¿QUIÉN DEFIENDE TUS DATOS?

CHILE
2018

PABLO VIOLLIER

@ DERECHOS DIGITALES
América Latina

EFF
ELECTRONIC FRONTIER FOUNDATION

¿QUIÉN DEFIENDE TUS DATOS?

DERECHOS DIGITALES
América Latina

ELECTRONIC FRONTIER FOUNDATION

Portada y diagramación: Constanza Figueroa.
Edición y correcciones: Juliana Guerra.
Mayo 2018.
Este informe fue realizado por Derechos Digitales, con el apoyo de EFF

DERECHOS DIGITALES
América Latina

ELECTRONIC FRONTIER FOUNDATION

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

Contenido

1. Introducción: ¿*Quién defiende tus datos?*

El presente documento corresponde a la segunda entrega del informe anual **¿Quién defiende tus datos?**, una evaluación sobre las políticas de privacidad y protección de datos de las empresas que proveen servicios de internet a sus clientes. El énfasis está puesto en evaluar hasta qué punto las empresas defienden los datos personales de sus usuarios, sea ante las solicitudes de la autoridad gubernamental como frente al tratamiento indebido que terceros pretendan hacer de los datos personales de los usuarios. Para ello, y como forma de continuar el seguimiento de la evaluación realizada en 2017,[1] nos proponemos responder las siguientes preguntas: ¿cuáles son las empresas que tienen las políticas de privacidad y protección de datos más transparentes al respecto? ¿Existen procedimientos claros en estos casos? ¿Notifican a sus usuarios de los requerimientos de información realizados por la autoridad?

La principal novedad en relación al informe publicado el año anterior, es la incorporación de la empresa WOM a la medición. Esta adición se realizó en razón de la importante penetración de mercado que WOM ha alcanzado en el segmento móvil, así que las empresas objeto de este estudio cubren el 95,8 % de las conexiones de internet fija y 98,5 % de las conexiones de internet móvil del país.

Después del informe de 2017, la situación nacional estuvo marcada por polémicas públicas vinculadas con la privacidad de los usuarios. En agosto de 2017, distintos medios de comunicación dieron a conocer que el gobierno preparaba la aprobación de un decreto para extender, de uno a dos años, la obligación legal de retención de distintos datos de comunicaciones[2] (o metadatos) por parte de las empresas, y que se almacenarían datos distintos a los exigidos en el artículo 222 del Código Procesal Penal. El denominado "decreto espía" finalmente no fue promulgado, ya que la Contraloría General de la República representó su constitucionalidad en el proceso de toma de razón, después de recibir una serie de solicitudes formales presentadas por distintas organizaciones de la sociedad civil solicitando su rechazo.[3]

1 *Disponible en: https://www.derechosdigitales.org/wp-content/uploads/qdtd-2017.pdf*

2 *BioBio (2017) "Gobierno firma decreto para guardar datos de tus llamadas, internet y mensajes por 2 años". Disponible en: http://www.biobiochile.cl/noticias/nacional/chile/2017/08/25/gobierno-firma-decreto-para-guardar-datos-de-tus-llamadas-internet-y-mensajes-por-2-anos.shtml*

3 *Cooperativa (2017). "Contraloría dejó sin piso al "decreto espía" de Aleuy". Disponible en: http://www.cooperativa.cl/noticias/tecnologia/internet/seguridad/contraloria-dejo-sin-piso-al-decreto-espia-de-aleuy/2017-11-28/154119.html*

Otra gran polémica se produjo en septiembre de 2017, cuando a propósito de la detención de ocho comuneros mapuches,[4] salió a la luz que la prueba utilizada para su detención consistía en mensajes de servicios de mensajería como WhatsApp y Telegram, los que por su sistema de cifrado no deberían haber podido ser obtenidos por las fuerzas del orden. En una trama que todavía no alcanza su desenlace definitivo, el Ministerio Público acusó formalmente a la Unidad de Inteligencia de Carabineros de falsificar esta prueba. Del mismo modo, se reveló que el supuesto sistema para interceptar los mensajes de estas aplicaciones dependía de que la víctima instalara un malware enviado por Carabineros a través de un sistema de *phishing* bajo una serie de condiciones improbables. Adicionalmente, se descubrió un oscuro entramado de escuchas ilegales por parte de la misma policía.[5]

Si bien las empresas de telecomunicaciones han jugado un rol secundario en estas dos historias, la confianza de la población respecto del nivel de resguardo de sus comunicaciones privadas y datos personales se ha visto afectada. Por lo mismo, es necesario que existan mecanismos de medición relativos al nivel de resguardo que estas empresas ofrecen a sus usuarios.

Para continuar con ese trabajo de evaluación, hemos mantenido en sus aspectos sustantivos la metodología utilizada en 2017. Más bien se han establecido pequeños ajustes con miras a realizar una medición más precisa. Con lo anterior, este informe puede compararse en líneas generales con su correspondiente de 2017, pues mide el estado de avance de las empresas a partir de los mismos indicadores. Al igual que en el informe anterior, no se analizará el cumplimiento de la legislación vigente, que constituye una obligación ineludible y un piso mínimo desde el cual las empresas deben operar. El foco estará en qué empresas van más allá del mínimo legal al momento de proteger a sus usuarios. Así, esperamos que este informe se transforme en una guía efectiva para que el usuario pueda tomar una decisión informada al momento de elegir una compañía de telecomunicaciones.

¿Quién Defiende Tus Datos? es parte de una serie de estudios similares realizados en América Latina, basados en **Who Has Your Back?**, un reporte anual publicado por la Electronic Frontier Foundation (EFF) en Estados Unidos, cuya metodología se adapta a la realidad nacional desde el punto de vista jurídico y de mercado. Este informe analiza las políticas de privacidad y los códigos de prácticas disponibles al público de las empresas proveedoras de

4 *C13 (2017). "De la aparatosa detención hasta el "montaje": los hitos de la "Operación Huracán"". Disponible en: http://www.t13.cl/noticia/nacional/de-aparatosa-detencion-montaje-hitos-operacion-huracan*

5 *Ciper (2018). "Operación Huracán": la secreta casa donde se hacían centenares de escuchas telefónicas ilegales. Disponible en: http://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/*

servicios de telecomunicación más grandes de Chile: WOM, Movistar, VTR, Claro, Entel y GTD Manquehue. A continuación, explicaremos cada una de las categorías de análisis.

1) Términos y condiciones contractuales y comerciales, y políticas de protección de los datos personales de los usuarios.

En este ítem queremos saber si las empresas publican los términos que rigen las relaciones contractuales con sus usuarios. Esta categoría incluye tanto la publicación de los contratos respectivos como las políticas de datos personales que puedan orientar a los clientes sobre las actividades de tratamiento. Además analiza lo difícil que puede resultar para el usuario comprender estos documentos.

La búsqueda de estos elementos se realizó en el sitio web de cada compañía analizada. No solamente es importante determinar que los documentos se encuentren disponibles, sino también si están vinculados de alguna forma, es decir, si el contrato menciona la existencia de una política de datos. En ausencia de una política formal, será solo el contrato el que entregará nociones sobre el modo en que una compañía realiza el tratamiento de datos.

2) Informe de transparencia

Se publican periódicamente y contienen las solicitudes de datos por parte de organismos gubernamentales y judiciales. La publicación de dichos informes suele indicar una disposición de las empresas para informar sobre el alcance y la naturaleza de las solicitudes de información personal de los usuarios, y demuestran preocupación por sus clientes. Si bien las empresas no están obligadas legalmente a publicarlos, constituye una buena práctica, ya asentada a nivel internacional.

Al no tratarse de una actividad regulada, su contenido suele ser muy variable. Pueden incluir el número de solicitudes que ha recibido, el número de veces que ha rechazado estas solicitudes y los argumentos esgrimidos; el tipo de solicitudes, de dónde provienen, su propósito y el número de usuarios afectados en cada petición.

3) Notificación a los usuarios

En este ítem queremos saber si, a través de sus términos de referencia o sus políticas de privacidad, las empresas se comprometen a informar a sus clientes en caso de que exista una solicitud para acceder a sus datos, en el primer momento permitido por la ley. También sería importante saber si abogan por mejores mecanismo de notificación ante el Congreso u otros organismos reguladores.

4) Guías de cumplimiento de obligaciones legales orientadas a la autoridad

Se trata aquí de saber si la empresa proveedora cuenta con información, públicamente disponible, que describa las pautas y procedimientos que las autoridades deben seguir cuando solicitan datos de sus clientes, de acuerdo a la ley. Dicha información debe indicar los requisitos y procedimientos para una solicitud de datos, incluida la posibilidad de remover contenidos.

Esta información se buscó en el sitio web de cada empresa estudiada, incluyendo en el análisis la información contenida en las denominadas "políticas de neutralidad", que usualmente entregan indicios sobre esta materia en ausencia de otro tipo de guía o documento específico.

5) Defensa de la privacidad ante los tribunales de justicia y el poder legislativo

Aquí el objetivo es conocer si la empresa proveedora ha efectuado alguna acción públicamente conocida para desafiar el surgimiento de nuevos proyectos de ley o normas legales que pudieran afectar la privacidad, o de una estrategia de litigio ante los Tribunales de Justicia frente a solicitudes de datos que las empresas hayan estimado excesivos o desproporcionados.

Para recabar la información correspondiente a esta categoría se recurrió a los reportes de transparencia publicados por las empresas, a otra información disponible en las páginas web de cada una de ellas y a reportes de prensa.

Más adelante, en el apartado denominado Metodología, cada una de las mencionadas categorías será desarrollada mediante parámetros específicos de medición, cuyo grado de cumplimiento hará a la empresa analizada acreedora de calificaciones medidas como estrellas o porciones de estrellas. En algunos casos excepcionales y justificados, hemos asignado una puntuación mayor a la que correspondería bajo un análisis estricto, dado que una empresa se encuentra notoriamente cercana a satisfacer los indicadores fijados para un parámetro. Cuando así suceda, se dejará constancia de ello.

2. Contexto Nacional

2.1. Marco regulatorio

No han existido modificaciones legales relevantes desde la publicación de la versión 2017 de este informe. La reforma a la Ley 19.628 sobre Protección de la vida privada, con miras a contar con una nueva ley de datos personales, es el esfuerzo más ambicioso para actualizar nuestra normativa en la materia. Presentado el 13 de marzo de 2017,[6] el proyecto de ley[7] se encuentra en primer trámite constitucional, habiéndose aprobado en general en el Senado.[8] Todavía está pendiente la discusión y aprobación de algunos artículos en el Senado, así como su discusión en la Cámara de Diputados.

Desde el punto de vista normativo, existen tres áreas del sistema jurídico que son particularmente relevantes para efectos de este estudio: las reglas de protección de datos personales, la ley general de telecomunicaciones y sus decretos complementarios, y la legislación procesal penal. Sin realizar un estudio exhaustivo de tales materias, es necesario explicar brevemente cómo interactúan estos cuerpos legales para comprender el enfoque y los resultados del presente trabajo.

En Chile, la ley contempla la posibilidad de obtener información personal en la investigación de ciertos delitos, mediante mecanismos que incluyen la interceptación y registro de comunicaciones privadas. Estas disposiciones se encuentran en el Código Procesal Penal y en algunas leyes especiales que rigen, por ejemplo, en la investigación del tráfico de sustancias ilícitas y de acciones terroristas. La recolección de esta información debe ser autorizada previamente por un tribunal,[9] a solicitud del Ministerio Público, órgano a cargo de la investigación y persecución criminal. Si la recolección de información tiene fines de inteligencia, la recolección de información procede a través de las direcciones de inteligencia de las Fuerzas Armadas y de las policías.

---

6 *Carey (2017). "Proyecto de Ley que Regula la Protección de Datos Personales y Crea la Agencia de Protección de Datos Personales". Disponible en: https://www.carey.cl/proyecto-de-ley-que-regula-la-proteccion-y-el-tratamiento-de-los-datos-personales-y-crea-la-agencia-de-proteccion-de-datos-personales/ [Fecha de consulta: 3 de mayo de 2018].*

7 *Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07 [Fecha de consulta: 3 de mayo de 2018].*

8 *Senado (2018). "Creación de Agencia de Protección de Datos pasa a Sala". Disponible en: http://www.senado.cl/creacion-de-agencia-de-proteccion-de-datos-pasa-a-sala/prontus_senado/2018-03-11/093136.html [Fecha de consulta: 3 de mayo de 2018].*

9 *El artículo 9 del Código Procesal Penal establece que "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa". Nuestra interpretación es que toda interceptación de comunicaciones privadas debe contar con una autorización judicial previa para su realización.*

El inciso quinto del artículo 222 del Código Procesal Penal obliga a las empresas proveedoras de servicios de internet a mantener un registro, no inferior a un año, de los números IP de las conexiones que realicen sus clientes, además de un listado actualizado de sus rangos autorizados de direcciones IP. Debido a la polémica generada por el intento de aprobación del "decreto espía", se produjo una discusión pública respecto al término "no inferior a un año" contenido en la ley. La redacción da a entender que las empresas podían retener esta información por un tiempo superior, pero no queda claro si estarían obligadas a entregarla de ser solicitada por la autoridad, o por cuánto tiempo máximo podrían retenerse, después de ese período de un año. Por lo mismo, este informe también dará cuenta de si las empresas transparentan el período por el cual retienen estos datos comunicacionales y su forma de eliminación.

El artículo 224 del mismo cuerpo legal señala que la medida de interceptación será notificada al afectado con posterioridad a su realización, cuando el objeto de la investigación lo permitiere y en la medida en que ello no pusiere en peligro la vida o la integridad corporal de terceras persona. Dicha notificación debe ser realizada por el Ministerio Público, pero nada obsta a que las empresas notifiquen a sus usuarios de las solicitudes realizadas por el Ministerio Público u otros organismos, en la medida que se cumplan los requisitos establecidos en el artículo mencionado.

Asimismo, la normativa sectorial de telecomunicaciones incluye el Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación (Decreto 142 de 2005), que se refiere a la obligación contenida en el Código Procesal Penal para que las empresas proveedoras de servicios de telecomunicaciones conserven un registro, al menos por un año, de los datos de las conexiones que hagan las direcciones IP asociadas a su servicio. Dicha información solamente puede ser dada a conocer a los órganos que la ley indique, resguardando la privacidad de sus abonados.

Otra arista a considerar es el régimen de protección de datos personales en Chile. La Ley 19.628, sobre Protección de la vida privada, data de la década de 1990 y ha sido un blanco de críticas desde el comienzo, por entregar amplias facilidades para el tratamiento de datos sin mayores peligros de incurrir en responsabilidad o de recibir sanción, ya que no provee un marco adecuado de fiscalización, reclamación, sanción y compensación.

La normativa privilegia el tratamiento de datos para el tráfico comercial por sobre los derechos de los individuos, no contempla una autoridad de control que vele por la protección de datos, ni hace mención al tratamiento transfronterizo de datos personales. Además, plantea fuertes desincentivos para accionar en tribunales: se tramita ante los tribunales ordinarios, se exige cumplir con un estándar de culpa muy difícil de probar, las sanciones son ba-

jas y no establece formas especiales de reparación. La ley protege solamente a personas naturales,[10] no exige el registro de los bancos de datos de entes privados y el titular de los datos no tiene real participación ante un proceso de comunicación a terceros de esta información.

De manera indirecta, existen otras normativas sectoriales que inciden en los resultados de este estudio. Debido a la fiscalización que ejercen tanto el Servicio Nacional del Consumidor (SERNAC), la Fiscalía Nacional Económica (FNE) y la Subsecretaría de Telecomunicaciones (SUBTEL), es posible encontrar en línea información sobre los contratos que vinculan a los clientes con las empresas de telecomunicaciones, como parte de los esfuerzos por transparentar las condiciones comerciales vigentes en el país.

En cuanto a la publicación de informes de transparencia y políticas de privacidad por parte de las empresas, si bien la legislación no los exige, tampoco los prohíbe. Por lo mismo, la publicación de este tipo de documentos será considerado una "buena práctica" para efectos de este informe.

2.2. Empresas de telecomunicaciones

Durante 2017 la empresa WOM aumentó notoriamente su participación en el mercado de las telecomunicaciones en Chile. Luego de haber adquirido a Nextel en 2015,[11] WOM pasó de un 3,5 % a un 7,7 % de participación en el mercado de telefonía móvil entre marzo 2016 y marzo 2017,[12] crecimiento que siguió aumentando durante el 2017, y para septiembre su participación alcanzó un 9,71 %.[13] Si bien WOM no cuenta con presencia en el mercado de internet fijo, su considerable participación como proveedora de internet móvil, método de conexión que ha determinado el aumento en el acceso a internet durante los últimos años,[14] justifica la inclusión de WOM en la versión 2018 de este informe.

---

10 *Jervis, P. (2006). "Modelo de Propuesta Regulatoria al Mercado de Datos Personales en Chile". Revista Chilena de Derecho Informático 8, pp. 152-155 . Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/ viewFile/10787/11035 [Fecha de consulta: 24 de abril de 2018].*

11 *Fayerwayer (2015). "Ya es oficial: Nextel Chile cambiará su nombre a WOM". Disponible en: https://www.fayerwayer.com/2015/06/ya-es-oficial-nextel-chile-cambiara-su-nombre-a-wom/ [Fecha de consulta: 3 de mayo de 2018].*

12 *SUBTEL (2017). "Sector de Telecomunicaciones". Disponible en: http://www.subtel.gob.cl/wp-content/uploads/2017/07/PPT_Series_MARZO_2017_V3.pdf [Fecha de consulta: 3 de mayo de 2018].*

13 *SUBTEL (2017). "Estadísticas sectoriales. Período Información Enero 2000 – Septiembre 2017". Disponibles en: http://www.subtel.gob.cl/estudios-y-estadisticas/telefonia/ [Fecha de consulta: 3 de mayo de 2018].*

14 *A septiembre 2017 la penetración de internet fija fue de 16,6 accesos por cada 100 habitantes, mientras que la penetración de Internet móvil 3G+4G alcanzó a 80,8 accesos por cada 100 habitantes. SUBTEL (2017). "Sector de Telecomunicaciones". Disponible en: http://www.subtel.gob.cl/wp-content/uploads/2018/01/PPT_Series_SEPTIEMBRE_2017_V1.pdf [Fecha de consulta: 3 de mayo de 2018].*

En cuanto a la participación en el mercado del resto de las empresas de telecomunicaciones, el más reciente informe de la SUBTEL[15] muestra cómo el mercado ha evolucionado durante el último año. De acuerdo con las estadísticas a septiembre de 2017, las cuotas de participación de las diferentes empresas proveedoras es la siguiente:

a. Movistar: 34,2 % en internet fijo y 28,6 % en internet móvil.
b. VTR: 38 % en internet fijo y 1,3 % en internet móvil.
c. Claro Chile: 13,8 % en internet fijo y 21,5 % en internet móvil.
d. Entel: 1,2 % en internet fijo y 32,8 % en internet móvil.
e. GTD Manquehue: 8,6 % en internet fijo y no cuenta con participación en el mercado de internet móvil.
f. WOM. No cuenta con participación en el mercado de internet fijo; 14,3 % en internet móvil.

Las seis empresas seleccionadas para este estudio representan una parte sustantiva del mercado de internet en Chile: un 95,8 % de los servicios de internet fijo y 98,5 % de conexiones móviles.

Según cifras a septiembre de 2017, el 97,5 % de la población tiene acceso a internet, mayoritariamente a través de servicios móviles, número que se ha mantenido al alza durante los últimos 6 años. En consecuencia, los resultados de esta evaluación dan cuenta de una situación que afecta a parte importante de la población chilena.

15 *SUBTEL 2015. "Sector Telecomunicaciones". Disponible en: http://www.subtel.gob.cl/wp-content/uploads/2015/04/PPT_Series_DICIEMBRE_2015_V5.pdf [Fecha de Consulta: 5 de septiembre de 2016]*

3. Metodología

Este informe busca dar cuenta de cómo las empresas proveedoras de servicio de internet protegen la privacidad de sus usuarios, y si cuentan con políticas para el correcto tratamiento de los datos personales de sus clientes. Con el fin de comparar la evolución de las políticas de las empresas entre el período 2017 y 2018, la metodología de esta versión 2018 no sufre grandes modificaciones respecto a la versión 2017.[16] Se realizan algunos ajustes para hacer más precisa la medición, pero que permiten la comparación de resultados en los dos años.

Al igual que en 2017, examinaremos el cumplimiento de determinados parámetros de estudio en dos niveles. El primero en relación con el nivel de transparencia que las empresas de telecomunicaciones muestran frente a sus usuarios. Para ello, nos pondremos en la situación del usuario y tendremos en consideración solamente la información que es posible encontrar en los sitios web de las empresas. El nivel de transparencia será medido en consideración a si las empresas hacen públicos en su sitio web: los términos y condiciones de uso o de contratación del servicio; la política de protección de datos personales (dirigida al usuario) y el procedimiento para solicitar dichos datos (dirigido a la autoridad, pero disponible para los usuarios); el informe de transparencia; la información sobre las notificaciones realizadas a los usuarios sobre requerimientos de datos y sobre defensas judiciales y legales.

Como adición para 2018, y producto de la polémica que surgió en 2017 por el intento de la autoridad de aumentar el período de retención de metadatos de telecomunicaciones,[17] en esta versión también se verificará si las empresas de telecomunicaciones informan a sus usuarios por cuánto tiempo almacenan sus datos de comunicaciones y si estos son eliminados transcurrido el tiempo mínimo exigido por la ley[18] para su retención. Sin embargo, para los fines de comparación mencionados, este último ítem no se considerará para efectos de calcular el puntaje de cada empresa.

---

16 *Disponible en: https://www.derechosdigitales.org/wp-content/uploads/qdtd-2017.pdf*

17 *Radio Universidad de Chile (2017). "Organizaciones alertan sobre "Decreto Espía" que pretende promulgar el Ministerio del Interior". Disponible en: http://radio.uchile.cl/2017/09/02/organizaciones-alertan-sobre-decreto-espia-que-pretende-promulgar-el-ministerio-del-interior/ [Fecha de consulta: 3 de mayo de 2018].*

18 *El artículo 222 del Código Procesal Penal establece que "los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados" (énfasis nuestro). Al referirse a un período "no inferior a un año", se deduce que las empresas proveedoras pueden retener dichos datos por más de un año. Por lo mismo, el hecho de que las empresas transparenten por cuánto tiempo realmente almacenan los metadatos, cómo son eliminados y cómo responden ante las solicitudes de la autoridad respecto de datos que ya han cumplido el período legal de retención, dan cuenta de un compromiso con la privacidad y protección de datos de sus usuarios.*

El segundo nivel de análisis se refiere a la evaluación de contenido, en términos de calidad, claridad y posibilidades de validación de la información, entre otros.

Al igual que en 2017, en ciertos casos excepcionales se ha hecho una calificación laxa, que ha resultado en la asignación de una puntuación mayor a la que corresponde cuando una empresa se encuentra notoriamente cercana a satisfacer los indicadores fijados para un parámetro. Intentamos así reflejar de mejor forma los matices de cumplimiento entre distintas empresas y evitamos modificar la escala de calificaciones, para no menoscabar la claridad de la información. Cuando así suceda, se dejará constancia de las oportunidades de mejora que existen en el ítem en cuestión.

Por último, y con el fin de entregar una escala de medición más precisa en esta versión del informe, la calificación por ítems no solo se realizará a través de una estrella completa o media estrella, sino que también se podrá calificar con un cuarto de estrella. En otras palabras, la empresa obtendrá una estrella si cumple de forma satisfactoria el parámetro, tres cuartos de estrella si cumple de forma casi satisfactoria, media estrella si cumple parcialmente, un cuarto si cumple de forma insatisfactoria y cero si no cumple el parámetro en lo absoluto. Nos parece importante que, a medida que aumenta el nivel de exigencia de los usuarios respecto de las condiciones de privacidad de sus empresas, este informe pueda realizar una medición más precisa. Con este informe entregamos a los usuarios una visualización que les permite diferenciar de forma más clara los distintos niveles de cumplimiento de las empresas proveedoras de servicios de internet en Chile.

A continuación formulamos las preguntas o inquietudes que el estudio pretende responder, junto con los parámetros de medición que deberían, idealmente, formar parte de la respuesta.

3.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

Parámetros de la respuesta:

- La empresa obtiene una estrella si cuenta con la copia del contrato de los servicios internet en todas sus modalidades –prepago, plan, fijo y móvil– y de las políticas de protección de datos.
- La política de protección de datos es clara y de fácil acceso para los usuarios.
- La política de protección de datos coincide con la normativa nacional.
- La política ofrece mecanismos para el ejercicio de los derechos.
- La empresa obtiene media estrella si cumple parcialmente con la descripción anterior, ya sea porque:
- Solo publica los contratos de un tipo de servicio.
- No permite acceso a las copias del contrato, pero sí a principios y términos

básicos que informan respecto a las obligaciones contractuales adquiridas con la empresa
- Publica, de alguna forma, la política de protección de datos, ya sea como parte de sus contratos o en su página web, pero no en un documento específico para ello.
- La empresa no obtiene estrella si es que no cuenta con ninguno de los elementos señalados anteriormente o no se encuentran publicados en la página web.

3.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

Parámetros de la respuesta:

- La empresa obtiene una estrella si cuenta con un informe de transparencia que se refiera, de alguna forma, a vigilancia de las comunicaciones. Dicho informe debería evidenciar alguno de los siguientes puntos:
- El informe de transparencia explica con claridad el manejo de los datos de los usuarios, si estos han sido administrados por terceros y qué acciones se han realizado para su protección. En caso de gestión por terceros, menciona si alguna autoridad ha solicitado acceso a los datos y si fueron entregados.
- El informe de transparencia muestra la cantidad de solicitudes que han hecho las autoridades, a través de diferentes entidades del Estado.
- El informe de transparencia indica la cantidad de solicitudes de información personal a las que ha accedido, y la cantidad que ha rechazado.
- El informe de transparencia evidencia el número de usuarios que han sido notificados en el último año, en relación con el número de solicitudes de la autoridad.
- El informe de transparencia indica cuántas veces ha procedido a bloquear o retirar contenidos de internet, a petición de un órgano estatal.
- El informe de transparencia informa si ha habido defensa (legal directa ante el organismo requirente, o a nivel judicial) de los usuarios cuyo contenido ha sido bloqueado o retirado, y los motivos para ello.
- La empresa obtiene media estrella si cuenta con un informe parcial de transparencia, aunque no se refiera específicamente a la protección de datos ni a la vigilancia de las comunicaciones, pero sí a otros tópicos (por ejemplo, medidas para la prevención de la corrupción en la empresa), a partir de los cuales podría ampliarse en la dirección antes señalada.
- La empresa no obtiene estrella si no cuenta con informe de transparencia de ninguna especie publicado en la web.

3.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

Parámetros de la respuesta:

- La empresa obtiene una estrella si notifica de manera oportuna a los usuarios, en un momento permitido por la ley, para que puedan inter-

poner recursos o efectuar defensas, de ser ello posible y necesario.

- La empresa obtiene media estrella si notifica a los usuarios cuando ha habido solicitud de datos por parte de alguna autoridad, pero no lo hace de manera oportuna, dificultando la interposición de recursos o la realización de defensas.
- La empresa no obtiene estrella si no hay constancia de que notifique a sus usuarios de las solicitudes de información de la autoridad.

3.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

Parámetros de la respuesta:

- La empresa obtiene una estrella si cuenta con una guía para el manejo de datos de los usuarios, publicado en su página web y destinado específicamente a orientar los requerimientos por parte de la autoridad, cuyo contenido se refiere a los siguientes puntos:
- La guía para el manejo de datos de los usuarios es clara y de fácil acceso.
- Especifica los procedimientos que tiene para responder a las solicitudes de información de los usuarios por parte de la autoridad.
- Especifica los requisitos necesarios para responder favorablemente a la solicitud (por ejemplo, una orden judicial).
- Es clara respecto al tiempo durante el cual guarda la información proporcionada por los usuarios, y su posterior eliminación.
- La empresa obtiene media estrella si cuenta con alguna guía publicada en su sitio web para el manejo de los datos de los usuarios, aún cuando no haya sido específicamente formulada para dirigirse a las autoridades (por ejemplo, políticas de neutralidad) y que solo cuenten parcialmente con algunos de los puntos antes mencionados.
- La empresa no obtiene estrella si en su página web no ha publicado ningún documento que sirva de guía a la autoridad para el manejo de los datos de los usuarios.

3.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

Parámetros de la respuesta:

- La empresa obtiene una estrella si ha recurrido a la justicia para dejar sin efecto requerimientos de datos que considera excesivos y ha representado los intereses de los usuarios ante el Congreso, en la discusión de una legislación invasiva, desproporcionada o lesiva de la privacidad de los usuarios.

- La empresa obtiene media estrella si ha efectuado defensas en uno de los dos ámbitos (judicial o legislativo) relacionadas con los intereses de los usuarios.
- Forma parte de coaliciones o iniciativas multisectoriales donde existen intercambios con usuarios o representantes del interés público.
- Ha emitido declaraciones públicas condenando iniciativas legales, administrativas o judiciales por afectar o amenazar la privacidad de sus usuarios.
- La empresa no obtiene estrella si no ha efectuado ninguna defensa de los usuarios, judicialmente ni ante el Congreso Nacional.

4. Análisis

4.1. WOM

4.1.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

Debido a que WOM se incorporó como empresa objeto de estudio en la presente versión de este informe, no es posible comparar su desempeño con la versión 2017.

En la portada de su sitio web, WOM tiene disponible la pestaña "Términos Comerciales, Contractuales y Transparencia", donde es posible acceder a una versión tipo del Contrato de Servicio[19] en formato PDF, así como de los anexos de "Planes y Tarifas Multimedia", "Planes Sólo Voz", "Planes Sólo Datos" y "Planes y Tarifas Internet".[20] El sitio web presenta la información a través de una serie de pestañas que se expanden al hacer clic, y resulta bastante claro e intuitivo acceder a ellas.

El contrato tipo hace las veces de base para suministro de servicios de toda clase y es complementado por los anexos dependiendo del servicio que se contrate. El contrato hace referencia a la protección de datos personales de sus clientes en su cláusula octava,[21] donde WOM se compromete a respetar los principios establecidos en la legislación de protección de datos personales, limitando el tratamiento de datos del cliente para los fines propios de la prestación de servicio. Del mismo modo, se establece que el cliente tendrá derecho a solicitar la modificación o eliminación de sus datos personales, y se entrega una vía específica para materializar dicha solicitud. Por otro lado, el contrato tipo no establece la fecha en que fue publicado o un identificador de la versión de que se trata,[22] por lo que no es posible para el cliente saber si las condiciones que él aceptó al momento de contratar fueron modificadas unilateralmente por la empresa, o si ellas han cambiado sustantivamente para los usuarios nuevos.

---

19 *WOM. Nuestro Contrato de Servicios. Disponible en: https://www.wom.cl/documents/20182/1291711/Contrato+servicios+persona/5fcfdce0-85f4-eefa-87d3-6fe1bab5f4b4 [Fecha de consulta: 23 de marzo de 2018].*

20 *WOM. Términos Comerciales, Contractuales y Transparencia. Disponible en: https://www.wom.cl/terminos_condiciones. [Fecha de consulta: 23 de marzo de 2018].*

21 *La cláusula octava del contrato establece que "WOM protege y asegura los datos personales de sus clientes garantizando que serán almacenados y su tratamiento será utilizado para los fines propios asociados a la prestación del servicio contratado, dando estricto cuidado a los principios de legitimidad, acceso, información, calidad de los datos, finalidad, proporcionalidad, transparencia, no discriminación, limitación de uso y seguridad en su tratamiento. En cualquier momento el cliente podrá solicitar la modificación o eliminación de sus datos personales y el no envío de información publicitaria, promocional y/o de entretenimiento acercándose a las sucursales habilitadas o llamando al 80066415" [Fecha de consulta: 23 de marzo de 2018].*

22 *Aún cuando la dirección URL del archivo PDF da a entender que se trata de una versión del año 2018.*

Los anexos de “Planes y Tarifas Multimedia”, “Planes Sólo Voz”, “Planes Sólo Datos” y “Planes y Tarifas Internet” complementan el contrato tipo en cada uno de los servicios referidos. Sin embargo, estos anexos contienen información de carácter técnico, especialmente referido a la velocidad y las condiciones de entrega de servicio, y no hacen referencia a las condiciones de privacidad o protección de datos de los usuarios.

En la pestaña “Políticas de privacidad y de seguridad” se pueden encontrar las políticas de protección de datos y de privacidad que aplican a las interacciones entre el usuario y el sitio web. En el subapartado titulado “Captura de datos personales” se establece que la empresa utilizará los datos personales del usuario únicamente para el fin por el cual la información es requerida, informando el propósito y condiciones de entrega de los datos. Del mismo modo, se compromete a no “revelar” datos personales de sus usuarios, ni comercializarlos con terceros ajenos a WOM y sus empresas relacionadas, salvo que cuente con el consentimiento del usuario. Por último y en sintonía con el principio de finalidad, la empresa se compromete a que, en la eventualidad de darle un uso distinto a los datos que tiene bajo su poder, informará tal circunstancia al usuario y le entregará la oportunidad de rechazar el uso de sus datos. En este último punto no queda claro si WOM entiende que requiere el consentimiento expreso del usuario, o que ante la notificación a este y la falta de un rechazo expreso (una especie de silencio circunstanciado) se encontraría habilitado para dar un uso distinto a los datos respecto del cual fueron recabados, lo cual podría contradecirse con lo establecido por la Ley 19.628.

La misma pestaña cuenta con un enlace a la Política de Privacidad y Seguridad,[23] que se encuentra en formato PDF. Este documento repite lo establecido en la pestaña de “Política de privacidad y seguridad”, pero señala que WOM podría verse obligada a dar a conocer los datos personales de sus usuarios, estrictamente a fin de cumplir con ciertos requerimientos legales (eventualidad que será estudiada en otro apartado de este informe), y entrega información sobre los vínculos a sitios de terceras partes en su sitio web y del funcionamiento de las encuestas que WOM realiza, en las cuales la empresa se compromete a anonimizar las respuestas del usuario.

Atendido a lo anterior, es posible concluir que WOM efectivamente pone a disposición de los usuarios sus contratos, con cláusulas sobre protección de datos y una política de privacidad. Si bien existe una mención a los principios de la Ley 19.628 y a los derechos que esta otorga a los titulares de datos personales, falta precisión respecto de la forma en que el usuario debe entregar su consentimiento para el tratamiento de datos para fines distintos a los

23 *WOM. Política de Privacidad y Seguridad. Disponible en: https://www.wom.cl/documents/20182/1291711/Pol%C3%ADtica+de+privacidad+WOM_marzo_2018/091f25ec-0c16-1e57-a3fc-be677bb38fd9 [Fecha de consulta: 23 de marzo de 2018].*

establecidos al momento de ser recabados. Del mismo modo, los documentos carecen de una fecha de publicación establecida o de una versión que les permita a los usuarios comparar la que actualmente les rige, respecto de las condiciones que aceptaron al momento de contratar

WOM obtiene una estrella, con las prevenciones señaladas en los párrafos anteriores.

4.1.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

En la pestaña titulada "Términos Comerciales, Contractuales y Transparencia" es posible encontrar el informe de transparencia de la empresa. Solo existe un documento disponible, correspondiente a 2018.[24] El informe es un documento bastante escueto, de una plana, en donde WOM declara que las empresas de telecomunicaciones tienen la obligación legal de responder los requerimientos de las autoridades, siempre y cuando dichos requerimientos cumplan todos los requisitos de su normativa.

A continuación, el informe entrega una estadística general de 2017, declarando que se realizó un total de 2.957 interceptaciones. Sin embargo, no existe un desagregado de cuántas solicitudes de interceptación recibió de parte de la autoridad, qué número o porcentaje fue rechazado y qué número o porcentaje fue otorgado. Por otro lado, no queda claro si dichas interceptaciones se refieren exclusivamente a interceptaciones de comunicaciones telefónicas o también incluyen otros tipos de comunicaciones.

En el mismo apartado, WOM declara haber recibido un total de 7.385 "solicitudes de información" durante el año 2017, para luego señalar a modo ejemplar qué tipo de información fue solicitada por la autoridad:

- Datos asociados a números telefónicos y simcards de WOM.
- Datos asociados a RUT de personas o empresas clientes de WOM.
- Números telefónicos asociados a IMEIs.
- Tráficos de líneas telefónicas.

Nuevamente, no existe un desagregado entre la cantidad de solicitudes de información por parte de la autoridad y el porcentaje de dichas solicitudes que fue otorgado por la empresa. Del mismo modo, no existe mayor precisión respecto a qué datos son entregados, por ejemplo, al referirse a "datos asociados a números telefónicos y simcards de WOM". No detalla este aspecto lo suficiente para adquirir certeza respecto a qué datos se refiere, ni se encuentran desagregados por cantidad en las cuatro categorías que el informe

24 *WOM. Informe de Transparencia año 2018. Disponible en: https://www.wom.cl/documents/20182/1291711/Informe+de+Transparencia/fb6398d5-b0bb-96cf-0b30-7d20dfb2158b [Fecha de consulta: 23 de marzo de 2018].*

establece de modo ejemplar. Del mismo modo, el informe no declara si dicha información es eliminada, ni bajo qué mecanismos, luego de haber transcurrido el plazo de un año establecido en la ley.

Por último, cabe destacar que el último párrafo del informe de transparencia declara que WOM espera poder generar más indicadores el próximo año, para así mantener a los ciudadanos más informados y velar por la mayor transparencia posible. Lo anterior da cuenta de una intención positiva de mejorar sus niveles de transparencia, especialmente considerando que se trata de una empresa relativamente nueva en el mercado.

WOM obtiene tres cuartos de estrella, en vista de la publicación de un informe de transparencia, al que le hace falta una desagregación estadística de los datos entregados y una mención acerca de su mecanismo de eliminación.

4.1.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

Una revisión del contrato tipo, de los anexos y de la Política de Privacidad y Seguridad muestra que no existe una referencia a la necesidad de notificar al usuario acerca de las solicitudes de informaciones que recibe la empresa por parte de las autoridades. El informe de transparencia del año 2018 tampoco cuenta con una mención al respecto.

Lo más cercano a una mención en esta materia puede encontrarse en el punto (ii) de la Política de Privacidad y Seguridad, el cual establece que "no obstante lo anterior, WOM podría verse obligada a dar a conocer tus datos personales estrictamente a fin de cumplir con ciertos requerimientos legales (ver Protocolo de Entrega de Información a la Autoridad)".

Sin embargo, el Protocolo de Entrega de Información a la Autoridad[25] no cuenta con ninguna referencia respecto de la notificación a los usuarios en caso de solicitudes de información por parte de la autoridad.

Por ello, WOM obtiene cero estrellas.

4.1.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

WOM cuenta con un documento que establece el procedimiento, requisitos y formalidades que una solicitud de requerimiento de información por parte

25 *WOM. Protocolo de Entrega de Información a la Autoridad. Disponible en: https://www.wom.cl/documents/20182/1291711/Protocolo+de+entrega+de+infor¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?maci%C3%B3n+a+la+autoridad/c6d2e481-cec9-9c56-7b9f-541b135dac08 [Fecha de consulta: 23 de marzo de 2018].*

de la autoridad debe cumplir. Dicho documento es titulado "Protocolo de Entrega de Información a la Autoridad" y se encuentra disponible en el sitio web de WOM a disposición de las autoridades y los usuarios para su revisión. También vale la pena mencionar que el documento hace referencia al año de su publicación, en este caso el 2018, dando a entender que se informará la fecha en que es modificado o actualizado.

El protocolo comienza por dar cuenta de los cuerpos jurídicos que pueden ser invocados por la autoridad para solicitar la interceptación de comunicaciones o la solicitud de información personal de los usuarios, entre ellos: el Código Procesal Penal (artículos 9, 219, 222 y 223); el Decreto 142 de 2005 del Ministerio de Transportes y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación; la Ley 19.974 sobre Sistema Nacional de Inteligencia; entre otras.[26]

Respecto de la interceptación de comunicaciones, el protocolo establece que debe ser solicitada por el Fiscal del Ministerio Público que investiga una causa, por Carabineros o por la Policía de Investigaciones, presencialmente en las oficinas de WOM o a través de un correo electrónico especialmente habilitado para tal efecto. Dicha solicitud debe contener: "Autorización/Resolución judicial debidamente firmada y timbrada. En caso de que la solicitud sea mediante correo electrónico debe estar íntegramente escaneada en PDF. Asimismo, velar porque ésta contenga los datos mínimos de interceptación, tales como RUC de la investigación, tribunal, fecha de la autorización, número a intervenir, plazo de la interceptación y número de derivación. En caso de que el correo lo envíe un funcionario de la PDI o de Carabineros, deberá poner en copia al fiscal de la causa".

Resulta positivo que la empresa haga explícita la necesidad de la autorización judicial que ordena la diligencia de interceptación de comunicaciones, pues es un requisito establecido explícitamente por el Código Procesal Penal, y es relevante que los usuarios lo conozcan. Del mismo modo, es positivo que la empresa se reserve el derecho a solicitar la rectificación de la solicitud en caso de no cumplirse alguno de los requisitos mencionados. Del mismo modo, el protocolo regula los casos de interceptación urgente, prórroga de la interceptación, modificación de canales de derivación y desconexión anticipada.

Respecto a la solicitud de información de tráfico,[27] esta deberá ser solicitada por el Fiscal, miembro de la Policía de Investigaciones o Carabineros a través de su correo institucional, solicitando la información pertinente, y

26 *Ibid.*

27 *Cabe decir que "información de tráfico" se refiere a los metadatos que las empresas de telecomunicaciones deben almacenar por un período no menor de un año, de acuerdo al inciso quinto del Artículo 222 del Código Procesal Penal.*

adjuntando la resolución judicial correspondiente. Esto es particularmente valioso, pues da a entender que la orden judicial previa es un requisito necesario no solo para la interceptación de comunicaciones, sino que también para solicitar la entrega de metadatos.

El protocolo también admite que en casos "urgentes" la solicitud se realice sin necesidad de enviar copia de la resolución judicial, poniendo en copia al fiscal de la causa. En este caso, se deberá acompañar la resolución con posterioridad a la realización de la diligencia. La excepción resulta cuestionable, ya que no existe una alusión a reglas legales que autoricen esa entrega. De acuerdo al artículo 9º del Código Procesal Penal "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa".[28] Sin embargo, el protocolo condiciona esta entrega a que "exista autorización judicial, pero esta no se tenga materialmente", exigiendo que el Fiscal de la causa a través de su correo institucional dé cuenta de la urgencia y la existencia de la orden judicial. Si bien esta situación no es ideal, y cuesta imaginar una circunstancia en donde exista una orden judicial pero no sea posible adjuntarla, la redacción del protocolo entrega certeza suficiente de que efectivamente se exige la existencia de una orden judicial previa para la entrega de información de sus usuarios.

WOM obtiene una estrella.

4.1.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

No existen antecedentes que den cuenta de la realización de este tipo de acciones en la web de la empresa, ni en los documentos publicados en ella.

Wom obtiene cero estrellas.

4.2. Movistar Chile

4.2.1. ¿La empresa proveedora tiene publicado en su sitio web una copia del contrato de servicios de internet y de su política de protección de datos?

Movistar no ha modificado su sitio web en relación al año anterior, encontrándose públicamente los términos y condiciones de sus servicios de telecomunicaciones en el apartado "Condiciones Comerciales y Contractuales" de su sitio web, contando con apartados distintos para el servicio de bancha

28 *El énfasis es nuestro.*

ancha hogar[29] y para el servicio de telefonía móvil y banda ancha móvil.[30]

Del mismo modo, las condiciones comerciales del servicio de Banda Ancha Móvil (BAM)[31] y las Banda Ancha Fija Prepago (BAF Prepago)[32] no han sufrido modificación alguna. En ambas es posible encontrar una cláusula muy escueta y abstracta, que da cuenta de que el tratamiento de datos personales se realizará de acuerdo a lo establecido por la Ley 19.628.

Asimismo, el documento titulado "Política de Privacidad Movistar"[33] no ha sido actualizado desde la publicación de la versión 2017 del presente informe.[34] En este documento se indica con claridad los datos que serán recolectados y el uso que la empresa se reserva poder realizar. El documento es de fácil acceso, al encontrarse en la misma sección que las condiciones contractuales y comerciales de los diferentes servicios de telecomunicaciones que Movistar Chile presta.

Se trata de un texto general, de una página de extensión, el cual señala regir "al contratar los servicios con Movistar", sin mayores precisiones. Lo anterior implica que los contratos de servicios de telecomunicaciones, incluido internet fijo y móvil, quedan sujetos a dicha política de privacidad de datos personales, aún cuando en ellos no se hace referencia alguna a la existencia y contenido

29 *Movistar Chile. Condiciones Comerciales y Contractuales de servicio hogar. Disponible en: http://www.movistar.cl/PortalMovistarWeb/centro-de-ayuda/condiciones-comerciales-y-contractuales-de-servicios-hogar [Fecha de consulta: 23 de marzo de 2018].*

30 *Movistar Chile. Condiciones Comerciales y Contractuales de telefonía y banda ancha móvil. Disponible en: http://hogar.movistar.cl/centro-de-ayuda/condiciones-comerciales-y-contractuales-de-telefonia-movil-y-banda-ancha-movil/ [Fecha de consulta: 23 de marzo de 2017].*

31 *Movistar Chile. Condiciones Contractuales del Servicio de Banda Ancha Fija Prepago. Disponible en: http://www.movistar.cl/PortalMovistarWeb/ShowDoc/WLP+Repository/Portlets/P030_Generico/Documentos/Contractuales_Baf_Prepago [Fecha de consulta: 23 de marzo de 2018].*

32 *Movistar Chile. Condiciones Contractuales del Servicio de Banda Ancha Móvil. Disponible en: http://www.movistar.cl/PortalMovistarWeb/ShowDoc/WLP+Repository/Portlets/P030_Generico/Documentos/BAM_1 [Fecha de consulta: 23 de marzo de 2018].*

33 *Movistar Chile. Política de Privacidad Movistar. Disponible en: http://www.movistar.cl/PortalMovistarWeb/ShowDoc/WLP+Repository/Portlets/P030_Generico/Documentos/Politica_de_Privacidad_Movistar_200214.pdf [Fecha de consulta: 23 de marzo de 2018].*

34 *Si bien el documento no cuenta con una fecha de publicación establecida, el título del archivo PDF da a entender que fue publicado el 20 de febrero de 2014.*

de la mencionada política, lo que no facilita a los usuarios su conocimiento.[35]

El documento, a diferencia de la Política de Privacidad y Seguridad de WOM, establece taxativamente los datos personales que Movistar recaba y trata, a saber:

- Nombre
- Apellido paterno.
- Apellido materno.
- Número de R.U.T.
- Número de serie de cédula de identidad
- Fecha de nacimiento.
- Número telefónico.
- Dirección particular y/o comercial.
- Dirección de correo electrónico.

Tras analizar su contenido podemos sostener que, si bien no se profundiza en cómo se protegen específicamente los datos de los usuarios, se señala que su tratamiento es efectuado de acuerdo a la ley chilena. Expresa claramente los datos que recogen y se indica la finalidad con que se tratarán. Sin embargo, no existe mención a la conservación de los metadatos a la que obliga el artículo 222 del Código Procesal Penal, ni una mención el período de conservación de los mismos o su método de eliminación.

Dado lo escueto del texto, no es posible sostener que, adicionalmente, mencione alguna medida destinada a evitar violaciones a la privacidad. Las políticas de Movistar se limitan a declarar que la empresa dará cumplimiento a la legislación de protección datos, no estableciendo mecanismos de protección del usuario que vayan más allá de lo establecido por la legislación.

Movistar obtiene tres cuartos de estrella, con las prevenciones indicadas.

4.2.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

Movistar cuenta con dos informes, uno de sostenibilidad en Chile[36] y otro de transparencia en el sitio web de su matriz internacional.

---

35 *En el caso de las condiciones comerciales y contractuales de servicios digitales que conlleven la intervención de un tercero, como sucede con las "Condiciones de suscripción a la aplicación Napster" aplicables a los servicios móviles, Movistar pone a disposición el link para revisar las políticas de privacidad y datos de esa empresa. Disponible en: http://www.movistar.cl/PortalMovistarWeb/ShowDoc/WLP+Repository/Portlets/P030_Generico/Documentos/Condiciones_suscripcion_Napster [Fecha de consulta: 23 de marzo de 2018].*

36 *Telefónica Chile. Informe de Sostenibilidad. Disponible en: http://www.telefonicachile.cl/telefonica-y-sociedad/informe-de-sostenibilidad/ [Fecha de consulta: 23 de marzo de 2018].*

El informe de sostenibilidad del año 2017 no ha sido publicado a la fecha de redacción de este informe, por lo que la última versión corresponde al año 2016, la misma que fue analizada en la versión anterior de este informe.[37] Esta versión no contempla información sobre vigilancia de las comunicaciones, ni alguno de los demás puntos considerados en la respuesta modelo. Con todo, resulta destacable que dicho informe manifieste el interés de la empresa por dar cumplimiento a ciertos estándares de protección de datos personales. Por ejemplo, se han elaborado unos "Principios de negocio responsable", orientados inicialmente a los trabajadores de la empresa pero que están destinados a reflejarse en la relación de ellos con todos aquellos con quienes interactúan, incluyendo lógicamente a los clientes. Entre esos principios destacan la protección de la confidencialidad, el aseguramiento de los datos personales, el respeto de la Declaración Universal de los Derechos Humanos y el cumplimiento de la ley, entre otros.

En el informe también se advierte una marcada inclinación hacia la promoción de la seguridad de la información, instituyendo una actividad denominada "Security day 2016", que involucró información sobre el cuidado de datos personales. En consecuencia, es posible sostener que existe un enfoque en la satisfacción del cliente. Lamentablemente ello parece no haber alcanzado áreas complejas como la información sobre solicitud, y eventual entrega, de sus datos a entidades de Gobierno que los hubieren requerido, bajo qué procedimientos y requisitos, ni si ello le fue comunicado al afectado o tuvo como efecto el retiro o bloqueo de contenidos.

En el informe de 2017 se dio cuenta de la paradoja de que Movistar transparente la cantidad de requerimientos de información de sus clientes, pero en un informe alojado en su sitio internacional y no en su sitio chileno. Para la presente entrega de este informe, nuevamente realizamos una búsqueda en el sitio web nacional de Movistar y no fue posible encontrar un informe de transparencia con estadísticas en esta materia.

En tanto, el "Informe de Transparencia en las Comunicaciones" alojado en el sitio internacional de Movistar ha sido actualizado a su versión de 2017.[38] Al igual que en su versión 2016, la versión actualizada del informe cuenta con información de 18 países, incluido Chile. El informe transparenta los requerimientos de información de los clientes de Movistar y las solicitudes para bloquear el acceso a sitios web, para bloquear o filtrar contenido y para suspender temporalmente el servicio.

---

37 *Telefónica Chile. Informe de Sostenibilidad 2015. Disponible en: http://www.telefonicachile.cl/wp-content/uploads/2016/04/informe-2015.pdf [Fecha de consulta: 29 de agosto de 2016].*

38 *Documento disponible en: http://www.movistar.es/rpmm/estaticos/residencial/transparencia/informe-transparencia-2017.pdf [Fecha de consulta: 23 de marzo de 2018].*

El informe establece que en 2016 Movistar Chile recibió 12.480 solicitudes de interceptación de comunicaciones (2.356 menos que en 2015), de las cuales 60 fueron rechazadas; 42.684 de acceso a metadatos (1.464 más que en 2015), de las cuales 127 fueron rechazadas; y ninguna solicitud para bloqueo y filtrado de determinados contenidos (en 2015 se registró una solicitud de bloqueo). Vale la pena mencionar que, a diferencia de 2015, la información del 2016 establece la cantidad de solicitudes que fueron rechazadas por Movistar, estadística que no se encontraba disponible en la versión anterior.

Al igual que el año anterior, este informe no está alojado ni enlazado en el sitio chileno de Movistar (donde los usuarios llevan a cabo la interacción en línea con la empresa), lo que dificulta que los clientes sepan del informe y accedan a él. Por lo tanto, no es posible aseverar que la mera publicación de este informe cumpla con los parámetros de transparencia establecidos en este estudio. Al mismo tiempo la interrogante se mantiene: por qué publicar información relativa a Chile en su sitio internacional pero sin enlace en portal chileno, o sin algún nivel local de difusión.

En definitiva, Movistar no muestra ningún avance sustantivo a nivel nacional en lo que respecta a la publicación de informes de transparencia. La única actualización en esta materia proviene del sitio web internacional de la empresa, la que liberó estadísticas actualizadas y más específicas relativas a las solicitudes de interceptación, solicitudes de información y bloqueo de sitios web respecto de los usuarios chilenos. Sin embargo, no hay esfuerzo alguno por presentar tales cifras a los usuarios nacionales.

A pesar de lo anterior, la información transparentada por Movistar a nivel internacional sigue siendo la más precisa en el mercado, lo que justifica la máxima calificación de este informe.

Movistar obtiene una estrella.

4.2.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

Al igual que en la versión anterior de este informe, no ha sido posible encontrar públicamente información al respecto. En los términos contractuales y comerciales de los servicios fijo y móvil –incluidas las políticas de privacidad existentes–, no se menciona nada respecto a solicitudes de información por parte de la autoridad, al menos desde una perspectiva que diera cuenta hipotética de cómo se procedería en caso de una solicitud.

Del mismo modo, el informe de sostenibilidad y de transparencia de la empresa no se pronuncian al respecto, y no fue posible encontrar un pronunciamiento en el sitio web de la empresa.

Movistar obtiene cero estrellas.

4.2.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

Movistar no presenta ningún avance en esta materia, ya que no ha sido posible encontrar información específica sobre este punto. Lo anterior agrega un factor de opacidad a la forma en que Movistar administra las solicitudes de información por parte de la autoridad, ya que de acuerdo a su Informe de Transparencia 2017, de las 42.684 solicitudes de acceso a metadatos recibidas, 127 fueron rechazadas. Sin embargo, a diferencia del caso de WOM, no se transparenta el criterio bajo el cual estas 127 solicitudes fueron rechazadas.

Por ello, Movistar obtiene cero estrellas.

4.2.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

Al igual que el año anterior, no consta ni en la web de la empresa ni en la documentación disponible en ella, que estas actividades hayan tenido lugar.

Sin embargo, en marzo de 2017,[39] Telefónica comenzó a formar parte de la Iniciativa de Red Global (GNI, por sus siglas en inglés), una red multisectorial que tiene como objetivo promover la privacidad, la libertad de expresión y la colaboración entre distintos actores del sector. La pertenencia a GNI obliga a Telefónica a suscribir una serie de principios que demuestran al menos una intención inicial por la protección de los derechos de los usuarios de internet. Queda pendiente de examen la materialización de esos compromisos en la oferta de servicios a nivel local.

Movistar obtiene un cuarto de estrella en función de su afiliación con la red GNI.

4.3. VTR

4.3.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

Bajo el apartado titulado “Condiciones contractuales y comerciales de VTR” en su sitio web, VTR tiene disponibles copias de los contratos y condiciones comerciales de sus servicios de internet, fijos y móviles (sin distinción entre

39 *Información disponible en: https://www.telefonica.com/es/web/public-policy/blog/articulo/-/blogs/nos-unimos-al-gni-para-impulsar-la-libertad-de-expresion-y-la-privacidad [Fecha de consulta: 1 de abril de 2018].*

las modalidades prepago y plan),[40] los que contienen cláusulas relativas a las políticas de datos personales. El acceso es bastante sencillo e intuitivo.

El contrato de suministro de internet fijo y móvil[41] es el mismo que se encontraba vigente cuando se publicó la versión anterior de este informe, por lo que no presenta ninguna innovación. En él, y de manera prácticamente idéntica para las modalidades fija y móvil, se establece que la empresa contempla mecanismos autorizados que registran el uso de los servicios y las interacciones que los usuarios tienen con la compañía. Estos serán utilizados por VTR con la exclusiva finalidad para mejorar sus servicios, procedimientos de atención e iniciativas comerciales, no asociando la información a algún cliente identificado o identificable.

Luego, indican que registran y analizan información individual de cada suscriptor, relativa al uso de los servicios y su interacción con VTR, con la finalidad de entregar adecuadamente los servicios contratados. Para ello, esta información es procesada, por VTR o por proveedores externos, velando por la aplicación de los adecuados estándares de confidencialidad, sin perjuicio del deber de VTR de informar a terceros algunos de estos datos, de acuerdo con la normativa vigente o el requerimiento de una autoridad competente.

Le sigue una cláusula en la cual el cliente autoriza a VTR y a las empresas terceras autorizadas a registrar y analizar información sobre el uso de servicios e interacción con la compañía, señalándose expresamente que estos datos serán procesados directamente por VTR y terceros, velando por los estándares de confidencialidad y recalcando las obligaciones legales de comunicar tales datos a terceros cuando una autoridad lo requiera. En conformidad a la Ley 19.628, el suscriptor autoriza a VTR a tratar, analizar y correlacionar los datos personales relativos a sus antecedentes de contacto, servicios contratados y comportamiento de pago.

Finalmente, se otorga al cliente la posibilidad de modificar sus datos y en el caso de los servicios móviles, la posibilidad de revocar la autorización antes referida.

Como vemos, por medio del contrato el cliente autoriza la recolección de una gran cantidad de datos personales de contacto, identificación y de sus hábitos de consumo. Aunque inicialmente se indica que serán tratados de forma estadística, luego se evidencia que podrían ser tratados de forma comercial,

40 *VTR. Revisa las Condiciones Contractuales y Comerciales de los Servicios VTR. Disponible en: http://vtr.com/productos/moviles/contratos [Fecha de consulta: 23 de marzo de 2018].*

41 *VTR. Solicitud de Suministros de Servicios de VTR. Disponible en: http://vtr.com/CS/vtr_f3/contrato-de-suministro.pdf y VTR. Condiciones de Suministro de Servicios Móviles. Disponible en: http://vtr.com/CS/vtr_f3/condiciones_de_suministro_de_servicios_moviles1.pdf [Fecha de consulta: 30 de agosto de 2016].*

no solo por VTR sino también por terceros autorizados por la empresa; en ningún momento se indica al cliente quiénes son estos terceros. Esta modalidad contrasta con la de WOM, que solo admite que sus empresas relacionadas utilicen los datos de sus usuarios para actividades comerciales.

Sin perjuicio de esto, se estipula que los terceros deberán enunciar su vínculo con VTR al momento de contactarse con un cliente para ofrecer servicios comerciales, pudiendo estos revocar esta autorización de acuerdo a las reglas generales de la Ley 19.628.

Por su parte, VTR también ha publicado un documento destinado exclusivamente a comunicar su política de privacidad,[42] que incluye un apartado sobre datos personales aplicable no solo a los usuarios del sitio web, sino a todos sus clientes. Lamentablemente, esta no se encuentra enlazada ni mencionada en los contratos; por el contrario, es la propia política la que señala que debe ser leída "en conjunto con la sección de 'condiciones generales de contratación del o los servicios'". De esta forma, en los hechos, las políticas y los contratos funcionan como dos documentos independientes, que requieren de un alto compromiso por parte de los usuarios para informarse sobre su contenido. Del mismo modo, ni el contrato ni la política de privacidad cuenta con una fecha de publicación o número de versión, que le permitan al cliente cotejar si la empresa ha modificado unilateralmente las condiciones que aceptó al momento de contratar sus servicios.

Analizada la política de privacidad, encontramos que se detallan los datos o información personal que es recolectada, indicándose al menos tres grupos de finalidades: en el primero se menciona el cumplimiento de las obligaciones legales de la compañía, así como la provisión y mejoramiento de sus productos y servicios. En el segundo grupo se habla sobre la posibilidad de mejorar la gestión de dichos productos y servicios. Finalmente se refiere a los fines propiamente comerciales de la empresa. A continuación, se mencionan los potenciales destinatarios de estos datos según el fin que se persigue, las medidas de seguridad que se adoptan para proteger la privacidad de los clientes y los procedimientos para que los usuarios ejerzan sus derechos.

En definitiva, VTR no presenta un avance en esta materia respecto del año anterior. En particular, no ha subsanado su falta de especificidad respecto de las entidades con las cuales puede compartir la información personal de sus clientes para efectos de comunicación comercial. A pesar de esto, en su sitio web es posible acceder a sus distintas modalidades contractuales, y a su política de privacidad.

VTR obtiene tres cuartos de estrella, con las prevenciones efectuadas en los párrafos anteriores.

42 *VTR. Política de privacidad del consumidor. Disponible en: http://vtr.com/privacidad/ [Fecha de consulta: 23 de marzo de 2017].*

4.3.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

VTR no muestra ningún avance en esta materia respecto del año anterior. De hecho, su informe de sustentabilidad más reciente corresponde al año 2015[43] y al entrar al enlace https://vtr.com/empresa/ y hacer clic en "sustentabilidad" la página arroja un error. Como señalamos en la versión anterior de este informe, el informe de sustentabilidad de 2015 contempla un acápite sobre "Administración Ética" de la compañía, donde se comprometen a "respetar la privacidad y proteger todos los datos personales que procesamos".

Adicionalmente, el informe contiene menciones a la política anticorrupción de la compañía, y alguna escueta mención al retiro y bloqueo de contenidos bajo la forma de una capacitación para los usuarios en cuanto al uso de una aplicación para bloquear contenidos de pornografía infantil, disponible de forma gratuita.

Resulta preocupante, sobre este punto, que VTR exhiba no más, sino menos información actualizada que en la versión anterior de este informe. Esperamos que, con miras a la información de sus usuarios actuales y potenciales, VTR contemple la publicación de informes de transparencia.

Debido a la falta de avance en la materia, VTR obtiene cero estrellas.

4.3.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

Al igual que el año anterior, no fue posible hallar una mención al respecto en los términos contractuales y comerciales de los servicios prestados por VTR, disponibles en el sitio web de la compañía, ni tampoco se publicó un nuevo informe de sustentabilidad que pudiese innovar en la materia.

Sin embargo, cabe destacar que en la mencionada política de privacidad, a propósito de las finalidades de recolección de datos, menciona expresamente:

"Primer Grupo: 1. Para cumplir con nuestras obligaciones legales. Podrían solicitarnos por ley revelar información personal para cumplir con los términos de un proceso legal válido o por requerimiento de otros organismos similares. Estas divulgaciones podrían ser hechas con o sin tu consentimiento y conocimiento, y con o sin aviso, en cumplimiento de los términos de un proceso legal. VTR se reserva el derecho a cuestionar el acceso a información personal a las autoridades".[44]

---

43 *VTR. Reporte de Sustentabilidad VTR 2014. Disponible en: https://vtr.com/empresa/pdf/REPORTE_SUSTENTABILIDAD_VTR_2015.pdf [Fecha de consulta: 23 de marzo de 2018].*

44 *VTR. Ibid.*

La mención, cuando menos, aporta a los usuarios algún antecedente acerca de la factibilidad de ser comunicados de una solicitud de sus datos, aún cuando se prescinde de detalles que puedan ser considerados como suficientes. Queda en duda la necesidad de discreción a que hace referencia la política.

Por ello, VTR obtiene media estrella. Aunque no satisfacen completamente el criterio, representa un avance en relación a sus pares en esta categoría. De todas formas, sería positivo que a futuro VTR definiera con más precisión en qué condiciones notifica y en qué condiciones no notifica a los usuarios de las diligencias que le son ordenadas por la autoridad.

4.3.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

VTR no ha avanzado en esta materia respecto del año anterior, ya que todavía no cuenta con un documento específicamente orientado a las autoridades sobre este tema.

Como se señaló con anterioridad, la política de privacidad menciona la posibilidad de que las autoridades hagan requerimientos de datos. Sin embargo, en ninguno de los casos se especifica el procedimiento que deben seguir las autoridades y bajo qué circunstancias una solicitud podría ser rechazada por VTR. En el mismo sentido, no consta en ningún documento público una mención de por cuánto tiempo VTR almacena los metadatos mencionados en el artículo 222 del Código Procesal Penal, ni se establece la modalidad de eliminación de estos, una vez cumplido el período legal de retención.

En cuanto al bloqueo y retiro de contenidos, es posible encontrar información en las políticas sobre neutralidad de VTR.[45] Allí se entregan algunas directrices, indicando bloqueo de puertos, de sitios que contienen pornografía infantil, el filtro de números IP asociados a usos maliciosos, impedimento a correos electrónicos de spam masivos y a transmisión de virus mediante puertos. Sin embargo, debido a que la publicación de dicha información se realiza cumpliendo con una obligación legal (contenida en la Ley 20.453), dicha circunstancia no puede ser considerada a la hora de otorgar puntaje en esta sección.

En un sentido similar, en sus "Condiciones de uso" la compañía establece medidas para la administración eficiente de sus redes, aduciendo razones de seguridad informática, la prevención del spam y la propagación de virus; entre las medidas contempladas se encuentra el bloqueo transitorio de ciertos

45 *VTR. Políticas de Administración de Red. En línea, disponible en: http://vtr.com/neutralidad/b4.php [Fecha de consulta: 23 de marzo de 2018]*

puertos. Estas medidas son aplicables tanto a los usuarios del sitio web de la compañía, como a los clientes del servicio de acceso a internet provisto por VTR, complementando lo dispuesto en el contrato de suministro de servicios y las "Condiciones Generales de Contratación de Suministro de Servicios por Banda Ancha VTR", que regulan el servicio de internet y los servicios conexos que haya contratado cada cliente.

Finalmente, cabe consignar que en las condiciones comerciales aplicables a los "servicios hogar",[46] documento que entrega información anexa a los contratos, se contemplan normas sobre bloqueo de contenidos. A propósito de la gestión de la red, se menciona el bloqueo de acceso a sitios de abuso infantil y el mecanismo para levantar dicha medida, en caso de que sea improcedente. Si bien este documento fue actualizado en enero de 2018, no cuenta con modificaciones sustantivas.

VTR obtiene cero estrellas.

4.3.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

Al igual que el año anterior, no existen antecedentes adicionales que den cuenta de la realización de este tipo de acciones en la web de la empresa, ni en los documentos publicados en ella.

La única mención al punto corresponde a la de las ya citadas políticas de privacidad, que sobre el uso de datos para dar cumplimiento a sus obligaciones legales indican que "VTR se reserva el derecho a cuestionar el acceso a información personal a las autoridades",[47] sin entregar mayores detalles. Sin embargo, a diferencia del año anterior VTR no es la única empresa que contempla esta posibilidad. Al establecer un protocolo para la solicitud de información por parte de la autoridad, WOM y Claro han establecido públicamente los requisitos necesarios que la autoridad debe cumplir para solicitar la interceptación de comunicaciones y solicitud de entrega de información. Estos se encuentra definidos de forma precisa y permiten a la empresa solicitar la rectificación de la solicitud cuando estos no se cumplen.

Por lo mismo, no es posible entregar a VTR media estrella, como sucedió en la versión anterior de este informe. Puesto que subsiste algún nivel de información, la calificación desciende sin perderse por completo.

VTR obtiene un cuarto de estrella.

---

46 *VTR. Condiciones comerciales Servicios Hogar. En línea, disponible en: http://vtr.com/CS/vtr_f3/condiciones_contractuales_comerciales.pdf [Fecha de consulta: 23 de marzo de 2018].*

47 *Ibid.*

4.4. Claro Chile

4.4.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

En la sección "Claro Transparente"[48] existe un apartado sobre condiciones contractuales y comerciales donde se puede acceder a una copia digital de los contratos, tanto de servicios fijos como móviles, sin distinguir entre prepago y plan. Se contemplan los servicios fijos (hogar) por cable (no satelital) y para los móviles, denominándolo servicio de datos o acceso a internet.

A diferencia del año anterior, Claro Chile hoy cuenta con una política de privacidad publicada en su sitio web, la cual hace mención expresa a la protección de datos personales de sus usuarios.[49] En ella, Claro establece que solo efectuará tratamiento de datos personales respecto de aquellos que han sido entregados voluntariamente por los clientes y/o usuarios a través de su sitio web.

A continuación, la política de privacidad de Claro indica que el tratamiento de los datos personales de sus usuarios puede realizarse con fines estadísticas, de marketing, comunicar ofertas y promociones y con el objeto de entregar información y/o beneficios de la empresa. Del mismo modo, se establecen los casos en que Claro podrá comunicar los datos personales de sus usuarios a terceros, pero limita esta hipótesis exclusivamente al "objeto de entregar información y/o beneficios de CLARO". De esta forma queda descartada la posibilidad de que Claro pueda vender a terceras partes la información personas de sus clientes con fines comerciales. El resto de la política se limita a reproducir derechos contenidos en la Ley 19.628.

Claro ha avanzado sustantivamente en esta materia en comparación con el año anterior, al publicar un documento dedicado específicamente a dar cuenta de sus términos y condiciones en materia de protección de datos personales. Del mismo modo, resulta valorable que se haya establecido una finalidad acotada para la recolección y tratamiento de datos para efectos promocionales y de marketing.

Claro Chile obtiene una estrella.

---

48 *Claro Chile. Contrato Servicios Claro. Disponible en: http://www.clarochile.cl/portal/cl/pc/personas/institucional/legal-y-regulatorio/#06-condiciones-comerciales-y-contractuales [Fecha de consulta: 23 de marzo de 2018].*

49 *Claro Chile. Política de Privacidad. Disponible en: https://www.clarochile.cl/portal/cl/legal-regulatorio/lightbox/descripcion-ED-48.html [Fecha de consulta: 23 de marzo de 2018].*

4.4.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

En este ítem Claro también ha mostrado un avance respecto del informe anterior, donde no contaba con un informe de transparencia. Hoy en su página de inicio es posible encontrar un enlace titulado "Protección de Datos", el cual redirige a un archivo PDF titulado "Política de Protección y Requerimiento de Datos", documento actualizado a abril de 2018.[50] El tercer apartado de este documento, titulado "Estadísticas de requerimientos de información y de interceptación por parte de las autoridades" presenta las estadísticas en la materia correspondientes al segundo semestre de 2017.

Estas estadísticas se presentan de manera simple y directa, dividiéndose en dos ítems: "Solicitud de información general (Titularidad, tráfico y georreferenciación, etc.)" y "Solicitudes de interceptación telefónica".[51] Estas estadísticas también se encuentran desagregadas en zonas: Norte, Centro y Sur.

El cuadro muestra que durante el segundo semestre de 2017 existieron 12.276 solicitudes de "información general (Titularidad, tráfico y georreferenciación, etc.)" y 2.349 solicitudes de interceptación telefónica. Un pie de página en el mismo documento establece que "se hace presente que del universo total de solicitudes de realizadas durante el 2° semestre de 2017, se procedió a objetar y/o solicitar rectificar a 139 requerimientos, lo que corresponde al 0,1 % aprox. que no cumplían las exigencias establecidas en las normas precedentemente citadas". Esta estadística es valiosa, pero no desglosa cuántos fueron derechamente rechazados y cuántos solo fue necesario rectificar para luego ser aprobados.

Claro muestra un evidente avance en esta materia, dando a conocer estadísticas que si bien no son del todo desagregadas, permiten al usuario conocer la cantidad de solicitudes de metadatos y de interceptaciones telefónicas realizadas por la autoridad, y un aproximado del total que son de alguna forma objetadas por las empresa.

Claro Chile obtiene una estrella.

4.4.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

Al igual que el año anterior, no fue posible encontrar mención alguna respecto a los aspectos evaluados en esta categoría en el sitio web de la empresa, ni en los demás documentos ahí disponibles.

Claro Chile obtiene cero estrellas.

---

50 *Claro Chile. Protección y Requerimiento de Datos. Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/proteccion-y-requerimientos-de-datos-vf_20180424.pdf [Fecha de consulta: 28 de abril de 2018].*

51 *Esto resultaría bastante extraño, ya que el término "interceptación" se encuentra en el título del apartado.*

4.4.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

Al igual que en el ítem de informes de transparencia, Claro Chile ha mostrado un avance respecto del año anterior en este ítem. En el documento titulado "Protección y Requerimiento de Datos" antes mencionado, el segundo apartado se titula "Protocolo de implementación y coordinación en materia solicitudes de requerimientos e interceptaciones de comunicación".

El documento establece que la finalidad de este apartado es dar cumplimiento al Protocolo acordado con el Ministerio Público y Claro Chile (el cual no está disponible en su sitio web). El documento luego establece que, para aceptar o rechazar una solicitud de requerimiento se debe cumplir con los siguientes requisitos:

Para solicitar tráfico de teléfono: es necesario tener una orden judicial enviada por un tribunal o una autorización con un poder simple por el propietario del número.

Para solicitar georreferencia, información de propietario, información de número, IMEI, tráfico IMEI, tráfico de antena, contratos, es necesario que a la orden judicial, se adicione la respectiva instrucción particular emanada del Ministerio Público, la cual, circunscribe, coordina y especifica los términos sobre los cuales versa la señalada resolución judicial que accede a la entrega de la información. Todo requerimiento que no cumpla con el procedimiento descrito debe ser rechazado u objetado.

Resulta positivo que para solicitar el tráfico del teléfono,[52] el protocolo haga explícita la exigencia la presentación de la orden judicial correspondiente, y que Claro declare que todo requerimiento que no cumpla con los requisitos será rechazado.

Del mismo modo, y al igual que en el caso de WOM, resulta sumamente positivo que Claro explicite que la solicitud de datos comunicacionales referidos a georreferencia, información de propietario, información de número, IMEI, tráfico IMEI, tráfico de antena y contratos también requieren de la presentación de una orden judicial previa para su entrega.

Por lo anterior, Claro Chile obtiene una estrella, la puntuación máxima.

---

52 *Este término es más bien ambiguo, y no queda realmente claro si se refiere a la interceptación de las comunicaciones telefónicas en los términos establecidos por el Código Procesal Penal, o al tráfico de datos de internet que un teléfono con plan de navegación puede generar.*

4.4.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

La nueva política de privacidad establece que "Claro Chile, podrá discutir, cuestionar y pedir aclaración del alcance del requerimiento a la autoridad solicitante, con el objeto de resguardar y proteger la privacidad de los datos personales de sus Clientes y/o Usuarios". A diferencia de la mención genérica establecida por VTR en esta materia, lo establecido por Claro da cuenta de una intención positiva, ya que eventualmente podría objetar las solicitudes de información de la autoridad, con el objetivo explícito de resguardar la privacidad de sus usuarios.

En atención a lo anterior, Claro Chile obtiene media estrella.

4.5. Entel

4.5.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

El sitio web de Entel no ha sufrido mayores modificaciones en el último año. En él se encuentran disponibles los contratos de servicios móviles y hogar, dentro de los cuales están los referentes a internet,[53] sin distinción entre las modalidades plan y prepago.

En la sección de privacidad de su sitio web es posible acceder a la "Política de Privacidad",[54] pero este documento no cuenta con una fecha de publicación o la indicación de una versión que le permita al consumidor cotejar si ha existido algún cambio unilateral con la versión que aceptó al momento de contratar los servicios de Entel.

La Política de Privacidad establece que los datos personales únicamente serán tratados para el fin por el cual la información es requerida, informando el propósito y condiciones de entrega de dichos datos. Del mismo modo, Entel se compromete a no revelar estos datos personales, ni comercializarlos a terceros, salvo mediar el consentimiento del titular. De forma similar a lo establecido por WOM, en la eventualidad de que a los datos capturados se les

---

53 *Entel. Contratos. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P63200157451364998548342 [Fecha de consulta: 23 de marzo de 2018].*

54 *Entel. Política de Privacidad. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P860032801126903180234 4. [Fecha de consulta: 23 de marzo de 2018].*

pudiera dar algún uso diferente al propósito para el cual fueron capturados, Entel se compromete a informar al usuario de tal circunstancia, otorgándole la oportunidad para rechazar dicho uso de sus datos.

Del mismo modo, Entel cumple con informar, de forma poco precisa, que pueden verse obligados dar a conocer los datos datos personales del usuario con el fin de cumplir requerimientos legales, hecho que el usuario debe declarar aceptar.

Entel obtiene tres cuartos de estrella.

Cabe mencionar también que la empresa cuenta con unas políticas de privacidad aplicables solo a la navegación en su sitio web, por lo que difieren del análisis aquí efectuado.[55]

4.5.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

En el sitio web de Entel solo es posible encontrar un "Reporte de Sustentabilidad"[56] que, al igual que Movistar, es una guía que transparenta la organización corporativa de la empresa, el plan de acción de la compañía y avances en la prestación de servicios.

La última versión disponible del documento corresponde a 2016,[57] y a diferencia de la versión 2015 contiene un apartado especialmente dedicado a la Seguridad de la Información y Protección de Datos. En él, se menciona que la empresa mejoró la calidad de su certificación ISO 27001-2013 y que se implementará un Comité Táctico de Ciberseguridad.

Sin embargo, el documento no entrega estadísticas sobre solicitudes de acceso a información personal ni peticiones de retiro de contenidos por parte de la autoridad.

En consecuencia, no es posible encontrar información relacionada con vigilancia de las comunicaciones y su prevención, pero sí sobre otro tópicos relevantes como la prevención de la corrupción.

Entel obtiene cero estrellas, en función de la ausencia de un informe que corresponda a 2018.

---

55 *Entel. Condiciones generales de uso. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P5180016078135171388448 4 [Fecha de consulta: 23 de marzo de 2018].*

56 *Entel. Sustentabilidad. Disponible en: http://informacioncorporativa.entel.cl/sustentabilidad/ [Fecha de consulta: 23 de marzo de 2018].*

57 *Entel. Reporte de Sustentabilidad 2016. Disponible en: http://entel.cl/libros/memoria-anual-2016-reporte-sustentabilidad/#2 [Fecha de consulta: 23 de marzo de 2018].*

4.5.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

No existe mención alguna en los documentos públicamente disponibles que se refieran a las solicitudes realizadas por agencias gubernamentales relativas al acceso a información de los usuarios.

Entel obtiene cero estrellas.

4.5.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

En el sitio web de Entel no existen guías orientadas al Gobierno para el requerimiento de información de sus usuarios. Dicha información tampoco se encuentra disponible en su Política de Privacidad, que se limita a informar al usuario que se encuentran legalmente obligados a entregar información personal cuando se realice en función de un requerimiento legal.

Dado lo anterior, Entel obtiene cero estrellas.

4.5.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

No consta en la web de la empresa, ni tampoco en informes públicos de prensa, que estas actividades hayan tenido lugar.

Entel obtiene cero estrellas.

4.6. GTD Manquehue

4.6.1. ¿La empresa proveedora tiene publicado en su sitio web el contrato de servicios de internet y su política de protección de datos?

GTD Manquehue pone a disposición del interesado una copia de su contrato de servicios de telecomunicaciones que aplica a todo servicio contratado con la empresa,[58] además de las condiciones generales de contratación de estos mismos,[59] no diferenciándose entre móvil y fijo, prepago o plan. Ambos do-

58 *GTD Manquehue. Solicitud y Contrato de Servicios GTD Manquehue. Disponible en: https://nuevo.gtdmanquehue.com/condiciones-comerciales/contratos-de-servicios-gtd-manquehue/solicitud-y-contrato-de-servicios-gtd-manquehue [Fecha de consulta: 23 de marzo de 2018].*

59 *GTD Manquehue. Condiciones Generales de Contratación de Servicios de GTD Manquehue S.A. Disponible en: https://nuevo.gtdmanquehue.com/condiciones-comerciales/contratos-de-servicios-gtd-manquehue/condiciones-generales-de-contratacion-gtd-manquehue [Fecha de consulta: 23 de marzo de 2018].*

cumentos fueron actualizados respecto de la última versión de este informe, pero sin modificaciones sustanciales en materia de privacidad y protección de datos.

En las condiciones generales, la empresa contempla una cláusula donde explica el procedimiento para poder modificar datos y para dejar de recibir información comercial, publicitaria, promociones u ofertas de entretenimiento, que son los fines con los cuales normalmente las empresas proveedoras de servicio en Chile, sus empresas relacionadas y terceros autorizados, tratan los datos de sus clientes.

Por su parte, no es posible encontrar en el sitio web de GTD Manquehue un documento o una sección del sitio con las directrices a seguir en materia de protección de datos personales de sus usuarios. Como suele ser usual en las empresas de telecomunicaciones nacionales, todo lo relativo a datos se regula contractualmente.

GTD Manquehue obtiene media estrella.

4.6.2. ¿Cuenta la empresa proveedora con un informe de transparencia?

No es posible encontrar públicamente una copia de un informe de transparencia, ni algún documento afín que regule las materias contempladas en este ítem.

Por ello, GTD Manquehue obtiene cero estrellas.

4.6.3. ¿La empresa proveedora notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad?

No existen documentos ni información en la web de la empresa que den cuenta de información respecto a si se notifica o no a los usuarios de estos requerimientos.

GTD Manquehue obtiene cero estrellas.

4.6.4. ¿La empresa proveedora publica el procedimiento, los requisitos y las obligaciones legales que la autoridad debe cumplir al requerir información personal de sus usuarios?

No es posible encontrar un documento que haga mención al procedimiento que debe seguir una petición de parte del gobierno para obtener información de un usuario.

En este sentido, debemos mencionar que la empresa tampoco cuenta con una política de neutralidad que pudiere haber abordado de manera tangen-

cial el tema, como sucede en el caso de otras compañías, limitándose solo a redireccionar a la normativa aplicable en esa área.

GTD Manquehue obtiene cero estrellas.

4.6.5. ¿La empresa proveedora ha defendido la privacidad y ha protegido activamente los datos de sus usuarios, ya sea públicamente, en juicio o en el marco de una discusión legislativa en el Congreso?

No consta en la web de la empresa, ni tampoco en documentos disponibles en ella, que ninguna de estas actividades haya tenido lugar.

GTD Manquehue obtiene cero estrellas.

¿QUIÉN DEFIENDE TUS DATOS?

DERECHOS DIGITALES

LA EMPRESA	Presenta claridad en los contratos y políticas internas	Realiza reportes de transparencia	Notifica al usuario en caso de que haya una solicitud de información	Publica los requisitos legales a la autoridad para pedir información de sus usuarios	Ha defendido la privacidad de sus usuarios en juicio	Balance
Movistar	★	★	☆	☆	☆	31%
VTR	★	☆	★	☆	☆	30%
Claro	★	★	☆	★	☆	70%
Entel	★	☆	☆	☆	☆	15%
GTD	☆	☆	☆	☆	☆	10%
WOM	★	★	☆	★	☆	55%

★ cumple todos los parámetros

★ cumple casi satisfactoriamente

★ cumple parcialmente

☆ no cumple

☆ cumple de forma insuficiente

5. Conclusiones

El análisis de los indicadores propuestos en este informe dan cuenta del nivel de avance o de estancamiento en cuanto a la protección de la privacidad de sus usuarios que las principales empresas de telecomunicaciones presentaron durante 2017. La principal novedad se encuentra en la incorporación de WOM en el estudio, la que con un puntaje de dos estrellas y tres cuartos se posiciona de entrada entre las empresas que mejor resguardan los derechos de sus usuarios.

Por otro lado, Claro es la empresa que más ha avanzado en sus indicadores de desempeño, pasando de media estrella en 2016 a tres estrellas y media en la presente entrega. En otras palabras, Claro pasó del último lugar en la tabla, al primero. La puntuación obtenida por estas dos empresas no es casualidad, ya que fueron las que más interés mostraron en mejorar sus condiciones de privacidad cuando los resultados de la primera versión de este informe fueron publicadas.

Movistar y VTR corresponden al segmento de empresas que fueron relativamente bien evaluadas durante 2016, pero que presentaron avances moderados o inexistentes durante 2017. Es posible que estas empresas se hayan confiado en su relativo buen puntaje anterior, y producto de ello fueron superadas con creces por Claro y WOM.

Por último, Entel y GTD Manquehue fueron las dos empresas que habiendo sido mal evaluadas en el informe de 2017, mostraron avances sumamente limitados o nulos durante este año. En algunos casos, incluso, la ausencia total de información nueva significa una pérdida neta de información actualizada por parte de los usuarios. Esta falta de interés es indicativa de una voluntad limitada para avanzar en la protección de la privacidad de sus usuarios.

Si bien la notable mejora de algunas empresas da cuenta de un interés positivo por parte de algunos actores en la industria, el estancamiento de una parte sustantiva de la misma da cuenta de que no es transversal a todo el sector de las telecomunicaciones. Esta falta de mejora resulta más preocupante si se tiene en consideración que muchos de los indicadores de este informe, como la publicación de los contratos o los informes de transparencia, son más bien de carácter formal, y no requieren de grandes esfuerzos para su realización.

Como se mencionó en la tercera sección de este informe, la metodología se mantuvo respecto del año anterior, con el fin de poder comparar los puntajes de este año con la versión anterior, y de esta forma medir el nivel de avance de las distintas empresas. La próxima versión de Quién Defiende Tus Datos se propondrá modificar su metodología a fin de establecer exigencias más sustantivas a la industria en lo relativo a la protección de la privacidad de sus usuarios, con el fin de establecer una vara cada vez más alta en cuanto a las buenas prácticas de las empresas, en lo que respecta a la protección de la privacidad y los datos personales de los usuarios.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina