there is no data protection law in force in Brazil. As a result, data protection practices remain mostly obscure. The information publicly disclosed concerning how all the four major companies deal with personal data and data requests by the government could be found in contracts,¹⁸ in websites, and in public statements delivered in processes of public consultation (such as public consultations for the regulation of the Marco Civil da Internet and a Public Hearing on 24th November 2015 concerning Cybercrimes, chaired by the Brazilian Congress).

No company in the sector publishes transparency reports disclosing relevant information about data protection – which is considered an "innovative" practice in Brazil. After the first edition of the QDSD project was finished, these companies (specially TIM) said that they would try to adopt more transparency practices, but these are still modest and uncommon in the sector.

ii Telecommunication Companies' Data Protection Practices

i Questions answered exclusively by InternetLab

In this section, InternetLab answers some of the questions in the survey based on previous research.

¿La empresa elabora informes de transparencia? En caso afirmativo, ¿qué información incluye en tales informes? ¿Son de acceso público? ¿Cómo se accede a ellos? ¿Con qué frecuencia los elabora?

¹⁸ All the contracts analyzed in "Who Defends You Data" project are available in the website: <http://quemdefendeseusdados.org.br/pt/>, under the item "Nossas Fontes".

En caso que la respuesta fuera negativa, ¿Por qué no los elabora?

Most companies elaborate transparency reports (usually, they are referred as "Relatório de Sustentabilidade" in portuguese). However, these reports do not disclose any relevant information about data protection practices and policies. Those reports are released annually and they are available in their websites, addressing financial and infrastructure investments made during the year, social programs and corporate governance practices. Usually, they briefly mention their concern with their client's data security and state that they take the appropriate measures in order to ensure it. The only exception we could find is Oi's report, in which the company presents the numbers of cases dealing with complaints about data leaks. However, they do not disclose any information about demands from the government.

¿El poder judicial o algún tribunal de su país le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

In Brazil, the judiciary may request account information and connection logs, according to the Marco Civil da Internet (Brazil's Internet Bill of Rights), art. 10, second paragraph.

Most of the companies in Brazil have departments that deal with requests from the judiciary and the government in general. There is no information about the particularities of each company, but during the Parliamentary Inquiry Committee concerning cybercrimes and internet security, held in November 24th, 2015, in Brasilia, all the representatives of telecom companies (Vivo/Telefonica, Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze this kind of demands. On this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

Companies follow legal guidelines to give the information. For instance, the request has to be specific: they have to inform the telephone number or IP address (when asking for account information) and also the determined period in which the information will be collected. They do not notify the users about those requests.

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para cancelación y/o suspensión del servicio? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

Usually, the conditions that may lead to the suspension of the service are listed in the companies'

contracts with customers. The contracts are all available in the companies' websites. There is no information about how frequently this content is updated.

Examples of actions that if engaged by the client will end in the termination of the service and blockage of content are: lack of payment for the service, misuse of the service (according to the contract), dissemination of viruses, invasion of privacy, engagement (voluntarily or not) in any harmful activities to the the servers or to third parties. The dissemination of child pornography and racist content (in Vivo/Telefonica's case) may also engage the blockage of content.

En caso de no contar con un protocolo o política de procedimiento para la cancelación y/o suspensión del servicio, ¿cuál es la razón? ¿Qué criterios utiliza para la cancelación y/o suspensión del servicio? ¿Informa al usuario de la potencial cancelación y/o suspensión del 9 servicio en forma previa a efectuarlo? ¿Informa al usuario de la cancelación y/o suspensión del servicio en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con la cancelación y/o suspensión del servicio? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del servicio acerca de este procedimiento?

The conditions and the proceedings are in service contracts. The user has to be notified and also has the right to defend himself/herself according to the Consumer Protection Code.

¿Existe en su país alguna normativa protectora de datos personales? ¿Informa a sus clientes de los derechos que gozan de acuerdo a la ley de protección de datos personales? ¿Cómo?

Currently, there is no specific law about personal data. As stated in the previous version of this report, the Consumer Protection Act (Act n. 078/90) regulates some aspects of the treatment personal data related to the manage of databases for credit analysis.

More specifically, this act, in the article 43, dictates that the consumers must be able to access their data and know about the source of each information. Moreover, the consumer must be informed about the creation of this kind of database and can ask for necessary corrections, which must be accomplished within a 5-day period.

Finally, databases may not contain negative information related to a period longer than five years.

ii Pending questions: Companies' answers

In this section, we will compile the questions sent to the companies and add our commentary when necessary in order to clarify some answers.

¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa, ¿está publicada dicha política de protección de datos? ¿Dónde? ¿Cómo se accede

a su política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

TIM: We respect customers' personal data and do not authorize undue access and use of it. Our 'Customers' Data Privacy Policy' guarantees that the acquisition of users' records and communication data will be allowed only to the collaborators that need to access this information for professional activities. Besides, we guide our actions based on the best market practices, in compliance with the ISO 27001, international norm for information security. Quite the contrary, in the absence of a specific discipline on personal data privacy and protection, TIM adopts as beacon the most compliant practices to the body of norms in force, directing its conduct not only by the Constitution and current law of telecommunications services but also in Law no. 12,965 of 2014 ("Marco Civil da Internet"), Law no. 10,406 of 2002 ("Civil Code") 8078/1990 ("Consumer 10 Protection Code), Law no. 12,850 of 2014 ("Criminal Organizations Act") and Law no. 9,613 of 1998 ("Money Laundering Act").

InternetLab Commentary: TIM did not say whether they publish their 'customer's data privacy policy' and how can we access it, nor has it provided us with a copy of its terms. The only privacy policy InternetLab has been able to find was that relating to the use of TIM's website, in the following link: <http://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade/coletas-dedados-do-usuario>.

¿Algún organismo o repartición estatal le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

TIM: All requests for customer information coming from public agencies are attended only if required under the law or court order. Despite not having a Privacy Chief Officer, any data request made by public agencies to TIM is necessarily subject to the assessment of the internal area responsible for processing such requests, in addition to legal and regulatory sectors of the provider, which act to ensure that the formalities related to such requests are met, including in terms of the legitimacy. Notwithstanding TIM has chosen transparency as one of the values, including the strengthening of internal and external relations grounded on the principles of loyalty and exchange of information, the provider considers - in the absence of legal protection - the publication of statistics not to be recommended, for security reasons, except in case information sharing with oversight committees of the judiciary or law enforcement, when so specifically requested. In fact, whenever so requested in a motivated form by the competent authorities, TIM provides statistics and depersonalized information. Example of TIM's performance in this regard was the collaboration in the parliamentary committee of inquiry of Illegal Wiretapping, in the House of Representatives.

InternetLab Commentary: TIM preferred not to disclose details about user data requests made by government authorities. Although we acknowledge that TIM is not legally obliged to do so, we consider the transparency about data demands is a best practice to be adopted. Law no. 12.965/2014, article 10, 3rd paragraph, allows competent authorities to request personal data without previous judicial order. The law n. 12.850/2013 states that a chief police officer (delegado de polícia, in Portuguese) and the public attorney's office, during investigations involving criminal organizations, may request personal data without a judicial order.

The personal data those authorities may request are: information regarding personal qualification exclusively, parental information, and addresses kept by the electoral justice, telecom companies, financial institutions, internet providers and credit card companies.

Also, the regulatory agency of the telecom sector (Agência Nacional de Telecomunicações – ANATEL) may request personal data, according to the article 8o. of the law n. 9472/97. The Brazilian intelligence institution (Sistema Brasileiro de Inteligência - SISBIN) may have some partial access to this kind of information by forming collaboration with other public institutions, according to the decree n. 4376, article 6, V.

We have no information about specific protocols used by each company and it was not provided by them. During the Parliamentary Inquiry Committee concerning cybercrimes and internet security, held on November 24th, 2015, in Brasília, representatives of the major telecom companies (Vivo/Telefonica, NET/Claro/Embratel, Oi and Tim) claimed that they have special teams whose task is to analyze these kinds of demands. On this matter, ANATEL said that they have a work group which aimed to elaborate a form to be used by all competent authorities when requesting this information. This form is already used by the Federal Prosecution Office (Ministério Público Federal), State Prosecution Offices of the states of Rio Grande do Sul and of Distrito Federal and by the Federal Police.

One of the companies stated that the members of those teams have their identities protected inside the company – the other departments do not know who the people who evaluate data requests are as a measure of security.

Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

InternetLab Commentary: As mentioned in the previous answer, companies follow legal guidelines to give information. During the “Who Defends Your Data” project, InternetLab found out that companies do not notify their users about data demands. It is not mandatory to the companies to do so, but it was mentioned during the meeting with the companies that there was the possibility that most of the requests might be made with a gag order (even if the subject might not require such confidentiality), making it impossible to inform its users in those cases. InternetLab believes that

there are plenty of situations in which confidentiality is not a requirement and that user notification is possible. For instance, in cases in which the Federal Reserve (Receita Federal) might request data: the law does not say those requests are confidential.

¿Cuenta la empresa con protocolos o políticas de procedimiento interno para el filtrado, retiro o bloqueo de contenido? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

InternetLab Commentary: As stated in the first part, the contracts have some information (e.g child pornography) about this point, but companies did not supply additional information.

En caso de no contar con un protocolo o política de procedimiento para el filtrado, retiro o bloqueo de contenido, ¿cuál es la razón? ¿Qué criterios utiliza para el filtrado, retiro o bloqueo de contenido? ¿Informa al usuario y/o titular del contenido del potencial filtrado, retiro o bloqueo del contenido, en forma previa a efectuarlo? ¿Informa al usuario y/o titular del contenido del filtrado, retiro o bloqueo del contenido, en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con el filtrado, retiro o bloqueo del contenido? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del contenido acerca de este procedimiento?

InternetLab Commentary: As stated in the first part, the contracts have some information (e.g child pornography) about this point, but companies did not supply additional information.

¿Tiene su empresa bases de datos inscriptas en algún registro nacional o provincial o departamental? ¿Existe algún tipo de regulación normativa o legal?

InternetLab Commentary: The companies did not inform about this point.

¿La empresa comercializa o cede los datos personales de sus clientes a otras empresas? En caso afirmativo, ¿sigue algún procedimiento determinado para la comercialización o cesión? ¿Comunica esta situación a sus clientes en forma previa o posterior?

TIM: We respect customers' personal data and do not authorize undue access and use of it. Our Customers' Data Privacy Policy guarantees that the acquisition of registrations and communication data of users will be allowed only to the collaborators that need to access this information for professional activities. Besides, we guide our actions based on the best market practices, in compliance with the ISO 27001, international norm for information security.

¿Cuáles son las medidas de seguridad adoptadas para proteger la seguridad y confidencialidad de los datos personales de sus clientes? ¿Estas medidas son de público conocimiento? ¿Son de conocimiento de sus clientes? ¿Con qué frecuencia son estas medidas revisadas o actualizadas? ¿Se notifica la revisión o actualización de medidas a sus clientes? ¿En forma previa o posterior?

TIM: Particularly regarding the safety standards adopted in collection routines, use, data processing and storage of its users, TIM follows in its practices rather strict and rigid standards, as can be

seen from the provider's internal policy of customer data privacy. Still on security standards regarding operations involving personal data, TIM, committed to the protection of its user information, submitted comments to the Public Consultation on the regulation of the "Marco Civil da Internet" promoted by CGI.br by the National Telecommunications Agency ("ANATEL") and the Ministry of Justice, arguing, among other things, the need for detailing in the regulation of Law - in the name of legal certainty - of the minimum standards of information security to be observed by connecting providers and application providers, as well as the obligations relating to transparency and publicity for such measures. For no other reason, TIM is quite enthusiastic about the current draft of the regulatory decree of the "Marco Civil da Internet".

In the case of an eventual claim by the customer of any situation of violation of privacy, we analyze the situation and provide for the necessary clarifications for the solution of the eventual problem. Data privacy practices are communicated to customers through the terms of use of the service plans at the time of signature of the contract. In 2015, no complaints about loss of privacy were recorded. TIM's contracts and website provide users with a link to the website of ANATEL and the direct contact with the Agency, allowing consumers broad access to the current law to be observed by the provider. In addition to being easily accessible on the TIM website, contracts and service provider plans are available to users in the interaction page. By providing in the service contract that [TIM] "shall respect the inviolability of privacy and secrecy of its users communications," TIM extends the reach of the agreement, enabling the aforementioned clause to be filled out with all the regulations established on the protection of rights of telecommunications users, in the best spirit of an irradiation of fundamental rights on private relations. In fact, either for a historical position of TIM or because of its own regulations, the provider does not restrict the protection of its users' data to provisions in the contract.

InternetLab Commentary: The company did not inform how often those measures are updated and are unlikely to do so in the future for security reasons.

¿Qué tipo de medidas toma para que el consentimiento necesario para el tratamiento de datos personales sea libre, expreso e informado?

InternetLab Commentary: The company did not comment about this point, but all the companies agreed during the public debates regarding the Data Protection Law Bill that it should be considered that the user consented to have his/her data treated in the moment it signed the contract – the consent is implicit, not explicit. InternetLab considers that the consent debate is complex and multilayered. It might be too costly for companies to adopt "explicit" consent policies, but if consent could be "implicitly" given, it would be indispensable to provide throughout information about data treatment (which is not a current practice)

¿Tienen un procedimiento para que los usuarios puedan ejercer los derechos de acceso, rectificación y supresión de sus datos?

InternetLab Commentary: The company did not provide more information on this point. However, as stated in the report regarding the review of the Brazilian law background on data protection, the Consumer's Law, in its article 43, states that one will have access to existing information on any consumer database and will have the right of correcting it and canceling it at any given time – the company did not inform how or if there is a specific protocol in this situation.

¿Han habido de casos de usuarios/as que han solicitado sus registros de datos personales? ¿Cuál fue la respuesta de la empresa?

InternetLab Commentary: TIM stated that in case of a breach of confidentiality regarding users' data, the users have ways to contact the company.

Teniendo en cuenta el uso de cookies que utilizan muchos sitios webs ¿Qué tipo de direcciones IP les asignan a sus usuarios? (las opciones son dinámicas o fijas)

InternetLab Commentary: TIM did not reply our questions on the implications of the use of cookies in the IP assignment. All it says about cookies in the Terms of Use¹⁹ of its website is what information is collected (number of accesses to the website; technical information about the browser, IP, operating system, and addresses of reference websites; and eventual solicited personal data, such as name, e-mail, telephone number and mobile device type), how it will not share this data with third parties, unless TIM in good faith understands that “disclosing this information is necessary to respond to claims that the content that you submit to this Site infringes the rights of others or is necessary to protect the rights, property and/or safety of TIM, the users of the TIM website and/or the general public” and how it has the right, but not the obligation to keep this data for a period that do not exceed the term provided by the law. Vivo also informs²⁰ that by accessing its website, some information and data will be obtained by cookies and online research. This data will only be used (with the user consent) to: send information about the company by mail; send email with news; inform about awards and special deals; do e-marketing research and actions.

Anexo: Guía de respuestas de TIM

A TIM é uma empresa comprometida com a proteção da privacidade e dos dados de seus usuários. Não de hoje, a TIM participa das mais relevantes discussões relacionadas ao tema, fomentando debates de mais alto nível, inclusive no plano acadêmico, sobre os desafios colocados pelo mundo digital à tutela dos direitos constitucionalmente estabelecidos.

Respeitamos as informações pessoais dos clientes e não autorizamos seu acesso e uso indevido. Nossa Política de Privacidade de Dados de Clientes garante que a obtenção dos cadastros e dos

¹⁹ Available in: <http://www.tim.com.br/sp/sobre-a-tim/institucional/seguranca/politica-de-privacidade/coletas-dedados-do-usuario> Last access on June 10th 2016.

²⁰ Available in: <http://vivo.tl/2kLiCDu> Last access on June 10th 2016.

dados de comunicação dos usuários será permitida apenas aos colaboradores que precisem acessar tais informações para atividades profissionais. Além disso, balizamos nossas ações nas melhores práticas de mercado, de acordo com a ISO 27001, norma internacional de segurança da informação.

No caso de alegação por parte do cliente de alguma situação de violação de privacidade, analisamos a situação e prestamos os devidos esclarecimentos para solução de eventual problema. As práticas de privacidade de dados são comunicadas aos clientes por meio dos termos de condição dos planos, no momento da assinatura do contrato. Em 2015, não foram registradas queixas e reclamações sobre perda de privacidade.

Todos os pedidos de informações de clientes advindos de órgãos públicos, são atendidos apenas se requeridos nos termos da lei ou da ordem judicial.

Os contratos da TIM e o sítio web da prestadora disponibilizam aos usuários link para a página da ANATEL e os telefones de contato com a Agência, permitindo aos consumidores amplo acesso à legislação de regência a ser observada pela prestadora.

Além de estarem facilmente acessíveis no sítio da TIM, os contratos e planos de serviço da prestadora encontram-se à disposição dos usuários na página de interação.

Ao dispor nos contratos de prestação de serviço que “respeitará a inviolabilidade da privacidade e o sigilo das comunicações de seus usuários”, a TIM amplia o alcance da avença, permitindo o preenchimento de referida cláusula com toda a disciplina normativa quanto à tutela dos direitos dos usuários de telecomunicações, no melhor espírito de irradiação de direitos fundamentais sobre as relações privadas. De fato, seja por uma posição histórica da TIM, seja em razão da própria regulamentação, a prestadora não restringe a proteção dos dados de seus usuários às disposições que constam do contrato.

Bem ao contrário, na ausência de uma disciplina específica sobre privacidade e proteção de dados pessoais, a TIM adota como baliza as práticas mais aderentes ao conjunto normativo em vigor, orientando seu proceder não apenas na Constituição Federal e na legislação de regência dos serviços de telecomunicações, mas igualmente nas Leis n.º 12.965/2014 (“Marco Civil da Internet”), 10.406/2002 (“Código Civil”), 8.078/1990 (“Código de Defesa do Consumidor”), 12.850/2014 (“Lei de Organizações Criminosas”) e 9.613/1998 (“Lei de Lavagem de Dinheiro”).

Particularmente quanto aos padrões de segurança adotados nas rotinas de coleta, uso, tratamento e armazenamento de dados de seus usuários, a TIM segue em suas práticas standards bastante rigorosos e rígidos, conforme se pode depreender da política interna da prestadora sobre privacidade de dados de clientes.

Ainda sobre standards de segurança quanto a operações envolvendo dados pessoais, a TIM, comprometida com a tutela das informações de seus usuários, apresentou comentários às Consultas Públicas sobre a regulamentação do Marco Civil da Internet promovidas pelo CGI.br, pela ANATEL

e pelo Ministério da Justiça, defendendo, dentre outros aspectos, a necessidade de detalhamento na regulamentação da Lei, em nome da segurança jurídica, dos padrões mínimos de segurança da informação a serem observados por provedores de conexão e provedores de aplicação, bem como das obrigações relacionadas à transparência e publicidade dessas medidas. Não por outro motivo, a TIM é bastante entusiasta da atual minuta de Decreto regulamentador do Marco Civil da Internet.

A TIM reitera, que na ausência de obrigações específicas, a prestadora, enquanto agente regulado, observou o conjunto normativo em vigor, que segue no mesmo espírito do Marco Civil da Internet, com obrigações inclusive mais onerosas do que aquelas ali estampadas, adaptando-se aos adendos do Decreto, sem dificuldade.

Apesar da TIM não ter um Privacy Chief Officer, toda e qualquer requisição de dados por órgãos públicos é necessariamente submetida à avaliação da área responsável interna para tratamento dessas requisições, além dos setores jurídico e regulatório da prestadora, que atuam para assegurar que as formalidades relacionadas a tal requisição sejam observadas, inclusive em termos de legitimidade da solicitação.

Em que pese a TIM tenha eleito a transparência como um dos valores, o que inclui o fortalecimento de relacionamentos internos e externos fundamentos em princípios de lealdade e troca de informações, a prestadora considera – na ausência de amparo legal – não recomendável a publicação de estatísticas, por motivos de segurança, salvo em caso de compartilhamento de tais informações com órgãos encarregados da correição do Poder Judiciário ou de segurança pública, quando assim expressamente requisitado. De fato, sempre que assim solicitado de forma motivada pelas autoridades competentes, a TIM fornece informações estatísticas e despersonalizadas. Exemplo de atuação da TIM nesse sentido foi a colaboração no âmbito da CPI de Escutas Telefônicas Ilegais, na Câmara dos Deputados.

IV Chile²¹

El presente apartado busca evidenciar la realidad actual del mercado de proveedores de Internet en Chile. Se busca constatar si las empresas cumplen con estándares de transparencia y responsabilidad a la hora de tratar los datos personales de sus usuarios. Por lo mismo, se analiza el nivel de concentración de mercado en este sector, y los siguientes puntos analizan los contratos de prestación de servicio para averiguar si existen protocolos públicos para el tratamiento de datos personales, y si éstos son públicos para los usuarios. Del mismo modo, su busca discernir si las empresas entregan un nivel adicional de protección a los datos de sus usuarios, o si se contentan con cumplir con las disposiciones de la legislación vigente.

²¹ Colaboraron en la elaboración de este informe: **Valentina Hernández** y **Pablo Viollier**, ambos investigador de Derechos Digitales, así como **Rodrigo Vargas**, **Constanza Alarcón** y **Bastián Riveros**, pasantes del equipo de investigación de Derechos Digitales.

Para esto la metodología utilizada fue la aplicación de una entrevista a dos objetos de estudio, con idénticas preguntas. Junto con eso se realizó un análisis de los términos y condiciones disponibles públicamente en la página web de las compañías, así como de las cláusulas de los contratos de servicio que se encontraban a también a disposición.

Las compañías objeto de análisis en la presente investigación son Movistar y VTR, dos de las mayores compañías de Internet chilenas. Movistar es una de las empresas de telecomunicaciones con mayor presencia y antigüedad en el país, se le conoce comercialmente con ese nombre pero su razón social es Telefónica Móviles Chile S.A, que es la continuadora jurídica de la fusión de 2007 entre Telefónica Móvil de Chile y Telefónica Móviles Chile S.A.²² La empresa ofrece dentro de sus servicios principales, telefonía móvil y fija, Internet y televisión, con servicios adicionales en digital. Por otra parte VTR de razón social VTR Comunicaciones SpA controlada en un 100% por Liberty Global Inc.,²³ ofrece igualmente telefonía móvil (desde 2012) y fija, Internet y televisión, desde hace más de veinte años en el país.

i Mercado de ISP en Chile

El panorama actual en el mercado de proveedores de internet (ISP), se ha caracterizado por su constante expansión, la que ha mantenido un ritmo considerable de crecimiento en los últimos 20 años.²⁴

Así, la oferta de servicios de acceso a Internet fijo continúa localizada exclusivamente en el sector privado, quedando el Estado con un rol fiscalizador y de supervigilancia sobre éstos,²⁵ siendo la Subsecretaría de Telecomunicaciones en conjunto con la Fiscalía Nacional Económica los entes encargados del seguimiento de estos actores.

Para comprender las características del mercado, antes de ahondar en la participación de los ISP, conviene tener en consideración además otros aspectos, en especial respecto al acceso y las características del servicio prestado.

ii Conexiones y Penetración del Internet

Observando la evolución de conexiones y penetración del internet fijo, la tendencia en los últimos años se ha mantenido según cifras de la SUBTEL, alcanzando los 2,74 millones de acceso a internet,

²²<http://www.telefonicachile.cl/inversionistas/telefonica-chile-s-a/la-compania/>[Fecha de consulta: 10 de noviembre de 2016]

²³<http://vtr.com/empresa/somosvtr/index.php>[Fecha de consulta: 10 de noviembre de 2016]

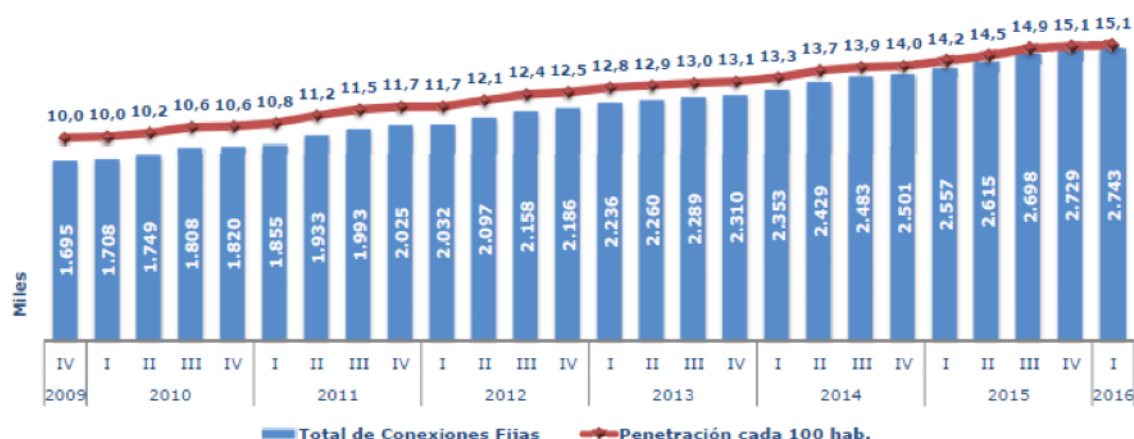
²⁴<https://www.fayerwayer.com/2012/01/internet-en-chile-20-anos-despues/>[Fecha de consulta: 10 de noviembre de 2016]

²⁵ Derechos Digitales, Estado de Internet en Chile. 2014. Pág. 10

experimentando un crecimiento de 7,3% con respecto al año 2015. Lo anterior se expresa en una penetración de internet fija de 15,1 accesos por cada 100 habitantes. En cuanto a sus destinatarios, cabe agregar que un 87,6% corresponde a accesos residenciales, y solo un 12,4% a comerciales.²⁶

Internet Fijo

Evolución de Conexiones y Penetración cada 100 hab.



Fuente: Subsecretaría de Telecomunicaciones, 2016.

Cabe tener presente que este crecimiento en el acceso si bien es sostenido, ha disminuido en relación a las cifras del año anterior (9,1% en el 2015)²⁷, lo que se explica en parte por el considerable aumento del acceso a internet móvil, que en los últimos tiempos ha superado ostensiblemente la conexión fija, alcanzando a marzo de 2016 una concentración de 58,7 accesos por cada 100 habitantes.²⁸

iii Velocidad del servicio

En este ámbito, es preciso distinguir entre la velocidad comercial, es decir, la publicitada por los proveedores y la velocidad real, demostrada por estudios hechos por terceros (Akamai). De esta forma, la velocidad comercial promedio por conexión fija en el año 2015 fue de 13 Mbps. A su vez, según Akamai, la velocidad real en el mismo período fue de 5,8 Mbps.²⁹

²⁶ SUBTEL, Informe Sector Telecomunicaciones Primer Semestre 2016. 2016. pág. 18

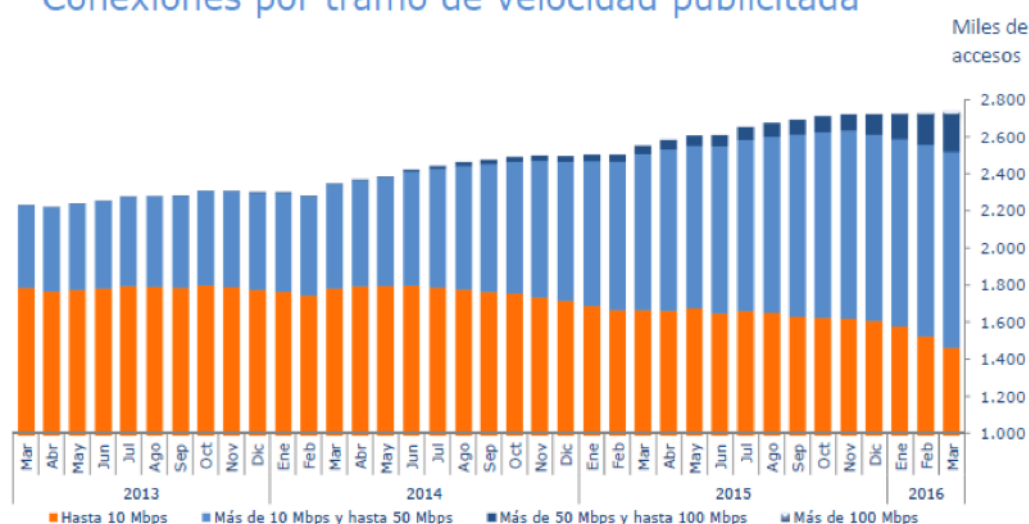
²⁷ SUBTEL, Informe Sector Telecomunicaciones Cierre 2015. 2016. pág. 18

²⁸ SUBTEL, "Informe Sector Telecomunicaciones Primer Semestre 2016. 2016 pág. 13

²⁹ Citado en Ibíd, pág. 20. Informe disponible en: <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-connectivity-report-q2-2016.pdf>

Internet Fijo

Conexiones por tramo de velocidad publicitada



Fuente: Subsecretaría de Telecomunicaciones, 2016.

iv Mercado de Acceso a Internet: Aspectos generales

El mercado de acceso a internet presenta una dinámica particular al estar directamente en comunicación con la innovación tecnológica, al cual influye directa y permanentemente. A su vez, precisa de inversiones para mantenerse vigente frente a nuevas tecnologías, lo que deviene en costos hundidos que significan verdaderas barreras naturales de entrada al mercado.³⁰

En cuanto a cobertura, existen diferencias entre proveedores en la capacidad de despliegue e infraestructura, generándose en ese plano desequilibrios en la participación, siendo aquellas empresas que abarcan gran parte del territorio nacional las favorecidas por la concentración de mercado generada.³¹

v Estructura de mercado

El mercado de ISP, si bien demuestra a todas luces ser de competencia imperfecta, presenta complicaciones a la hora de clasificarlo dentro de un modelo, dada la multiplicidad de servicios ofrecidos por las empresas, la convergencia tecnológica que experimenta el sector, y las distintas estrategias de venta.

³⁰ SALAS, Víctor y CIFUENTES, Diego, "Boletín de Estudios Sectoriales N° 5", Departamento de Economía USACH, pág. 5

³¹ Ibid, pág 15

Un mercado que se caracteriza por empresas que no son tomadoras de precios; diferencias en las economías de alcance expresada en las variedades de servicios y su eficiencia; y la existencia de barreras de entrada provocadas por la inversión que conlleva la actividad.

Estos elementos permiten afirmar que el mercado tiene una estructura oligopólica cuya competencia opera en función de la calidad del servicio y su estructura. Existe un alto grado de concentración de mercado expresado en un alto valor en el índice de Herfindhal-Hirschman.³² Asimismo, la ubicación es una decisión estratégica que impacta directamente en la diferenciación de productos y en la tasa de ventas.³³

Para entender de mejor manera la complejidad del sector, conviene observar las siguientes tablas, que dan cuenta de los comportamientos estratégicos en la distribución de las empresas a través del territorio nacional.

Número de empresas existentes en regiones y conexiones vendidas (2014)

Regiones	Cantidad de empresas existentes en la región	Conexiones Vendidas en la región
XV	13	31.222
I	13	44.588
II	13	107.863
III	13	34.557
IV	13	76.685
V	14	270.189
RM	18	1.214.078
VI	14	65.642
VII	17	73.262
VIII	19	241.761
IX	17	78.670
XIV	16	43.282
X	16	88.811
XI	15	10.876
XII	12	27.687

Fuente: Boletín de Estudios Sectoriales No5, USACH, 2014.

³² De acuerdo al Boletín de Estudios Sectoriales N 5 de la Universidad de Santiago (2014) el índice de Herfindhal-Hirschman (IHH) del mercado de conexiones de Internet fija es equivalente a 3.192,89905. Muy por sobre la media, y suficiente para caracterizar al mercado como de “alta concentración” de acuerdo estándares internacionales.

³³ Ibid, pág 16

Distribución regional de las empresas que venden conexión a Internet (2014)

Empresas	Regiones														
	XV	I	II	III	IV	V	RM	VI	VII	VIII	IX	XIV	X	XI	XII
AT&T Chile S.A.	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-
Entel-Chile S.A.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Telsur	-	-	-	-	-	-	-	-	-	X	X	X	X	X	-
Claro Comunicaciones S.A.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Telefónica	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CTR	-	-	-	-	-	-	X	-	X	X	X	X	X	X	X
Entelphone	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RTC	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
STEL Access	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-
GTD Manquehue	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-
Telcoy	-	-	-	-	-	-	-	-	-	X	X	X	X	X	-
VTR Banda Ancha	X	X	X	X	X	X	X	X	X	X	X	X	-	-	-
Claro Serv. Empresariales	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Fullcom	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CMET	-	-	-	-	-	X	X	X	X	X	-	-	-	-	-
GTD Internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	-
Netline	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Luzlinares	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
E-Money	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Netglobalis	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Luzparral	-	-	-	-	-	-	-	-	X	X	-	-	-	-	-
Pacífico Cable	-	-	-	-	-	-	-	-	-	X	X	-	X	-	-
Global Crossing	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Fuente: Boletín de Estudios Sectoriales No5, USACH, 2014.

vi Empresas participantes

Las empresas presentes en el mercado chileno, a junio del 2014, según información proporcionada por la SUBTEL y sistematizada por investigadores de la Universidad de Santiago, se caracterizan por ser ISP dedicados a dar conexión residencial (22) y empresas de conexiones móviles (9). Además, integran dicho grupo ISP especiales, orientados al sector empresarial (15) y otros a dar conexión internacional (2).³⁴

³⁴ Ibíd, pág. 9

Empresas del mercado de acceso a Internet (junio 2014)

ISP comunes		ISP especiales	
ISP orientados a Residencial	Empresas Internet Móvil	ISP orientados a empresas	ISP Internacionales
Cablevisión Alerce	Movistar	Axesat Chile S.A.	Global Crossing Chile S.A.
Claro Chile S.A.	Claro	Cibercenter S.A.	Telefónica International Wholesale Service Chile (TIWS)
Compañía de Teléfonos de Coyhaique S.A.	Entel PCS	Comunicaciones Netglobalis S.A.	
Compañía Nacional de Teléfonos, Telefónica del Sur S.A.	VTR Móvil	E-Money Chile S.A. parte nacional	
Complejo Manufacturero de Equipos Telefónicos (S.A.C.I.)	Virgin	Globalcom S.A.	
Comunicación y Telefonía Rural S.A.	GTD Móvil	Gtd Internet S.A.	
Empresa Nacional de Telecomunicaciones S.A.	Nextel	IFX Networks Chile S.A.	
Enlaces Regionales de Chile S.A.	Falabella	Ingeniería e Informática Asociada Limitada	
Fullcom S.A.	Telestar	Latlink Net S.A.	
Gtd Manquehue S.A.		NewPlanet (Servicios de Ingeniería de Tecnología de Información)	
Inalámbrica S.A.		Nivel 5 S.A.	
Internet Satelital Ltda.		Servicios Internet Ltda. (Tecnoera)	
ISP Consultec SPA		Soc. de Telecomunicaciones Geonet Ltda.	
Luzlinares S.A.		Verizon Chile S.A.	
Marcom Ltda.		Silica Networks Chile	
Netland Chile S.A.			
Netline Telecomunicaciones S.A.			
Optic			
Pacífico Cable S.A.			
Stel Chile S.A.			
Telefónica Chile S.A.			
VTR Banda Ancha S.A.			

Fuente: Boletín de Estudios Sectoriales No5, USACH, con información de la SUBTEL.

vii Participación de mercado

Si bien a simple vista el número de empresas participantes derriba la idea de un oligopolio, es necesario señalar que estas están altamente relacionadas entre sí, cambiando nombres en función del servicio específico prestado, operando en la materialidad como grupos empresariales en su actuación en el mercado. Para dar cuenta de esto, en la tabla presentada a continuación es posible observar la composición de los conglomerados, basada en datos recogidos el año 2014.³⁵

³⁵ SALAS, Víctor y CIFUENTES, Diego. Boletín de Estudios Sectoriales N° 5, Departamento de Economía USACH, 2014. pág. 18

Grupos económicos en el Sector de provisión de acceso a Internet en Chile (2014)

Grupo	Participación del grupo en el mercado	Empresas que componen el grupo de empresas
Grupo Movistar (ex Grupo Telefónica)	38,71%	1. Movistar
Grupo Entel	1,27%	1. Entel Chile S.A. 2. Entelphone
Grupo Claro	11,23%	1. Claro Comunicaciones S.A. 2. Claro Servicios Empresariales
Grupo GTD	7,69%	1. Telsur 2. GTD Manquehue 3. Telcoy 4. GTD Internet
Grupo VTR	38,23%	1. VTR Banda Ancha
Otros	2,87%	No constituyen un grupo de empresas

Fuente: Boletín de Estudios Sectoriales No5, USACH, con información de la SUBTEL.

Al igual que en años anteriores,³⁶ a la fecha es posible identificar a dos actores dominantes, VTR y Movistar,³⁷ que poseen en conjunto más del 74% del total de conexiones de internet fija, demostrando el oligopolio experimentado en el sector. Dicha situación es sostenida desde los últimos 5 años, lo que en suma atenta de manera sustancial a la competencia y dinamismo del mercado.

Estas cifras, como se observa en la tabla a continuación, han tenido variaciones insignificantes, persistiendo la concentración en el área. Lo anterior se ve reflejado en el desarrollo de infraestructura, teniendo las empresas anteriormente mencionadas gran parte de las conexiones efectuadas en el país en los últimos siete años.

Revisando el total del mercado, actualmente el porcentaje de participación por empresa proveedora se distribuye de la siguiente forma: VTR (37,4 %), Movistar (36,7 %), Grupo Claro (12,2 %), Grupo GTD (8,9 %), Grupo Entel (1,3 %) y otros actores (3,5 %).³⁸ Al respecto, haciendo un análisis pormenorizado de estos actores, es visible una disminución en la incidencia de Movistar de un 2%, con un correlativo aumento en la participación del Grupo Claro, que si bien es bajo (0,8%), conviene tener en consideración para análisis ulteriores.

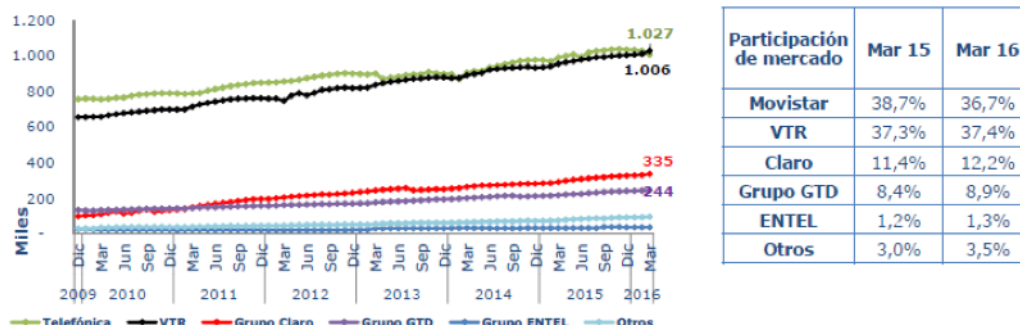
³⁶ SUBTEL. Estadísticas de la Industria de Telecomunicaciones, Mayo 2012. pág. 19

³⁷ De ahí que fuesen estas dos empresas las escogidas como objetivo de estudio a través del análisis de sus contratos y la realización de entrevistas.

³⁸ SUBTEL. Informe Sector Telecomunicaciones Primer Semestre 2016. 2016 pág. 19

Internet Fijo

Conexiones por Empresa y Participación de Mercado



Fuente: Subsecretaría de Telecomunicaciones, 2016.

Si bien no es posible establecer un nexo causal entre el nivel de concentración de mercado y las condiciones de protección de tratamiento de datos personales, esta circunstancia puede eventualmente servir como contexto para los hallazgos obtenidos a través de las entrevistas y el análisis de contratos. Análisis comparativo de disponibilidad de información en página web, respecto a términos y condiciones

En análisis de la información provista públicamente por las empresas objeto de estudio muestra VTR tiene una página web bastante intuitiva,³⁹ con acceso a sectores de información con un tamaño de fuente considerable y llamativas.

Del mismo modo, se encuentra disponible una sección donde está publicada, de forma sencilla y general, cada uno de los derechos que tienen los usuarios de tecnología y telecomunicaciones.⁴⁰ El reglamento de servicios de telecomunicaciones está públicamente disponible para descarga,⁴¹ acompañado de extracto general en un formato amigable para el usuario.

La información sobre los servicios de “Banda Ancha VTR”, así como las características y condiciones de neutralidad en la red,⁴² información de qué es Internet y de los servicios de la compañía en parámetros técnicos de banda ancha,⁴³ junto con las políticas de administración de red.⁴⁴

En el apartado de políticas de administración de red de VTR se encuentra en detalle la administración de qué puertos y filtros IP utiliza, luego una breve sección de información respecto de gestión de

³⁹<http://vtr.com>[Fecha de consulta: 10 de noviembre de 2016]

⁴⁰<http://vtr.com/productos/derechosdeusuario/>[Fecha de consulta: 10 de noviembre de 2016]

⁴¹<http://vtr.com/reglamentotelco/>[Fecha de consulta: 10 de noviembre de 2016]

⁴²<http://vtr.com/neutralidad/>

⁴³<http://vtr.com/neutralidad/a1.php>[Fecha de consulta: 10 de noviembre de 2016]

⁴⁴<http://vtr.com/neutralidad/b4.php>[Fecha de consulta: 10 de noviembre de 2016]

acceso a contenidos recurrentes, de administración de capacidades, y de bloqueo al acceso a sitios de abuso infantil. También se puede encontrar un apartado de contratos donde se puede descargar los siguientes documentos:⁴⁵

- ◆ De formularios la solicitud de servicios fijos y solicitud de servicios móviles;
- ◆ De contratos de suministro de servicios fijos, servicios móviles y negocios;
- ◆ De características del servicio de televisión, las características de televisión VTR, listado de canales fijos y variables, y
- ◆ De condiciones comerciales, servicios móviles, condiciones de arriendo de equipos, servicios hogar y negocios.

En contraste, Movistar cuenta con un sitio web llamativa en el sentido comercial, sin embargo en cuanto a la información sobre derechos del consumidor y/o usuario de telecomunicaciones muestra altos grados de déficit.

Si bien existe información disponible, esta está presentada en forma poco amigable con el usuario. Mucha de la información se presenta en forma de documentos disponibles para descarga en formato PDF o redireccionamiento a documentos estatales de normativa, sin tener una pestaña general y amigable con el usuario que de forma general y resumida presente los reglamentos y normas a las que en virtud de normativa estatal queda limitada o sujeta la actividad de la compañía en la entrega de servicios. Los derechos del usuario/consumidor tampoco está disponible de forma accesible para los clientes.

Los documentos que Movistar tiene en su página para descarga son:⁴⁶

- ◆ Deberes de los usuarios; reglamentos de reclamos de servicios de telecomunicaciones aprobado por el Ministerio de Transportes y Telecomunicaciones;
- ◆ Derechos de los usuarios de telecomunicaciones;
- ◆ Decreto de Reglamento de Servicios de Telecomunicaciones;
- ◆ Acuerdo con la Fiscalía Nacional Económica;
- ◆ 15 documentos para descarga de los diferentes planes de contrato de telefonía móvil;
- ◆ 2 documentos de condiciones contractuales de planes de contrato de telefonía prepago; condiciones contractuales de servicio “Movietalk”;

⁴⁵<http://vtr.com/productos/moviles/contratos>[Fecha de consulta: 10 de noviembre de 2016]

⁴⁶<http://www.movistar.cl/PortalMovistarWeb/centro-de-ayuda/condiciones-comerciales-y-contractuales-de-telefonía-movil-y-banda-ancha-movil>[Fecha de consulta: 10 de noviembre de 2016]

- ◆ Condiciones contractuales de servicio multiasistencia premium 505;
- ◆ Documento para descarga de política de privacidad de movistar (de tan solo una plana, y que se remite a repetir partes de la ley 19.628 por lo que no está disponible en la página una política de privacidad de la compañía en la página);
- ◆ Finalmente otros dos documentos para descarga de solicitud de servicios y otro de servicio “smart kids”.

El sitio también cuenta con una sección referida a la neutralidad en la red.⁴⁷ En ella se encuentran disponibles una serie de documentos para descarga, titulados: “Sobre características comerciales de los servicios” (qué servicios incluye cada plan y costo); “Medidas de gestión de tráfico y administración de red”, donde se puede descargar un documento para servicio de “banda ancha fija y satelital” y otro para servicio de “Banda ancha móvil, planes multimedia, planes de datos y planes de internet en tablet”.

Estos documentos disponen información general sobre, en qué consisten y por qué se realizan, acciones tales como almacenamiento temporal de CDN y la gestión de sesiones del usuario, señalando por ejemplo, que estas se cierran en un tiempo máximo de 29 horas para distinguir el inicio y fin de una sesión e identificar al cliente y así responder a solicitudes de los juzgados sobre esta información. También refiere a la gestión de equipamiento de terminal del lado usuario, administración de las direcciones IP, etc. Sin embargo, no se señala en términos técnicos ni con el detalle debido cómo se intervienen o administran estos puertos ni se establece un protocolo para ello, solo el fin de las acciones y qué pasaría de no realizar estas providencias.

Respecto de las cláusulas y condiciones de los contratos, resulta preocupante constatar que sólo se encuentran disponibles los contratos de datos y telefonía móvil y de telefonía fija por separado y de televisión fija. No están disponibles los contratos de los servicios más promocionados en la página web, es decir, no están publicados para descarga o consulta online el contrato de servicios trío, o dúo (internet + televisión + telefonía; o internet + televisión o telefonía), ni de ninguno de los otros servicios que ofrece la compañía relacionados con Internet fija hogar.⁴⁸

Incluso, fuimos capaces de constatar que los mismos usuarios, que son clientes de Movistar y tienen una cuenta en su “Sucursal Virtual” tampoco pueden acceder de forma inmediata a una copia de su contrato vigente, ni sus condiciones. Del mismo modo, para aquellos clientes que tienen una cuenta en la Sucursal Virtual, está disponible un enlace llamado “Condiciones Contractuales”, el cual al momento de realizarse esta investigación dirigía a la página principal de la compañía, impidiendo a

⁴⁷ <http://www.movistar.cl/web/movistar/neutralidad-en-la-red> [Fecha de consulta: 10 de noviembre de 2016]

⁴⁸ <http://www.movistar.cl/PortalMovistarWeb/centro-de-ayuda/condiciones-comerciales-y-contractuales-de-servicios-hogar> [Fecha de consulta 10 de noviembre de 2016]

los clientes y usuarios de Movistar tener acceso a los términos y condiciones de su contrato de forma transparente y expedita.

viii Análisis de contratos

En cuanto a los contratos de servicio, es posible constatar que en el sitio web de VTR se encuentran disponibles los contratos de suministro de servicio de telefonía local, televisión e internet, este contrato se encuentra bajo el título de “Contrato de Suministro Servicios Fijos”.⁴⁹

El estudio de los distintos contratos de servicio de VTR muestra que, por ejemplo la cláusula quinta del contrato sobre servicios de telefonía local no establece ningún tipo de condición o protocolo para el procesamiento de requerimientos judiciales de interceptación de la línea. En el mismo sentido, la cláusula sexta sobre acceso a internet, en su punto 2 señala que VTR podrá aplicar políticas de administración de la red y del tráfico, sin establecer claramente las circunstancias ni formas en que dicha administración de la red y tráfico operaría. De esta forma, al no detallarse debidamente estas circunstancias en el contrato, aun cuando la información se encuentre disponible en la página, podría considerarse que se están faltando a los deberes de información en materia de derecho del consumidor. En efecto, el artículo 3 de la ley 19.496 de protección y derechos del consumidor establece como obligación del proveedor la entrega de información básica comercial, deber que podría considerarse incumplido por las condiciones antes descritas.

Más preocupante aún, resulta constatar que el punto 11.1 de servicio de acceso a Internet, se señala que las disposiciones contenidas en este punto se complementan con las condiciones de uso que se encuentran disponibles en la misma página web. Es importante señalar que si bien esto se señala en el contrato, este material que efectivamente está disponible en la página web, no se puede considerar parte del contrato, puesto que no se incluye ni en un anexo.

Lo anterior se vuelve más preocupante, si se tiene en consideración que esto puede permitir a la empresa modificar unilateralmente las condiciones establecidas en su página web, las cuales tampoco cuentan con una fecha cierta. Esto implica que dicha cláusula puede eventualmente constituir una cláusula abusiva de acuerdo al artículo 16 de la Ley del Consumidor.

La cláusula 11.6, referida a la Administración de la Red y Modificaciones Tecnológicas, señala que VTR podrá aplicar políticas de administración eficiente de su red y del tráfico cursado por la misma, señalando vagamente en qué puede consistir las medidas y los fines que tiene al implementarla y los casos en que son aplicables. En esta materia la cláusula también una remisión abierta a las condiciones establecidas en la página web de la compañía, pero sin establecer un enlace específico, ni una fecha cierta de dichas condiciones.

⁴⁹http://vtr.com/CS/vtr_f3/contrato-de-suministro.pdf

En el punto 11.7 se busca limitar la responsabilidad de la compañía por acciones realizadas por el el suscriptor del contrato. Las circunstancias en las cuales el usuario incurriría en responsabilidad tampoco están contenidas en el contrato, sino que en una remisión abierta al sitio web de VTR.

La cláusula 13 sobre Datos Personales establece, en su punto 13.1, que VTR mantendrá registros automatizados de la interacción del cliente con los servicios de la compañía sin que estas operaciones impliquen la asociación a un cliente identificado o identificable. En el punto 13.2 se señala que la empresa analiza y registra la información de cada suscriptor en la interacción con los servicios de VTR, con la finalidad de entregar adecuadamente los servicios contratados. Entre dicha información se menciona la fecha de películas contratadas, el número y duración de llamada telefónica, las fechas de pago, etc. Del mismo modo, se establece que esta información es directamente procesada por VTR, velando por la confidencialidad de estos datos, sin perjuicio de que se establezca un deber para VTR de informar algunos de datos según la normativa actual vigente o a requerimiento de una autoridad competente.

Es importante respecto de este punto comentar que es grave que se establezca de forma alternativa que se procederá a este requerimiento ya sea en virtud de la ley o en el señalamiento genérico de “una autoridad competente”. Esto deja en evidente desprotección la privacidad del usuario, pues al señalar “una autoridad competente” y sin que el requisito de, en virtud de una norma, se establezca de forma copulativa, podría entenderse que bastará el requerimiento de cualquier autoridad con competencia sin señalar si esta competencia debe ser respecto de investigar un posible delito, o competencia específica para requerir información privada, o si basta una competencia de autoridad administrativa, o autoridad judicial, etc.

Estos requisitos deberían estar establecidos de forma copulativa, es decir, autoridad legalmente habilitada para requerir información privada y en virtud de una norma de derecho público o autorización de juez.

Finalmente, la cláusula 13.3, y en virtud del artículo 4 de la ley 19.628 sobre protección de datos personales, se establece que VTR se reserva la facultad de poder tratar y remitir a terceros los datos personales del usuario con fin de comunicar servicios o productos y que el suscriptor en la firma del contrato autoriza a VTR para estas acciones, conservando el cliente la facultad de revocar esta autorización. Es importante señalar que si bien esta cláusula se encuentra en el marco de lo legal, esta facultad ha sido altamente criticada por la doctrina chilena cuya crítica y posición se detalla en este estudio más adelante.

En la página Movistar solo se encuentran disponibles dos tipos de contrato,⁵⁰ de entre todos los servicios que la compañía ofrece, estos son “Condiciones Contractuales del Servicio de Banda Ancha Móvil” y “Condiciones Contractuales de Servicio Telefónico Móvil”.

⁵⁰ <http://bit.ly/1intd28>; <http://bit.ly/2jqYcTg>

La cláusula 5 de “Condiciones Contractuales de Servicio de Banda Ancha Movil”, se refiere a datos personales. En 5.1 se señala la facultad de la Compañía para los datos sean, en virtud de ley 19.628 sean, tratados y utilizados por la Compañía. La cláusula es sumamente genérica, ya que simplemente se remite al contenido de la ley, sin señalar tampoco algún artículo en específico de la misma. Esto deja en evidencia que Movistar no aplica un nivel adicional de protección al establecido por la legislación vigente, el cual es considerado por la mayoría de la doctrina como sumamente insuficiente, como hemos dado cuenta en la primera parte de este informe.

La cláusula 7 refiere a medidas de gestión de tráfico y administración de red. Al igual que en el caso de VTR, el punto 7.1 del contrato de Movistar señala que las características técnicas y operativas se pueden encontrar en el documento de Neutralidad de la Red, alojado en su sitio web. Como hemos mencionado anteriormente, dicho documento carece de detalle técnico y sólo señala los fines y riesgos de ejecutar las acciones de administración. La misma cláusula también establece que “la enumeración de estas medidas de gestión de tráfico y administración de red no es taxativa, pudiendo TMCH tomar o ejecutar medidas o acciones adicionales que autorice la normativa sectorial y que no afectarán el Servicio contratado por el Cliente”.

ix Análisis de entrevistas

VTR

La compañía Movistar accedió a dos entrevistas con dos profesionales. El primero cumple funciones vinculadas con la protección de datos, en particular con los requerimientos de información a través de procesos judiciales y el segundo vinculado al área de administración de la red y datos de servicios de telefonía. La empresa VTR accedió a la entrevista en un formato escrito el que se contestó por diferentes áreas en cada materia, hasta ser reenviado a los investigadores. A ambas empresas le fueron realizadas las mismas preguntas.

De acuerdo a las respuestas entregadas por VTR, es posible constatar que declaran contar con una política de privacidad, la que se encuentra publicada en su página web.⁵¹ Del mismo modo, la empresa señala que no cuentan con una política de actualización periódica de las mismas, sino que las modificaciones son realizadas cuando resulta necesario.

La empresa no cuenta con informes de transparencia relacionados con el tratamiento de datos personales, pero sí con “informes de sustentabilidad”⁵², además de información general acerca de la compañía en su sitio web.⁵³ Sin embargo, ninguno de dichos documentos contiene apartados

⁵¹ Disponible en: <http://vtr.com/privacidad/>

⁵² La última versión de este informe está disponible en (PDF): <http://bit.ly/2jRBm3i>

⁵³ Disponible en: <http://vtr.com/empresa/somosvtr/index.php>

especiales relacionados con el tratamiento de datos personales ni entrega mayores luces sobre el asunto.

Respecto de la entrega de datos personales a propósito de procedimiento judiciales y de investigaciones criminales, señalan que efectivamente han recibido requerimientos de información, y que la información que ellos tienen respecto de sus clientes es principalmente en relación con la contratación de servicios y documentos presentados por el cliente.

Los requerimientos que han recibido son del Ministerio Público el que actúa a través de la Policía o Carabineros, la petición se les formaliza mediante un oficio emitido por los tribunales el que se canaliza o por oficio de la compañía o a través del sistema informático que poseen para dar respuesta a estos requerimientos. Sin embargo, no existen estadísticas públicas de la empresa en lo relacionado a la cantidad de solicitudes y el porcentaje que son acogidas por la empresa.

Señalan que la información que la compañía envía es estrictamente la solicitada, sin adjuntar copias de documentos a menos que esto sea expresamente requerido y se envía de forma directa al tribunal requirente. Respecto de los requerimientos del Ministerio Público, igualmente la compañía accede a ellos, pero sólo si se extienden en el marco de la investigación de un delito, el que generalmente se gestiona igualmente por organismos policiales. Para ello, se solicita a estos, la orden de investigar emanada por el fiscal a cargo de la investigación junto al oficio respectivo. Dichas solicitudes son bajo obligación de confidencialidad por parte de las autoridades, por lo que se ven impedidos de informar al cliente el requerimiento.

La empresa también da cuenta de haber recibido requerimientos de organismos o reparticiones estatales tales como Subtel, quienes requieren información general de la compañía invocando el artículo 37 inc. 2 de la Ley General de Telecomunicaciones. En algunas ocasiones los documentos solicitados contienen información personal de los clientes y en esos casos la VTR solicita a la autoridad que esta mantenga reserva de la información suministrada, por ejemplo, cuando se requieren boletas específicas de un cliente para verificar el cumplimiento de alguna obligación).

Con el fin de responder a los requerimientos de la autoridad administrativa, la compañía señala que verifica que el requerimiento se encuentre enmarcado en el cumplimiento de funciones específicas de cada autoridad, y que en los casos que sea posible entregar a la autoridad la información solicitada sin revelar información personal de un cliente se procede excluyendo estos datos.

Respecto del filtrado, retiro o bloqueo de contenido en internet, señala que la compañía contempla esta posibilidad frente a algún requerimiento judicial asociado a una potencial infracción a la propiedad intelectual.⁵⁴ Sin embargo a la fecha no han debido ocupar este protocolo,⁵⁵ pues no han recibido tales solicitudes judiciales y por lo mismo no han estructurado un proceso interno formal.

⁵⁴ Artículo 85 y siguientes de la ley de propiedad intelectual.

⁵⁵ Disponible en <http://vtr.com/productos/propiedadintelectual>

Adicionalmente VTR adhiere a un proyecto de responsabilidad social que contempla el bloquear el acceso a contenidos que tengan las características de abuso infantil, para este efecto aplican un procedimiento en coordinación con la Internet Watch Foundation.⁵⁶

Respecto a la existencia de un protocolo interno de cancelación y/o suspensión del servicio, se señala que efectivamente se contempla esta posibilidad en el contrato de suministro⁵⁷ en caso de que el cliente incurra en una infracción al mismo, como puede ser la falta de pago de la cuenta mensual. A pesar de que no cuentan con un protocolo para este tipo de situaciones, la infracción al contrato por no pago es recurrente y en casos graves se contempla informar al cliente sobre la terminación del contrato.

Respecto de la base de datos de clientes, señalan que la empresa no tiene base de datos inscritas en algún registro nacional, provincial o departamental, luego que la compañía no comercializa ni cede bases de datos con la información de los clientes. La empresa matriz que es Liberty Global prohíbe la venta de datos personales, tanto de clientes como colaboradores, no obstante tienen proveedores y socios comerciales a quienes autorizan el tratamiento de los clientes a nombre de VTR bajo los fines estrictos de alguna actividad específica encomendada, sin que tengan autorización para usar esa información para otros fines u en otros ámbitos.

La compañía señala contar con diversas medidas y políticas que tienen por fin proteger la seguridad y confidencialidad de los datos de los clientes. En la política de privacidad del consumidor se entrega una orientación general sobre cómo proceden. Las medidas que adopta VTR para que el consentimiento en el tratamiento de datos personales sea libre, expreso e informado, es que se indica en el contrato la finalidad que tiene el tratamiento de estos datos, y que el cliente se reserva la posibilidad al momento de contratar de autorizar o no el uso de sus datos para la remisión de ofertas comerciales, el cliente tiene derecho a que su información personal incompleta o incorrecta sea corregida, para ese efecto tienen habilitada la dirección privacidad@vtr.cl para recibir esas solicitudes. La empresa señala que hasta el momento no han recibido por parte de sus clientes solicitudes de registro de sus datos personales. Finalmente, teniendo en cuenta el uso de cookies que utilizan muchos sitios webs, VTR señala que utiliza un criterio de asignación dinámica de números IP.

Movistar

En el proceso de entrevistas, Movistar señaló que como empresa formar parte del Grupo Telefónica. Este tiene un comité global de privacidad, liderado en la matriz en España, donde se elaboran los lineamientos y principios generales para todo el grupo Telefónica.

Sin embargo, todas las teleoperadoras también tienen una política de privacidad local, que sigue la

⁵⁶ Más información disponible en <http://vtr.com/neutralidad/b4.php>

⁵⁷ Disponible en http://vtr.com/CS/vtr_f3/contrato-de-suministro.pdf

misma línea de la legislación actual vigente en Chile. Actualmente Telefónica cuenta con una guía, de alrededor de una plana, de política de protección de datos que da lineamientos muy generales. Sin embargo, expresaron su voluntad de subsanar dicha situación y entregar un material más detallado.

Al igual que VTR, dicha política de protección de datos no es actualizada con una regularidad establecida, sino que se modifica según sea necesario. El material que está disponible en la página web en condiciones contractuales y comerciales está siempre en permanente revisión y pasa por un procedimiento de validación interna donde opinan diversas áreas como regulación, legal, tributaria, operaciones, etc.

Respecto de los informes de transparencia en la realidad regional o local, anualmente tiene que informar a la matriz central a través de un “informe de sostenibilidad” donde analiza, entre otros ámbitos, los casos de riesgo que han tenido en materia de protección de datos. Entre ellos, incidencias, procedimientos administrativos sancionatorios, o procedimientos judiciales en materia de datos, además de informar el cambio normativo local en materia de datos personales, estos se reportan a Telefónica España.

Telefónica Chile recibe regularmente requerimientos de la autoridad judicial, cuyo procesamiento está a cargo de la unidad de requerimientos judiciales. Esta unidad canaliza las solicitudes judiciales o del Ministerio Público, requerimientos que pueden incluir la entrega de datos personales de los clientes por parte de la empresa. Señalan que de conformidad a la normativa vigente se puede pedir por ejemplo registro de tráfico, de conexiones, registros de IPs, etc.

Señalan que al acceder a estos requerimientos actúan simplemente en cumplimiento de la ley. El área a cargo lo que realiza es, una revisión sobre la legalidad y la validez del requerimiento, y cuando no están en forma conforme a la ley entonces se han sido debidamente rechazado. Sin perjuicio que la autoridad judicial sea un tribunal ordinario o especial, la empresa informó tiene suscrito un acuerdo con la Fiscalía Nacional del Ministerio Público, el que se traduce con un protocolo de buenas prácticas respecto a la interceptación de legal de comunicaciones. Este acuerdo surgió a instancias del Fiscal Nacional y fue suscrito por las otras empresas del rubro y no es de carácter público.

Otro punto interesante que fue mencionado en las entrevistas es que la empresa señaló que ellos consideran dentro de comunicaciones privadas el almacenamiento de metadatos, y que en ese sentido el requerimiento por la autoridad de esa información está sometido al mismo resguardo.

Existe además un caso que se da en la práctica pero que no está detallado en la ley, que es el de autoridades administrativas que solicitan información personal de clientes, que debe suministrarse por tratarse del ejercicio de facultades implícitas que han sido conferidas por la ley. Un ejemplo entregador fue el de la Subsecretaría de Telecomunicaciones (SUBTEL), no tiene expresamente conferida la facultad legal para solicitar información o datos personales de los clientes, pero que ellos consideran como una facultad implícita, ya que de lo contrario sería impracticable que pudiera fiscalizar el cumplimiento de la normativa de telecomunicaciones. Por ejemplo, cuando la misma ha

solicitado a través de un oficio información respecto de una falla masiva de un servicio, es habitual que pida información sobre el número de usuarios que se vieron afectados, cuáles son esos usuario, qué líneas son, etc.

Respecto de si se informa o no a los clientes acerca de la recepción de un requerimiento de información, o de la entrega de información a la autoridad, la compañía señala que no tiene contemplado un protocolo y que es de cargo de la autoridad al formalizar una investigación, el informarle al usuario que se interceptaron sus comunicaciones.

Consultados sobre si la empresa cuenta con un protocolo interno para cancelación o suspensión del servicio, se señaló que, primero que todo la prestación de servicios que realizan tiene un objeto definido, es distinto el contrato que hace una persona natural para uso doméstico a una persona natural o jurídica que lo solicita para fines comerciales como una residencial u hotel. Cuando la empresa advierte que se está haciendo mal uso del servicio, lo que implica utilizarlo para un fin distinto, por ejemplo lucrar, y cobrar por utilizar televisión o internet que estaba destinado a uso doméstico, no se les cancela o suspende de inmediato, pero sí se interviene dentro de la legalidad, para que el usuario deje de efectuar el fin indebido.

En cuanto a la cancelación o suspensión por no pago, es una acción que está expresamente contemplada en el Decreto 18 de 2014 del Ministerio de Transportes y Telecomunicaciones. Debido a que este sería un contrato regulado, señalan que la compañía no tiene muy flexibilidad al momento de establecer las condiciones del mismo.

Respecto a si la compañía tiene o no bases de datos inscriptas en algún registro nacional o provincial o departamental, ninguno de los dos profesionales consultado de telefónica tenía claridad de si esto era así o no. Sin embargo, refirieron a que de todos modos el registro de bases de datos es obligatorio solo para los organismos públicos pero voluntario para los privados.

Consultados sobre si la empresa comercializa o cede los datos personales de sus clientes a otras empresas, se señaló que al encontrarse expresamente regulado en el Decreto 18, y al ser Telefónica una empresa global, declaran que los datos recopilados sólo son utilizados para los fines específicos de la prestación del servicio. Es una norma que el cargo de Data Protection Officer de Telefónica Chile debe resguardar por su estricto cumplimiento en todas las iniciativas comerciales de la compañía. En aquellos proyectos en que participan otras personas o entidades del grupo telefónica, siempre se levantan los requerimientos legales en materia de datos personales, ocupándose de salvaguardar el cumplimiento de la normativa de protección de datos personales. Para ello la empresa declara tomar las medidas de seguridad pertinentes, lo que puede significar por ejemplo la anonimización de datos, o establecer específicamente quién es el responsable del tratamiento de datos y a quién se le asigna la calidad de encargado de tratamiento en conformidad a la ley.

Señalan que en las relaciones con empresas proveedoras se estipula que la información entregada en virtud de los contratos sólo puede ser utilizada para lo fines específicos del mismo y no puede

desviarse para otros fines, y que una vez terminado el contrato esta información debe destruirse.

Las medidas que toma Telefónica para que el consentimiento en el tratamiento de datos personales sea libre expreso e informado, las entienden subsumidas en la suscripción misma del contrato, ya sea por vía remota o en la suscripción del formulario de contrato. Esto ya que este documento a las condiciones contractuales y comerciales están publicadas en la página web. En dichas se señalan los fines de almacenamiento de datos. Telefónica entiende que a través de este acto el cliente autoriza al menos implícitamente el uso de información personal para que la compañía pueda prestar los servicios o productos que contrata, ya que sin esa información personal es imposible prestar el servicio de telecomunicaciones.

La compañía tiene múltiples procedimientos de atención y además existe un portal interno donde se revisan los procedimientos para que los usuarios puedan ejercer los derechos de acceso, rectificación y supresión de sus datos. Es frecuente que los usuarios pidan información, la compañía por su parte se ocupa de que esta sólo sea entregada al titular del servicio, ya que sólo este tiene la facultad y la soberanía sobre sus datos personales.

En cuanto al uso de cookies que utilizan muchos sitios webs las direcciones IP que la compañía asigna a sus usuarios se distingue. Los usuarios del segmento masivo que consumen los productos hogar tienen IP dinámicas. Cuando se trata de un cliente empresa, donde se requiere un volumen de conexiones de datos mucho mayor, donde hay por ejemplo un servicio de enlace, internet dedicado o servicio de VPN, estos servicios requieren de conexiones IPs fijas.

x Hallazgos en el análisis de caso ISP chilenas

Remisiones abiertas a condiciones contractuales que pueden ser modificadas unilateralmente

Ambas ISP, en sus contratos de suscripción al servicio, remiten y complementan el mismo, con información extracontractual disponible en el sitio web de la compañía. Lo anterior sin anexar el documento al contrato mismo, sin hacer una referencia específica al documento que pretende complementar el contrato, y sin una fecha cierta o enlace específico de remisión. Esta situación atenta contra intangibilidad del contrato, ya que si se admite el enlace de remisión como parte del contrato, significaría que existen condiciones del mismo que podrían modificarse unilateralmente y sin conocimiento ni consentimiento del suscriptor. Al tratarse de un contrato de adhesión a servicios, este tipo de cláusulas pueden merecen la calificación de cláusula abusiva en virtud del artículo 16 de la ley 19.496.

Asimismo, al faltar en el mismo contrato información importante en la contratación del servicio y al no ser válida esta remisión al material que está en la página web, se estaría faltando al artículo 3

de la misma ley por infringir el deber de información de información básica sobre las condiciones y uso del servicio o producto.

En esta materia la doctrina está conteste en que lo firmado por los contratantes es ley para las mismas, y que sólo podría ser objeto de modificación en cuanto ambas consientan en ello. Rodrigo Momberg (2013) señala que “[e]l principio de la fuerza obligatoria del contrato o pacta sunt servanda es uno de los pilares básicos del derecho de contratos, reconocido por la mayoría de los ordenamientos jurídicos y consagrado positivamente tanto en las codificaciones decimonónicas como en las contemporáneas. Dicho principio, lo mismo que los principios de libertad contractual y del efecto relativo de los contratos, se considera el corolario necesario del dogma de la autonomía de la voluntad”.⁵⁸ En el paradigma de contratos tradicionales donde ambas partes tienen una fuerza negociadora equivalente, sin embargo en contratos de adhesión, como es la situación del presente estudio, donde una parte simplemente acepta o rechaza las condiciones de contrato que una parte le impone a la otra, la intangibilidad del contrato toma una relevancia crítica, pues no puede el derecho dejar en la desprotección a quien ya se encuentra en una situación desmejorada a la hora de negociar y contratar.

Así la sola posibilidad de que estas condiciones puedan ser modificadas unilateralmente en el sitio web de la empresa, sin que la otra parte obligada al contrato siquiera pueda percatarse, constituye en sí misma una falta grave.

En opinión de Iñigo de la Maza la existencia de estas cláusulas abusivas se explicarían principalmente a razón de una falla de mercado basada en las denominadas "asimetrías informativas"⁵⁹, pues el consumidor difícilmente entenderá en la revisión de un contrato de adhesión. Si es que se encuentra frente a una cláusula que lo pone en una situación de desmedro, y si es que llega a notarlo, la persona que oferta el contrato no tiene tampoco la capacidad de negociar los términos del mismo.

De este modo, las cláusulas en ambos contratos se enmarcan dentro de la la legislación define como “cláusulas abusivas”. Estas son definidas por la letra a) del artículo 16 de la Ley Protección y Derechos del Consumidor como aquellas “otorguen a una de las partes la facultad de dejar sin efecto o modificar a su solo arbitrio el contrato(...)”. El remedio establecido por la legislación para este tipo de cláusulas es tenerlas como no escritas para todos los efectos legales. Como ha señalado la doctrina, “[e]l catálogo contenido en el artículo 16 de la ley 19.496 constituye una “lista negra” es decir, advertida la existencia de una de estas cláusulas en un contrato por adhesión que satisfaga las condiciones de aplicación de la ley, el juez debe necesariamente declarar su ineficacia”.⁶⁰

Este beneficio para el consumidor implica que la relación contractual puede continuar en ausencia

⁵⁸ MOMBERG, Rodrigo (2013): “El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato”, cita MJD1001, consultado 15 de noviembre 2016.

⁵⁹ DE LA MAZA, Iñigo (2004): “El control de las cláusulas abusivas y la letra g)” disponible en: http://works.bepress.com/inigo_de_la_maza/16/, consultado 12 de noviembre 2016.

⁶⁰ DE LA MAZA, Iñigo (2004)

de la eficacia de la cláusula, en otras palabras *“En cuanto a los efectos de la incorporación de cláusulas abusivas, se dispone que no vincularán al consumidor y, si resulta posible, el contrato seguirá subsistiendo sin éstas”*.⁶¹ Sin embargo, resulta problemática dicha solución en el caso particular, pues significaría dejar sin términos y condiciones de tratamiento de datos personales a los contratos involucrados.

Entrega de información privada sin mediar orden judicial

Ambas ISP refirieron en sus entrevistas que las compañías comprendían dentro del concepto de comunicación privada los metadatos de servicios de Internet móvil y hogar, así también los de telefonía fija o móvil, y con ello el contenido de las mismas.

Al ser consultadas por los protocolos que seguían respecto de los requerimientos de comunicación privada de sus clientes, ambas compañías hicieron la distinción de cuando estas eran requeridas a través de orden judicial, y de cuando estas eran requeridas por el Ministerio Público, personalmente por el Fiscal, o a través de la policía teniendo como uno requisito que la solicitud se enmarcara en la investigación de un crimen o delito.

Ante esto cabe hacer algunas precisiones, lo que evidenciaría que, las mencionadas compañías no estarían cumpliendo con estándares adecuados a la hora de entregar información solicitada por la autoridad sin exigir la entrega de la orden judicial que ordene la realización de diligencias que puedan vulnerar derechos garantizados en la Constitución y en los distintos tratados internacional ratificados por Chile.

En este sentido la Constitución Política de la República delega en el legislador la facultad de señalar cuáles serán las circunstancias en que el hogar pueda allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse. De esta forma, y en virtud del artículo 9 del Código Procesal Penal de Chile, podemos decir que el legislador ha seguido la tendencia internacional que se encuentra en armonía con los Derechos Humanos, esto es la inexcusable exigencia de una sentencia u orden judicial que autorice violentar esas garantías fundamentales, la que deberá expresar específicamente qué es aquello que se debe interceptar, el plazo para realizar las acciones, la finalidad y necesidad de ellas, etc.

Es decir, si bien en el sistema Procesal Penal chileno se establecen para el Ministerio Público y en específico para el fiscal, las facultades de perseguir e iniciar investigaciones con su sola iniciativa, así como es obligación de las policías alertar al órgano persecutor cuando alguna actividad presumible de delito se les aparezca, lo cierto es que estas facultades tienen como límite el requerir la autorización del Juez de Garantía cuando tales actividades investigativas pongan en riesgo alguno de los derechos fundamentales consagrados en la Constitución

⁶¹ Ibíd

En consecuencia, cuando una diligencia de investigación pudiere producir alguno de tales efectos, el fiscal deberá solicitar previamente autorización al juez de garantía. Tratándose de casos urgentes, en que la inmediata autorización u orden judicial sea indispensable para el éxito de la diligencia, podrá ser solicitada y otorgada por cualquier medio idóneo al efecto, tales como teléfono, fax, correo electrónico u otro, sin perjuicio de la constancia posterior, en el registro correspondiente. No obstante lo anterior, en caso de una detención se deberá entregar por el funcionario policial que la practique una constancia de aquélla, con indicación del tribunal que la expidió, del delito que le sirve de fundamento y de la hora en que se emitió”. Vale la pena mencionar que dichas garantías son irrenunciables, y por tanto no pueden ser modificadas a través de cláusulas contractuales”.⁶²

En atención a lo anterior, resulta sumamente preocupante que dos de los mayores ISP del país no establezcan como requisito ineludible la presentación de una autorización judicial que ordene la entrega de la información de sus clientes, y no al simple requerimiento de la autoridad, sino exigiendo como requisitos copulativos que el requerimiento sea presentado por autoridad facultada por la ley y en virtud de una orden judicial.

xi Conclusiones

Respecto al Mercado de los proveedores de Internet, un análisis de esta muestra que si bien Chile muestra altas cifras en lo relativo al porcentaje de población con acceso a Internet en sus hogares, el mercado muestra altos niveles de concentración económica, con un número reducido de oferentes concentrando la gran mayoría de los clientes.

Respecto del caso de estudio, el análisis de los contratos, términos y condiciones públicas y entrevistas a ejecutivos de dos de los principales ISP de Chile entrega resultados preocupantes. Por un lado es posible constatar que la información respecto de las condiciones de contratación y otra información relevante no siempre está disponible de forma clara y simple en los sitios de las empresas proveedoras de Internet. Por otro lado, detectamos cláusulas relativas al tratamiento de datos personales en los contratos de suministro de Internet que hace remisiones abiertas a términos y condiciones alojados en el sitio web de las empresas, las que corren el riesgo de ser modificadas unilateralmente.

Por último, resulta sumamente preocupante que dichas empresas hagan entrega de información de carácter personal relativa a sus clientes a las policías o entes de persecución policial sin mediar una orden judicial previa.

Todas las falencias antes descritas no solo deben ser abordadas por las empresas a través de la autoregulación, sino que es necesario que el Estado tome un rol activo, tanto en la fiscalización del cumplimiento de la legislación vigente, como en la regulación del sector. Dicha regulación debería

⁶² ISLAS, Alfredo (2008): “Intervención en las comunicaciones telefónicas y derechos fundamentales”. Disponible en (PDF): <http://bit.ly/2kQm6DN>

ser diseñada e implementada de forma multisectorial, teniendo en consideración las posturas del sector privado, pero también de la sociedad civil y los consumidores.

V México⁶³

R3D ha contactó diversas empresas de telecomunicaciones en México para formular una serie de preguntas relacionadas con la protección de datos de sus usuarios.

Telcel (América Móvil)

Telcel es el mayor proveedor de telefonía móvil en México. R3D sostuvo una teleconferencia con Daphne Glusman Gerbilsky, Gerente Jurídico y Paula García Sabido, Gerente de Relaciones Institucionales el 14 de Abril de 2016. En dicha conversación se acordó el envío del cuestionario el cual fue enviado días después. El 11 de agosto se reenvió el cuestionario. Existieron múltiples llamadas telefónicas entre los meses de agosto y octubre para insistir sobre los cuestionarios. Las últimas llamadas fueron realizadas el 27 de septiembre el 2 de octubre y el 3 de noviembre de 2016.

AT&T

AT&T es una de las mayores compañías de telefonía en el mundo. Recientemente ingresó al mercado mexicano. R3D tuvo una reunión con Daniel Ríos Villa el 19 de Abril de 2016. Como producto de la conversación se acordó mantener la comunicación y el envío del cuestionario. El 13 de julio, Daniel Ríos recibió vía correo electrónico el cuestionario nuevamente, sin embargo no hubo respuesta. El 11 de agosto hubo confirmación de que habría respuesta al cuestionario. El 2 de septiembre existió una nueva reunión con Daniel Ríos. Existieron contactos posteriores los días 27 de Septiembre, 2 de Octubre y 13 de Octubre sin que el cuestionario haya sido enviado. También existió una reunión con Jimena Gómez, Directora de Asuntos Públicos de AT&T, el 26 de Septiembre, en la cual se recordó sobre el cuestionario pendiente, sin embargo no hubo respuesta.

Telefónica Movistar

Telefónica es una de las empresas telefónicas más importantes en América Latina. R3D sostuvo una reunión con Pablo Barrionuevo el 18 de agosto de 2016. El 2 de octubre fue enviado un correo fijando una fecha límite para el envío de las respuestas al cuestionario, sin embargo no hubo respuesta a pesar de diversos recordatorios.

⁶³ El presente capítulo fue realizado por el equipo de la **Red en Defensa de los Derechos Digitales (R3D)**, México.

i Evaluación de proveedoras de servicios de telecomunicaciones

1. ¿La empresa posee una política de protección de los datos personales de sus clientes? Si la respuesta es afirmativa, ¿está publicada dicha política de protección de datos? ¿Dónde? ¿Cómo se accede a su política de protección de datos? ¿Con qué frecuencia modifica y/o actualiza su política de protección de datos? ¿Nos puede suministrar una copia de su política de protección de datos?

Telcel: cuenta con un “Aviso de Privacidad”, que se encuentra disponible en: <http://www.telcel.com/aviso-de-privacidad>. En dicha política está incluida una política de protección de datos. En la parte superior de dicho aviso está indicada la versión y la fecha de última actualización de la misma.

AT&T: cuenta con un “Aviso de Privacidad” que se encuentra disponible en: <https://www.att.com.mx/documentos/aviso-de-privacidad-integral-att.pdf>. En dicha política está incluida una política de protección de datos. En la parte superior de dicho documento se especifica la última fecha de actualización, y la empresa recomienda que es el usuario quien debe estar al tanto de los cambios entrando periódicamente a visitar el enlace que la contiene.

Telefónica: cuenta con un “Aviso de Privacidad Integral” que se encuentra disponible en: <http://www.telefonica.com.mx/aviso-de-privacidad>. En la parte inferior de dicho aviso está indicada la versión y la fecha de última actualización del mismo. Además, Telefónica cuenta con una certificación en materia de protección de datos personales, otorgada por Normalización y Certificación Electrónica, S.C en materia de datos personales.

2. ¿Elabora informes de transparencia? En caso afirmativo, ¿qué información incluye en tales informes? ¿Son de acceso público? ¿Cómo se accede a ellos? ¿Con qué frecuencia los elabora? En caso que la respuesta fuera negativa, ¿Por qué no los elabora?

Telcel: No se encontraron informes de transparencia públicos. R3D le solicitó a la empresa en agosto de 2016 dichos informes y a noviembre de 2016 no los ha enviado.

AT&T: No se encontraron informes de transparencia públicos. R3D le solicitó a la empresa en agosto de 2016 dichos informes y a noviembre de 2016 no los ha enviado.

Telefónica: No se encontraron informes de transparencia públicos. R3D le solicitó a la empresa en agosto de 2016 dichos informes y a noviembre de 2016 no los ha enviado.

3. ¿El poder judicial o algún tribunal de su país le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

Telcel: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas

autoridades. Telcel no posee un protocolo público respecto de la manera en que da cumplimiento a dichas solicitudes. En particular no existe una política pública que indique que éstas solicitudes únicamente son cumplidas con autorización judicial.

AT&T: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas autoridades. AT&T especifica en su apartado “Colaboración con las autoridades Mexicanas en Materia de Seguridad y Justicia” disponible en <https://www.att.com.mx/documentos/procedimiento-att.pdf> las condiciones en las que podrá entregar datos a las mismas citando los datos del área responsable de ello, la dirección para recibir documentación física y cuenta con un apartado referente al “Procedimiento de Atención de Órdenes de Intercepción de Comunicaciones”. Sin embargo, AT&T no posee un protocolo público respecto de la manera en que da cumplimiento a dichas solicitudes. En particular no existe una política pública que indique que éstas solicitudes únicamente son cumplidas con autorización judicial.

Telefónica: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas autoridades. Telefónica explica en el apartado de su sitio “Requerimientos Autoridad” disponible en <http://www.movistar.com.mx/requerimientos-autoridad> que se apeg a los Lineamientos de Colaboración en Materia de Seguridad y Justicia para la entrega de datos, pero no especifica por cuenta propia como lo hace ni si dichas solicitudes únicamente son cumplidas con autorización judicial.

4. Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

5. ¿Algún organismo o repartición estatal le ha solicitado información de sus usuarios? En caso afirmativo, ¿qué tipo de información se le solicitó? ¿Cómo se formalizó la petición? ¿Tiene su empresa protocolos de actuación o alguna política establecida para este tipo de solicitudes? En caso afirmativo, ¿puede entregar una copia del protocolo? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo? ¿Es de público acceso?

Telcel: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas autoridades. Telcel no posee un protocolo público respecto de la manera en que da cumplimiento a dichas solicitudes. En particular no existe una política pública que indique que éstas solicitudes únicamente son cumplidas con autorización judicial.

AT&T: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas autoridades. AT&T especifica en su apartado “Colaboración con las autoridades Mexicanas en Materia de Seguridad y Justicia” disponible en <https://www.att.com.mx/documentos/procedimiento-att.pdf> las condiciones en las que podrá entregar datos a las mismas citando los datos del área responsable de ello, la dirección para recibir documentación física y cuenta con un apartado referente al “Procedimiento de Atención de Órdenes de Intercepción de Comunicaciones”. Sin embargo, AT&T no posee un protocolo público respecto de la manera en que da cumplimiento a dichas solicitudes. En particular no existe una política pública que indique que éstas solicitudes únicamente son cumplidas con autorización judicial.

Telefónica: Sí. Se ha documentado que se han recibido solicitudes de datos de usuarios, incluyendo metadatos de comunicaciones y datos de localización geográfica en tiempo real, por parte de diversas autoridades. Telefónica explica en el apartado de su sitio “Requerimientos Autoridad” disponible en <http://www.movistar.com.mx/requerimientos-autoridad> que se apeg a los Lineamientos de Colaboración en Materia de Seguridad y Justicia para la entrega de datos, pero no especifica por cuenta propia como lo hace ni si dichas solicitudes únicamente son cumplidas con autorización judicial.

6. Si no tiene protocolos de actuación o política interna para el caso mencionado en el punto anterior, ¿qué criterios sigue para la entrega de información? ¿Informa a sus usuarios en caso de solicitud de información? ¿Informa a sus usuarios en caso de entrega de información?

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

7. ¿Cuenta la empresa con protocolos o políticas de procedimiento interno para el filtrado, retiro o bloqueo de contenido? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

8. En caso de no contar con un protocolo o política de procedimiento para el filtrado, retiro o bloqueo de contenido, ¿cuál es la razón? ¿Qué criterios utiliza para el filtrado, retiro o bloqueo de contenido? ¿Informa al usuario y/o titular del contenido del potencial filtrado, retiro o bloqueo del contenido, en forma previa a efectuarlo? ¿Informa al usuario y/o titular del contenido del filtrado, retiro o bloqueo del contenido, en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de

acuerdo con el filtrado, retiro o bloqueo del contenido? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del contenido acerca de este procedimiento?

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

9. ¿Cuenta la empresa con protocolos o políticas de procedimiento interno para cancelación y/o suspensión del servicio? En caso afirmativo ¿puede entregar una copia del protocolo o política? ¿Con qué frecuencia modifica y/o actualiza dicho protocolo o política? ¿Es de público acceso?

Telcel: en los **Términos y Condiciones** y en el **Código de Prácticas Comerciales** de la empresas se especifican las condiciones de cancelación y suspensión del servicio. Asimismo, la empresa cita en su sitio web la “Carta de los derechos de los usuarios”, promovida por el acuerdo DOF: 06/07/2015 entre la Profeco y el IFT.

AT&T: en los **Términos y Condiciones** de la empresa se especifican las condiciones de cancelación y suspensión del servicio. En la **Política de uso** de la empresa se detalla cuales son los usos específicos de los equipos y algunas causas de suspensión o cancelación del servicio. Asimismo la empresa cita en su sitio web la “Carta de los derechos de los usuarios”, promovida por el acuerdo DOF: 06/07/2015 entre la Profeco y el IFT.

Telefónica: La empresa explica en su **Código de Prácticas Móvil** las condiciones de contratación y cancelación de sus servicios. Asimismo la empresa cita en su sitio web la “Carta de los derechos de los usuarios”, promovida por el IFT.

10. En caso de no contar con un protocolo o política de procedimiento para la cancelación y/o suspensión del servicio, ¿cuál es la razón? ¿Qué criterios utiliza para la cancelación y/o suspensión del servicio? ¿Informa al usuario de la potencial cancelación y/o suspensión del servicio en forma previa a efectuarlo? ¿Informa al usuario de la cancelación y/o suspensión del servicio en forma posterior a efectuarlo? ¿Puede el usuario y/o titular del contenido manifestarse en forma previa y/o ejercer algún tipo de defensa en caso de no estar de acuerdo con la cancelación y/o suspensión del servicio? ¿Cuál es el procedimiento previsto? ¿Cómo conoce el usuario y/o titular del servicio acerca de este procedimiento?

Telcel: En los documentos anteriormente mencionados no se describen recursos previos de notificación o defensa ante cancelaciones o suspensiones. Tampoco hay descripciones proporcionadas a la contratación sobre suspensiones y/o cancelaciones de los servicios de la empresa.

AT&T: En los documentos anteriormente mencionados no se describen recursos previos de notificación o defensa ante cancelaciones o suspensiones. Tampoco hay descripciones proporcionadas a la contratación sobre suspensiones y/o cancelaciones de los servicios de la empresa.

Telefónica: En los documentos anteriormente mencionados no se describen recursos previos de notificación o defensa ante cancelaciones o suspensiones. Tampoco hay descripciones proporcionadas a la contratación sobre suspensiones y/o cancelaciones de los servicios de la empresa.

11. ¿Tiene su empresa bases de datos inscriptas en algún registro nacional o provincial (estatal) o departamental (municipal)? ¿Existe algún tipo de regulación normativa o legal?

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

12. ¿La empresa comercializa o cede los datos personales de sus clientes a otras empresas? En caso afirmativo, ¿sigue algún procedimiento determinado para la comercialización o cesión? ¿Comunica esta situación a sus clientes en forma previa o posterior?

Telcel: La empresa especifica que podrá ceder o transferir los datos personales con fines comerciales o judiciales. “Telcel podrá transferir, sin requerir de su consentimiento, los datos personales necesarios a autoridades competentes en los casos legalmente previstos; a terceros tanto nacionales como extranjeros, intervinientes en la prestación de los servicios solicitados por usted; así como aquellas empresas afiliadas y/o subsidiarias de Telcel para que éstas le puedan contactar, directa o indirectamente, para llevar a cabo actividades de promoción y/u ofrecimiento de productos y/o servicios que dichas subsidiarias y/o afiliadas de Telcel pueden comercializar y/o prestar de manera conjunta con Telcel o de manera independiente”.

AT&T: AT&T especifica con detalle las causas, circunstancias y procedimientos por los cuales podría transferir datos a terceros, especificando condiciones primarias y secundarias, incluidos fines comerciales.

Telefónica: Telefónica especifica con detalle las causas, circunstancias y procedimientos por los cuales podría transferir datos a terceros, especificando condiciones primarias y secundarias, incluidos fines comerciales.

13. ¿Cuáles son las medidas de seguridad adoptadas para proteger la seguridad y confidencialidad de los datos personales de sus clientes? ¿Estas medidas son de público conocimiento? ¿Son de conocimiento de sus clientes? ¿Con qué frecuencia son estas medidas revisadas o actualizadas? ¿Se notifica la revisión o actualización de medidas a sus clientes? ¿En forma previa o posterior?

Telcel: La empresa especifica en su Aviso de privacidad que cuenta con “políticas de privacidad vigentes” y el Código de Prácticas Comerciales especifica que la empresa es la responsable de su protección, pero no se indica bajo qué estándares.

AT&T: La empresa no especifica información al respecto de manera pública.

Telefónica: La empresa aclara en su Aviso de Privacidad Integral que “los datos personales recolectados se encontrarán protegidos por medidas de seguridad administrativas, técnicas y físicas adecuadas contra el daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizados, de conformidad con lo dispuesto en la LFPDP y la demás legislación aplicable”. Pero inmediatamente hace un ejercicio de deslinde, a la letra “no obstante lo señalado anteriormente, Telefónica no garantiza que terceros no autorizados no puedan tener acceso a los sistemas físicos o lógicos de los Titulares o del Responsable o en los documentos electrónicos y archivos almacenados en sus sistemas. En consecuencia, Telefónica no será en ningún caso responsable de los daños y perjuicios que pudieran derivarse de dicho acceso no autorizado.”

14. ¿Existe en su país alguna normativa protectoria de datos personales? ¿Informa a sus clientes de los derechos que gozan de acuerdo a la ley de protección de datos personales? ¿Cómo?

Telcel: La empresa menciona la Ley Federal de Protección de Datos Personales en Posesión de los Particulares como normativa regulatoria.

AT&T: La empresa menciona en su Aviso de privacidad la normativa, “ Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento”.

Telefónica: La empresa menciona la Ley Federal de Protección de Datos Personales en Posesión de los Particulares como normativa regulatoria.

15. ¿Qué tipo de medidas toma para que el consentimiento necesario para el tratamiento de datos personales sea libre, expreso e informado?

Telcel: El consentimiento se obtiene mediante la puesta a disposición del aviso de privacidad.

AT&T: El consentimiento se obtiene mediante la puesta a disposición del aviso de privacidad.

Telefónica: El consentimiento se obtiene mediante la puesta a disposición del aviso de privacidad.

16. ¿Tienen un procedimiento para que los usuarios puedan ejercer los derechos de acceso, rectificación y supresión de sus datos?

Telcel: En el “Aviso de privacidad” de la empresa se menciona como pueden ejercerse los derechos ARCO (acceso, rectificación, cancelación u oposición).

AT&T: En el “Aviso de privacidad” de la empresa se menciona como pueden ejercerse los derechos ARCO (acceso, rectificación, cancelación u oposición).

Telefónica: En el “Aviso de Privacidad Integral” de la empresa se menciona como pueden ejercerse los derechos ARCO (acceso, rectificación, cancelación u oposición).

17. ¿Han habido de casos de usuarios/as que han solicitado sus registros de datos personales? ¿Cuál fue la respuesta de la empresa?

Telcel: R3D solicitó el acceso a los metadatos de comunicaciones conservados por la empresa. La empresa negó el acceso a dichos datos. Después de la interposición de un recurso de protección de

derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), dicho Instituto ordenó la entrega de los datos. La resolución aún se encuentra pendiente de cumplimiento.

AT&T: R3D solicitó el acceso a los metadatos de comunicaciones conservados por la empresa. La empresa negó el acceso a dichos datos. Después de la interposición de un recurso de protección de derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), dicho Instituto ordenó la entrega de los datos. La resolución aún se encuentra pendiente de cumplimiento.

Telefónica: R3D solicitó el acceso a los metadatos de comunicaciones conservados por la empresa. La empresa negó el acceso a dichos datos. Después de la interposición de un recurso de protección de derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), aún se encuentra pendiente la resolución, aunque se prevé una resolución similar a otros precedentes generados por R3D.

18. Teniendo en cuenta el uso de cookies que utilizan muchos sitios webs ¿Qué tipo de direcciones IP les asignan a sus usuarios? (las opciones son dinámicas o fijas)

Telcel: No existe información públicamente disponible.

AT&T: No existe información públicamente disponible.

Telefónica: No existe información públicamente disponible.

VI Hallazgos principales. Conclusiones y recomendaciones finales

La lectura de cada uno de los casos de estudio permite detectar determinadas tendencias en los países en análisis, que nos permiten inferir las mismas tendencias en la región. A saber:

- ◆ Por lo general hay falta de información relativa al uso y tratamiento de los datos personales. Y cuando lo hay, consiste en remisiones generales a las leyes vigentes o está compartida de modo poco amigable para el usuario.
- ◆ No se incluyen opciones o procedimientos de fácil uso (formularios en el sitio web, por ejemplo) para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, aunque sí hay variadas opciones y procedimientos de muy fácil uso para la adquisición de productos o servicios.

- ◆ La publicación de informes de transparencia como práctica para informar al público en general, mediante la provisión de datos cuantitativos y cualitativos, acerca de, por ejemplo, qué cantidad de usuarios han solicitado acceder a sus datos; si las solicitudes de los usuarios fueron admitidas o denegadas y por qué motivos, o si hay recibido y en qué cantidad solicitudes de entrega de información por parte de autoridades administrativas o judiciales, cuál la respuesta brindada a dichas solicitudes y los motivos de la misma, etc., no se encuentra implementada en la región. Aunque sí pueden encontrarse informes de transparencia (o de sustentabilidad) para brindar información financiera y presupuestaria.
- ◆ Las compañías no informan a sus usuarios cuando revelen su información personal ante requerimiento de autoridades administrativas o judiciales y tampoco parecen tener protocolos de actuación para estos casos, aunque sí se estima que al menos las grandes empresas cuentan con equipos legales internos para atender estos requerimientos.
- ◆ En muchos casos, las empresas entregan información sin mediar orden judicial.
- ◆ Tampoco cuentan con protocolos públicos relativos al filtrado, bloqueo o retiro de contenidos, con excepción de la mención de alguna causal en particular (por ejemplo, pornografía infantil).
- ◆ Sí se destaca que las empresas de empresas suelen contar con la certificación ISO 27001 de seguridad de la información.
- ◆ Las empresas no tienen como práctica informar a sus clientes en caso de vulneración de la información.
- ◆ Las modificaciones en los términos y condiciones y políticas de privacidad suele realizarse cuando la empresa lo estima conveniente y sin dar aviso al cliente. Es decir, no suele haber procedimientos de actualización o revisión previamente establecidos.
- ◆ En el caso de las compañías que son parte de firmas multinacionales, suelen seguir lineamientos y prácticas establecidas por sus casas matrices.
- ◆ Por lo general, la empresas no cuentan con información pública en relación a su política de cookies.
- ◆ En Argentina y México, países que cuentan con leyes de protección de datos personales que aplican al sector privado, las empresas que se avinieron a responder el cuestionario han manifestado dar cumplimiento a los recaudos previstos en la normativa. Esto no aplica al caso de Chile que, si bien cuenta con una ley de protección de datos personales, deja al sector privado en discrecionalidad plena para estar a su cumplimiento o no.

Las tendencias reseñadas previamente permiten concluir que, en general, hay todavía un largo camino por recorrer para el desarrollo e implementación de buenas prácticas empresariales, respetuosas de derechos de los usuarios, en particular en relación a la adecuada protección de los datos personales.

De tal suerte también, se efectúan las siguientes propuestas que, como ya se mencionó en la introducción, no intentan ser un posicionamiento acabado, sino un disparador de propuestas básicas para próximos diálogos multisectoriales.

Publicidad: Las empresas deberían publicar reportes de transparencia, en los cuales den cuenta de la forma en que realizan el tratamiento de los datos de las personas incluidas en sus bases. Este informe debería incluir -entre otros- el modo en que la empresa comparte sus datos personales con otros actores, tanto del sector público como del sector privado.

Información clara y accesible: Las personas deben poder saber con detalle la forma en que las empresas van a realizar el tratamiento de sus datos. Por lo tanto, éstas deberían difundir sus políticas de privacidad en un lugar de fácil acceso. En este sentido, la colocación al pie de página de los sitios web mediante una leyenda que las identifique claramente resulta un paso necesario pero no suficiente, ya que debe ser complementada con información que amplíe y especifique las operaciones que la empresa lleva a cabo con los datos de las personas. Por lo tanto, no se ajusta al deber de información que las políticas difundidas solo se limiten a repetir lo que dicen las leyes vigentes.

Comunicación a los usuarios: Las empresas deberían notificar a los usuarios de manera inmediata las situaciones que puedan afectar de manera intensa la protección de sus datos personales. Dentro de estas situaciones, la necesidad de informar acerca de solicitudes de información de datos por parte de las autoridades y sobre la existencia de prácticas de retención de datos se vuelve imprescindible, debido a los riesgos que estas conductas plantean al ejercicio de determinados derechos y garantías, como la intimidad o el debido proceso. Resulta deseable que las empresas no entreguen datos sin mediar una orden judicial o expresa obligación legal.

Términos y condiciones que respeten la dignidad de las personas: El manejo que las empresas realizan de los datos personales de sus usuarios suele estar contemplado en los famosos « términos y condiciones » que cada persona debe aceptar antes de poder contratar un servicio. Al estar compuestos de largas y engorrosas páginas con letra chica y lenguaje técnico, se vuelve muy difícil acceder a la política de privacidad contenida en ellos. Por lo tanto, las empresas deberían implementar documentos que de manera sencilla y mediante un lenguaje accesible, cumplan con el deber de informar de manera clara y detallada a los usuarios acerca de las políticas que tal empresa llevará a cabo con sus datos y evitar modificaciones unilaterales sin conocimiento de los usuarios.

Mayor apertura a la sociedad civil: Al ser actores privados, las empresas suelen estar fuera del alcance de ciertas obligaciones que le atañen al sector público, como el deber de brindar información reconocido por las leyes de acceso a la información pública. Por lo tanto y como parte de un proceso de transparencia, las empresas deberían ser más receptivas a los pedidos de organizaciones de la sociedad civil que buscan conocer sus prácticas de tratamiento de datos. Esto implicaría la respuesta positiva a los pedidos de información, la disposición a participar en entrevistas o mesas de trabajo y cualquier otro comportamiento que implique la voluntad de las empresas a involucrarse en un diálogo inclusivo con todos los sectores interesados en la protección de los datos personales.

