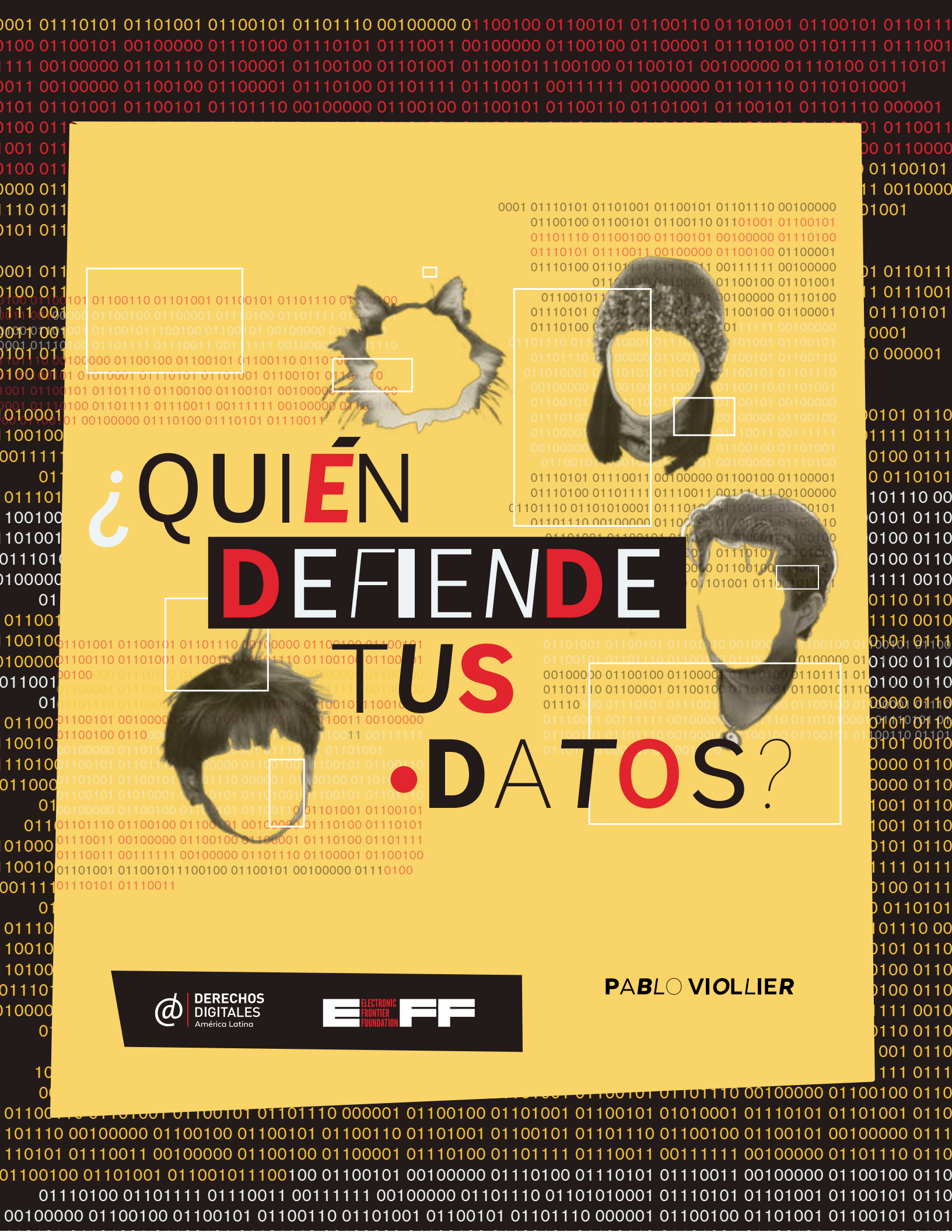

¿QUIÉN DEFIENDE TUS DATOS?

PABLO VIOLLIER

@ DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

¿QUIÉN DEFIENDE TUS DATOS?

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

PABLO VIOLLIER

Portada y diagramación: Constanza Figueroa.
Edición y correcciones: Vladimir Garay.
Revisión de pruebas: Rocío Consales.

Julio 2019.
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 de los derechos humanos en internet, la libertad de expresión, el acceso a la cultura y la privacidad.

Contenido

1. Introducción

El presente informe corresponde a la tercera entrega del reporte anual *¿Quién defiende tus datos?*, una evaluación que da cuenta de la forma en que las compañías chilenas que proveen servicios de internet resguardan los datos de sus clientes, especialmente frente a posibles abusos de la autoridad estatal. El énfasis está puesto en evaluar hasta qué punto las empresas defienden la privacidad de sus usuarios, sea ante las solicitudes de la autoridad frente al tratamiento indebido que terceros pretendan hacer de los datos personales de sus usuarios. Para ello, y como forma de continuar el seguimiento de la evaluación realizada el año 2018,[1] nos proponemos responder las siguientes preguntas: ¿Cuáles son las empresas que tienen las políticas 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 pasado, es una sustancial modificación en la metodología: en la anterior versión del reporte, publicada en 2018, mantuvimos la metodología del informe del del año 2017, con el objetivo de poder comparar con la misma vara el avance de las empresas en un año. Ya que en 2018 muchas empresas lograron mejorar sustantivamente respecto de la primera evaluación, este año hemos planteado una medición más exigente en términos sustantivos. De esta forma buscamos fomentar una "carrera hacia el tope", en donde las empresas comiencen a competir por quien entrega mejores condiciones de privacidad en el mercado y no solo por el precio de sus productos o la calidad de su servicio de conectividad.

La agenda política del año 2018 estuvo marcada por el interés creciente en la protección de los datos personales. Como demostración, el proyecto de ley que reforma el estatuto de protección de datos personales[2] ha avanzado sustantivamente y se encuentra pronto a superar su primera etapa de tramitación en el Congreso. Es por ello que, en esta versión del informe, nos hemos querido adelantar a la entrada en vigencia de la ley y exigir un estándar de protección de datos a las empresas mayor al contenido en la actual Ley 19.628. Por lo mismo, nos propusimos evaluar los términos y políticas de privaci-

1 Disponible en: https://www.derechosdigitales.org/wp-content/uploads/qdtd-2018.pdf

2 Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07 [Consultado el 30 de junio de 2019].

dad de las empresas a la luz de los principios de protección de datos contenidos en el proyecto de ley.

¿Quién Defiende Tus Datos? es parte de una serie de estudios similares realizados en América Latina y España, basados en ***Who Has Your Back?***, un reporte anual publicado por la Electronic Frontier Foundation (EFF) en Estados Unidos, cuya metodología seguimos adaptando a la realidad chilena, desde el punto de vista jurídico y de mercado. Nuestro informe analiza las políticas de privacidad y los códigos de prácticas disponibles al público de los proveedores de servicios de telecomunicación más grandes de Chile: Claro, Entel, GTD Manquehue, Movistar, VTR y WOM.

A continuación explicaremos cada una de las categorías de análisis. Para su formulación se han considerado los reportes realizados en años anteriores en Chile y otros países latinoamericanos, como Brasil, Colombia y México.

¿QUIÉN DEFIENDE TUS •DATOS?

TABLA DE RESULTADOS 2019

LA EMPRESA PROVEEDORA	WOM	Movistar	VTR	Claro	Entel	Manquehue GTD
¿Tiene en su sitio web una copia del contrato de servicios de internet y de su política de protección de datos?	★	☆	☆	★	★	☆
¿Cuenta con un informe de transparencia?	★	★	★	★	☆	☆
¿Notifica a los usuarios acerca de solicitudes de información del Gobierno?	☆	☆	☆	★	☆	☆
¿Publica el procedimiento, los requisitos y las obligaciones que el Gobierno debe cumplir al requerir información personal de sus usuarios?	★	☆	★	★	★	☆
¿Ha defendido la privacidad de los usuarios activamente, ya sea en juicio o en el marco de una discusión legislativa en el Congreso?	☆	☆	☆	☆	★	☆
*De un máximo de **5 estrellas,** obtiene:*	**4**	**1**	**2.**75	**4.**25	**3.**5	**0.**25

La escala de medición indica que:

- ★ cumple todos los parámetros
- ★ cumple casi satisfactoriamente
- ★ cumple parcialmente
- ☆ cumple de forma insuficiente
- ☆ no cumple

Más información en https://derechosdigitales.org/qdtd-2019

2. Metodología

La primera vez que se intentó utilizar la metodología de ***¿Quién Defiende tus Datos?*** en Chile, ninguna empresa analizada logró una calificación total superior a una estrella y media. La metodología fue revisada con el propósito de proveer incentivos a aquellas empresas que, al menos, mostraban una disposición a avanzar en la dirección correcta. El primer informe nacional, lanzado el año 2017[3] cuenta con una metodología de carácter más bien formal, ya que la industria no había avanzado en aspectos básicos como contar con informes de transparencia, políticas de privacidad disponibles al usuario o protocolos para la entrega a la autoridad de información de los usuarios.

La segunda versión del informe, publicada el año 2018,[4] mostró un importante avance a nivel de la industria en los distintos parámetros medidos. Sin embargo, con el fin de poder establecer una comparación con los resultados obtenidos el año 2017, la metodología se mantuvo inalterada. Si bien se agregaron ciertos aspectos a tener en consideración, estos fueron de carácter informativo y no tuvieron repercusión en el puntaje asignado a las empresas.

En esta entrega de ***¿Quién Defiende Tus Datos?*** nos interesa ir más allá. La industria ha avanzado considerablemente en aspectos como contar con políticas de protección de datos de forma pública, transparentar estadísticas de acceso a la información personal y la interceptación de comunicaciones privadas de los usuarios, y publicar los requisitos establecidos a la autoridad para acceder a dichas solicitudes. Es por ello que este año nos proponemos elevar la barra de medición: no nos detendremos en lo relativo a la protección de los derechos de las personas frente a posibles peticiones de la autoridad, sino en la protección de los datos personales en términos más generales. Si bien la lógica subyacente al proyecto original de EFF y a sus diversas variantes a nivel iberoamericano apunta al resguardo frente al abuso estatal, entendemos que un presupuesto básico de la defensa de los derechos de las personas pasa por una protección integral de los datos personales frente a otro tipo de amenazas.

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

4 Disponible en: https://www.derechosdigitales.org/wp-content/uploads/qdtd-2018.pdf

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

A diferencia de las entregas anteriores, el primer parámetro no se medirá de forma exclusivamente formal: para obtener la máxima puntuación las empresas no solo deberán tener disponibles públicamente sus contratos y sus políticas de protección de datos, sino que dichos documentos deben reflejar un compromiso sustantivo de la empresa con la defensa de los usuarios, su privacidad y la protección de sus datos personales. Establecer un parámetro para dicho compromiso no es tarea fácil, especialmente teniendo en consideración que muchas veces estamos exigiendo que las empresas vayan más allá de lo exigido por la ley. Por lo mismo, hemos establecido una serie de principios que sirven como criterio para discernir el nivel de compromiso de la empresa con la protección de los datos personales de sus usuarios.

Estos principios han sido obtenidos, en su mayoría, del texto del proyecto de ley de datos personales que hoy se tramita en el Congreso Nacional.[5] Ya que el texto de la versión final del proyecto de ley puede modificarse durante el proceso legislativo, se ha optado por una versión más genérica de estos principios, que por lo demás son universalmente aceptados en la protección de datos personales a nivel comparado. Los principios que se tendrán en consideración son los siguientes:

Principio de licitud: la empresa se compromete a tratar los datos solo en aquellos casos en que se encuentre habilitada por la ley o cuente con el consentimiento expreso del titular.

Principio de finalidad: la empresa se compromete a recolectar datos con fines específicos, explícitos y lícitos. Además, se compromete a que el tratamiento que se le dará a dichos datos se limitará a los fines por los cuales fueron recogidos.

Principio de proporcionalidad: El tratamiento de los datos debe limitarse a aquellos que resulten necesarios para los fines para los cuales fueron recolectados, los cuales no pueden ser excesivos, inespecíficos o afectar los derechos del titular.

Principio de calidad: La empresa se compromete a que los datos personales que almacene deben ser exactos, completos y actuales en relación con los fines de su tratamiento. De esta forma, deberán ser modificados o eliminados cuando dejen de cumplir este parámetro.

5 El texto del proyecto se encuentra disponible para consulta en el siguiente enlace: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07 [Consultado el 6 de marzo de 2019].

Principio de responsabilidad: La empresa se compromete a responder legalmente por el incumplimiento de los principios y deberes legales relacionados con la protección de los datos personales de sus usuarios.

Principio de seguridad: La empresa se compromete a garantizar estándares adecuados de seguridad, con el fin de evitar el tratamiento no autorizado de datos, y prevenir su pérdida, deterioro, filtración o destrucción. Para ello, debe tomar todas las providencias técnicas y organizativas disponibles, de forma continua y desde una perspectiva de gestión de riesgos.

Principio de confidencialidad: La empresa se compromete a resguardar reserva acerca de los datos personales del titular. Del mismo modo, se compromete a establecer controles y medidas adecuadas para preservar su confidencialidad, solo entregando acceso a terceros cuando el titular ha consentido expresamente o cuando es requerido por la autoridad cumplimiento los requisitos legales establecidos por el ordenamiento jurídico.

Principio de minimización de datos: La empresa se compromete a recoger solo los datos que sean estrictamente necesarios para la finalidad de su tratamiento, evitando recolectar datos innecesarios, excesivos o inespecíficos. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

El único principio aquí listado y no contenido en el proyecto de ley es el principio de minimización de datos, que, si bien se encuentra relacionado con el de proporcionalidad, nos parece importante considerarlo de forma separada. El principio de minimización de datos busca que las empresas solo recolecten los datos estrictamente necesarios para cumplir con la finalidad de la entrega de servicios, minimizando el riesgo de mal uso o filtración de datos sensibles.

Por otro lado, no se incluyó el principio de transparencia, ya que existen otros parámetros en el informe que buscan medir el cumplimiento de esa obligación en específico. Por último, es importante recalcar que para cumplir con estos principios, las políticas de privacidad o protección de datos de las empresas no necesitan mencionarlos explícitamente, sino que debe inferirse del contenido de sus disposiciones que la empresa ha adquirido un compromiso efectivo con estos principios.

2.2. Informe de transparencia

El segundo parámetro ha sufrido modificaciones menores. El año anterior, tres de las seis empresas estudiadas contaba con información estadística relativa al número de solicitudes de la autoridad de acceso a información personal y de interceptación de comunicaciones

privadas. Este año, además de lo anterior, se exigirá que las empresas expresen el número y porcentaje de las solicitudes que fueron rechazadas por no cumplir con los requisitos legales. Del mismo, se exigirá que las empresas presenten la información de forma desagregada, estableciendo el número de solicitudes que solicitan acceso a los metadatos de sus clientes[6] y el número de solicitudes que buscan concretar una interceptación de comunicaciones privadas. Puntaje adicional será asignado a las empresas que hagan un desglose territorial de las solicitudes recibidas.

Por último, esta versión del informe también verificará si las empresas de telecomunicaciones informan a sus usuarios por cuanto tiempo máximo almacenan sus metadatos de comunicaciones y si estos son eliminados transcurrido el tiempo exigido por la ley para su retención por parte de las ISP.

2.3. Notificación a los usuarios

La notificación a los usuarios se mantiene como el parámetro con menor cumplimiento en las dos versiones anteriores del informe. En 2018 sola una empresa logró obtener media estrella, y el resto ninguna.

Muchas de las empresas han expresado sus reparos respecto a la medición según este parámetro, aduciendo que el cumplimiento de esta exigencia podría traer problemas con la autoridad o que incluso no resulta legalmente posible notificar al usuario de una diligencia intrusiva, ya que el Código Procesal Penal establece un deber de reserva en su realización.

Este último punto tiene algún asidero, pero no compartimos la interpretación. Efectivamente, el artículo 236 del Código Procesal Penal establece la posibilidad de que, mediando una autorización judicial, se lleve a cabo una diligencia intrusiva sin previa comunicación al afectado, cuando la gravedad de los hechos o la naturaleza de la diligencia permitiera presumir que dicha circunstancia resulta indispensable para su éxito. También es posible solicitar esta diligencia reservada y sin notificación al afectado cuando ya se ha formalizado la investigación, cuando la reserva resulta estrictamente indispensable para la eficacia de la diligencia.

Sin embargo, esta reserva tiene como objetivo garantizar la realización de la diligencia, no mantener la reserva respecto de su realización de forma indefinida. Tampoco se trata de una exigencia con carácter general, sino de una facultativa, procedente en las circunstancias calificadas por la ley (como la gravedad de los hechos o la

6 Por metadatos nos referimos a la información que el artículo 222 inciso quinto del Código Procesal Penal exige a las empresas proveedoras de internet almacenar por un período no inferior a un año.

naturaleza de la diligencia). Una falta de comunicación extendida en el tiempo terminaría produciendo indefensión en las personas afectadas. En los casos en donde se formaliza una investigación contra la persona afectada por la medida, se reduce ese riesgo, ya que la defensa tendrá acceso a la carpeta de investigación.[7]

En rigor, una vez transcurrido el plazo que establece la reserva de la diligencia, las empresas proveedoras de internet no se encuentran legalmente impedidas de notificar a sus clientes el haber sido objeto de una medida intrusiva para obtener datos sobre su historial de tráfico o la interceptación de sus comunicaciones.

Resulta entendible que las empresas sean cautelosas en no participar más de lo estrictamente necesario en los procedimientos penales. Sin embargo, para aquellos afectados que son objeto de medidas intrusivas y nunca son formalizados, el hecho de que la empresa los notifique se transforma en el único mecanismo posible para enterarse de que alguna vez sus comunicaciones fueron intervenidas por la autoridad y adoptar las medidas que estimen necesarias.

Es por ello que la metodología de este año entrega una estrella completa a aquella empresa que establezca algún mecanismo para notificar a sus usuarios de que la autoridad ha solicitado su historial de tráfico (metadatos) o una interceptación de sus comunicaciones privadas. Esta notificación debe realizarse luego de que la reserva de la diligencia ha sido levantada, pero también se les entrega flexibilidad a las empresas para ser precavidas y notificar a sus usuarios con un plazo más holgado, por ejemplo, cuando la investigación ha sido cerrada sin formalizar al afectado, a través de la decisión de no perseverar o alguna salida alternativa al procedimiento. De esta forma, se puede equilibrar el que las empresas notifiquen sin entorpecer o participar innecesariamente en los procedimientos penales.

Por último - y debido a que este es el punto en que más difícil ha sido el progreso por las empresas chilenas - el informe también entregará una fracción de estrella a aquellas empresas que públicamente muestren interés y una iniciativa concreta para implementar un sistema que a futuro permita notificar a los usuarios, a través de un diálogo con las autoridades pertinentes.

2.4. Guías de cumplimiento de obligaciones legales orientadas a la autoridad

Este parámetro no sufrió modificaciones sustantivas en relación con el informe del año 2018. Se busca constatar que las empresas cuen-

7 De hecho, el artículo 182 del Código Procesal Penal establece explícitamente el procedimiento para declarar secretas ciertas diligencias respecto del imputado, la que se podrá declarar por un período no superior a 40 días, el cual podrá ser ampliado por el mismo período, por una sola vez, con motivos fundados.

ten con una pauta públicamente disponible que establezca cuales son los requisitos que la autoridad debe cumplir para que una solicitud de información o de interceptación de comunicaciones sea considerada legítima, es decir, con apego a la ley.

Especial énfasis se pone en que las empresas hagan explícito si solicitan la existencia de una orden judicial previa para acceder a realizar este tipo de diligencias. Por último, esta versión del informe también asignará puntaje teniendo en consideración si la empresa exige una orden judicial para acceder a la entrega del historial de tráfico de navegación o metadatos del usuario.

2.5. Defensa de la privacidad ante los tribunales de justicia y el poder legislativo

El objetivo de este parámetro es conocer si la empresa proveedora ha recurrido a tribunales con el objetivo de defender a alguno de sus usuarios ante una solicitud de acceso a la información o de interceptación de comunicaciones que no cumpla con los requisitos legales o que haya sido estimada como excesiva o desproporcionada. También será considerado el hecho de que la empresa haya efectuado alguna acción públicamente conocida para oponerse a proyectos de ley, normas legales o políticas públicas que pudieran afectar la privacidad o la protección de los datos personales de sus abonados.

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

2.6. Aspectos generales de la evaluación

Al igual que en el informe anterior, en ciertos casos excepcionales se ha asignado una puntuación mayor a la estrictamente correspondiente en aquellos casos en que consideramos que 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 compañías y evitamos modificar la escala de calificaciones, menoscabando 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. Si bien esto puede afectar la visualización de las calificaciones, nos parece importante que, a

medida que aumente el nivel de exigencia de los usuarios respecto de las condiciones de privacidad de sus empresas, loeste informe pueda realizar una medición más precisa. De esta forma, se le entrega a los usuarios una visualización que les permite diferenciar de forma más clara los distintos niveles de cumplimiento de los IPS chilenos.

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.

2.7. Las cláusulas del contrato y las disposiciones de las políticas de privacidad de la empresa muestran un compromiso con la defensa del usuario, su privacidad y la protección de sus datos personales

Parámetros de la respuesta:

El proveedor obtiene una estrella si:

- El contrato y la política de privacidad se encuentra disponible públicamente y sus disposiciones reflejan los principios de protección de datos contenidos en este informe.
- 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, estableciendo un punto de contacto para poder hacer llegar la solicitud respectiva.

El proveedor obtiene media estrella si cumple parcialmente con la descripción anterior, ya sea porque:

- Los principios solo se encuentran parcialmente reflejados en las disposiciones del contrato y las políticas de privacidad.
- Solo publica los contratos de un tipo de servicio.
- No publica copias de las disposiciones contractuales, pero sí los 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.

El proveedor no obtiene estrella si es que no cuenta con ninguno de los elementos señalados anteriormente o no se encuentran publicados en la página web.

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

Parámetros de la respuesta:

El proveedor 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 las solicitudes que han hecho las autoridades, a través de diferentes entidades del Estado.
- El informe de transparencia indica la frecuencia con la cual la empresa ha entregado información personal de los usuarios a la autoridad.
- El informe de transparencia señala en cuantas oportunidades se ha rechazado una solicitud de acceso a información personal o de interceptación de comunicaciones por parte de la autoridad.
- El informe de transparencia divide el número de solicitudes por categorías, diferenciando aquellas que se refieren a la información que el artículo 222 inciso quinto del Código Procesal Penal obliga a las empresas proveedoras de internet a almacenar por un periodo no menor a un año y aquellas solicitudes relativas a la realización de interceptación de comunicaciones.
- El informe desagrega el número de solicitudes a través de un criterio geográfico (comuna, región, etc).

El proveedor obtiene media estrella si cuenta con un informe parcial de transparencia, aunque no se refiera específicamente a la protección de datos y 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.

El proveedor no obtiene estrella si no cuenta con informe de transparencia de ninguna especie publicado en su sitio.

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

Parámetros de la respuesta:

El proveedor obtiene una estrella si notifica a sus usuarios de la realización de alguna diligencia intrusiva una vez que la reserva o secreto de dicha actuación ha sido levantado. La empresa también obtendrá una estrella si notifica al usuario de dicha actuación una vez que la investigación ha concluido sin haber sido formalizada, ya sea por

una decisión del fiscal de no perseverar o por alguna salida alternativa al procedimiento.

El proveedor obtiene media estrella si demuestra que se encuentra en proceso de implementar un sistema para poder notificar al usuario de que ha sido objeto de una medida intrusiva, a través de algún mecanismo de cooperación con la autoridad.

El proveedor no obtiene estrella si no hay constancia de que notifique a sus usuarios de las solicitudes de información de la autoridad.

2.10. ¿La empresa 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:

El proveedor 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.
- La empresa específica los procedimientos que tiene para responder a las solicitudes de información de los usuarios por parte de la autoridad.
- La empresa especifica los requisitos necesarios para responder favorablemente a la solicitud (por ejemplo, una orden judicial).
- La empresa es clara respecto al tiempo que guarda la información proporcionada por los usuarios y su posterior eliminación.

El proveedor 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.

El proveedor 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.

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

Parámetros de la respuesta:

El proveedor obtiene una estrella si ha recurrido a la justicia para dejar

sin efecto requerimientos de datos que considera excesivos o que pueden afectar los derechos de sus usuarios, incluso si dicha defensa significa arriesgar sus intereses comerciales o la interposición de una multa por parte de la autoridad.

El proveedor obtiene media estrella si ha efectuado algún tipo de defensa de sus usuarios en instancias distintas a la litigación judicial, en acciones como solicitudes de carácter administrativo, incidiendo en la tramitación legislativa de proyectos de ley o en la discusión de políticas públicas que puedan afectar los derechos de los usuarios. Para la evaluación en la entrega de puntaje también podrá tenerse en consideración los siguientes puntos:

- El proveedor forma parte de coaliciones o iniciativas multisectoriales donde existen intercambios con usuarios o representantes del interés público.
- El proveedor ha emitido declaraciones públicas condenando iniciativas legales, administrativas o judiciales por afectar o amenazar la privacidad de sus usuarios.

El proveedor no obtiene ninguna estrella si no ha efectuado ninguna defensa de los usuarios, judicialmente, administrativa ni ante el Congreso Nacional.

3 . *Contexto* **Nacional**

3.1. Marco regulatorio

No han existido modificaciones legales relevantes desde la publicación de la primera versión de este informe. La reforma a la ley nº 19.628 sobre Protección de la vida privada, formulada con el propósito de renovar casi la totalidad del estatuto, se presenta como el esfuerzo más ambicioso para actualizar la normativa que cumple ya veinte años de vigencia. Presentado el 13 de marzo de 2017,[8] el proyecto de ley[9] se encuentra en primer trámite constitucional (discusión de su articulado en el Senado), habiéndose aprobado en general en el Senado,[10] recibiendo luego indicaciones y propuestas de modificación por el Presidente de la República y un grupo de senadores. Todavía está pendiente la discusión y aprobación de artículos en particular en el Senado y 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 relación con la legislación procesal, la ley chilena 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

8 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/

9 Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

10 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/senado/2018-03-11/093136.html

ser autorizada previamente por un tribunal[11] a solicitud del Ministerio Público, órgano a cargo de la investigación y persecución criminal. Si la recolección de información tiene fines de inteligencia, procede a través de las direcciones de inteligencia de las Fuerzas Armadas y de las policías.

El inciso quinto del artículo 222 del Código Procesal Penal obliga a los proveedores 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" en 2017,[12] se produjo una discusión pública respecto a la expresión "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 hacen público el período por el cual retienen estos datos comunicacionales y su forma de eliminación.

Con todo, debe hacerse presente que actualmente existe un proyecto de ley que establece normas sobre delitos informáticos con el objeto de adecuarlos al Convenio de Budapest.[13] Dicho proyecto pretende aprobar los principales elementos contenidos por el "Decreto espía" a través de la ampliación de la definición de "datos relativos al tráfico" para incluir información no contemplada hoy en la ley, incluyendo la localización territorial de las comunicaciones. Del mismo modo, el proyecto pretende extender el período de retención de datos de tráfico de uno a dos años –al igual que el "Decreto Espía"– y mantiene que este sería un período mínimo y no máximo.

El artículo 224 del Código Procesal Penal señala que la medida de interceptación de comunicaciones 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 personas. 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

11 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.

12 "¿Qué dice el llamado 'Decreto Espía'?", https://www.derechosdigitales.org/11400/que-dice-el-llamado-decreto-espia/

13 Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25

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 Nº 142 de 2005), que se refiere a la obligación contenida en el Código Procesal Penal para que los proveedores 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 legal a considerar es el régimen de protección de datos personales en Chile. La ley nº 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 personales 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 bajas y no establece formas especiales de reparación. La ley protege solamente a personas naturales,[14] 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 compañías 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, tam-

14 JERVIS, P. 2006. Modelo de Propuesta Regulatoria al Mercado de Datos Personales en Chile. Revista Chilena de Derecho Informático 8. En línea, disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10787/11035 [Consultado el 24 de abril de 2018], pp. 152-155.

poco los prohíbe. Por lo mismo, la publicación de este tipo de documentos será considerado una buena práctica para efectos de este informe.

3.2. Empresas de telecomunicaciones

El año 2018 estuvo marcado por el crecimiento de la empresa WOM en el mercado de las telecomunicaciones, en particular, de la telefonía móvil. Luego de haber adquirido a Nextel el año 2015,[15] la participación de WOM en el mercado de la telefonía móvil ha aumentado de de un 3,5 % a un 19,4 % entre marzo de 2016 y diciembre de 2018.[16] Si bien WOM no provee servicios de internet fijo, su considerable participación como proveedor de internet móvil -método de conexión que explica el aumento en el acceso a internet durante los último años-[17] justifica su inclusión en la versión 2019 de este informe.

En cuanto a la participación de mercado del resto de las empresas de telecomunicaciones, el más reciente informe de la SUBTEL[18] muestra cómo el mercado ha evolucionado durante el último año. De acuerdo a las estadísticas de diciembre de 2018, las cuotas de mercado entre los diferentes ISP son las siguientes:

1. *Movistar.* Participación de mercado: 31,5 % del mercado de internet fijo y 23,7 % del mercado de internet móvil.
2. *VTR.* Participación de mercado: 38,7 % del mercado de internet fijo y 1,3 % del mercado de internet móvil.
3. *Claro Chile.* Participación de mercado: 14,1 % del mercado de internet fijo y 21,2 % del mercado de internet móvil.
4. *Entel.* Participación de mercado: 1,8 % del mercado de internet fijo y 33,2 % del mercado de internet móvil.
5. *GTD Manquehue.* Participación de mercado: 8,1 % del mercado de internet fijo y no cuenta con participación en el mercado de internet móvil.

15 Wayerwayer (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/

16 SUBTEL. Marzo 2019, Sector Telecomunicaciones, Cierre 2018. Disponible en: https://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf

17 A diciembre 218 la penetración de internet fija fue de 17,2 accesos por cada 100 habitantes, mientras que la penetración de Internet móvil 3G+4G alcanzó a 95,7 accesos por cada 100 habitantes. SUBTEL. Marzo 2019, Sector Telecomunicaciones, Cierre 2018. Disponible en: https://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf

18 SUBTEL. 2019. Sector Telecomunicaciones, Cierre 2018. En línea, disponible en: https://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf [Consultado el 16 de junio de 2019].

6. *WOM.* No cuenta con participación en el mercado de internet fijo y un 19,4 % del mercado de internet móvil.

Las seis compañías seleccionadas para este estudio representan una parte sustantiva del mercado de internet en Chile: un 94,2 % de los servicios fijos y 98,8 % de conexiones móviles.

Según cifras de diciembre de 2018, el 97,5 % de la población tiene acceso a internet, mayoritariamente a través de servicios móviles,[19] 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.

19 Según las mismas estadísticas de SUBTEL, solo el 49,4 % de la población cuenta con internet fija al hogar.

4.1. *WOM*

4.1.1. ¿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?

Al igual que el año pasado, la portada del sitio web de WOM tiene disponible la pestaña "Términos Comerciales, Contractuales y Transparencia", en donde es posible acceder a una versión tipo del Contrato de Servicio en formato PDF,[20] así como a los anexos de "Planes y Tarifas Multimedia", "Planes Solo Voz", "Planes Solo Datos" y "Planes y Tarifas Internet".[21] El sitio web presenta la información a través de una serie de pestañas que se expanden al hacer clic y resulta claro e intuitivo acceder a ellas.

El contrato tipo –que hace las veces de base para todo tipo de suministro de servicios– 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.[22] Dicha cláusula fue modificada respecto del año pasado, y ahora menciona específicamente que WOM respetará los mismos principios mencionados en la metodología de este informe; además, limita la finalidad en el uso de los datos a la entrega del servicio y el envío de publicidad y beneficios.[23] Del mismo modo, la cláusula octava se ha modificado para incluir un enlace a los términos y políticas de privacidad

20 WOM. Nuestro Contrato de Servicios. Disponible en: https://www.wom.cl/documents/20182/1049626109/Contrato+de+Servicios.pdf/b0d87ff6-9400-13ed-2368-8134db0c0fba [Consultado el 16 de junio de 2019].

21 WOM. Términos Comerciales, Contractuales y Transparencia. Disponible en: https://www.wom.cl/terminos_condiciones [Consultado el 29 de junio de 2019].

22 La cláusula octava del contrato establece que "WOM protege y asegura los datos personales de sus clientes garantizando que serán recolectados, almacenados y su tratamiento será utilizado para los fines propios asociados a la prestación del servicio contratado, como también para el envío de ofertas comerciales, publicidad y otros beneficios de WOM, dando estricto cuidado a los principios de licitud, acceso, calidad, finalidad, proporcionalidad, transparencia, confidencialidad, responsabilidad, no discriminación, seguridad, limitación de uso y minimización de datos. 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 call center. Wom declara tener una política de privacidad, la cual se encuentra publicada en www.wom.cl/terminos_condiciones, la cual podría modificarse en el futuro, sin perjuicio de que los clientes tendrán acceso a las versiones anteriores." [Consultado el 23 de marzo de 2018].

23 Vale la pena mencionar que durante el proceso de redacción de este informe a todas las empresas estudiadas se les hace llegar un borrador de la metodología, de forma tal que puedan entregar retroalimentación respecto a los criterios que se utilizará para evaluar su desempeño.

de WOM, estableciendo que de modificarse, las versiones anteriores seguirán disponibles para el usuario. Esto permite al cliente comparar las políticas y condiciones de privacidad que estaban vigentes al momento de contratar con la versión actual.

Los anexos de "Planes y Tarifas Multimedia", "Planes Solo Voz", "Planes Solo Datos" y "Planes y Tarifas Internet" complementan el contrato tipo en cada uno de los servicios referidos. 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" existe un menú desplegable, en donde se describe en términos sencillos el contenido de la política de privacidad. En ese mismo menú se pueden encontrar tres enlaces: la política de privacidad, versiones anteriores de la política de privacidad y la política de contactabilidad.

Respecto al contenido de la política de privacidad, la versión vigente al cierre de este informe corresponde a junio de 2019 y también es posible acceder a las versiones anteriores, las que cuentan con una fecha de entrada en vigencia. En su preámbulo se señala qué se entiende por datos personales y se establece que la política es aplicable para el sitio web de WOM, los distintos canales de comunicación y todos los servicios que ofrece la empresa.

Al igual que el contrato tipo, la política menciona todos los principios contenidos en la metodología de este informe, los cuales se encuentran redactados en términos de compromiso y no como meros elementos de interpretación. Así, respecto al *principio de licitud* se señala que los datos de los usuarios serán tratados *"solo en aquellos casos en que se encuentre habilitada por la ley o cuente con el consentimiento expreso del titular de los mismos"*. En cuanto al *principio de finalidad*, la política establece que WOM *"solo solicitará cierta información personal en la medida necesaria para el objeto de establecer o perfeccionar la relación y comunicación con sus clientes y usuarios, así como también para mejorar la calidad de nuestro servicio"*.

WOM también se compromete a que la recolección de datos personales no puede ser hecha de modo inespecífico o excesivo, o afectar los derechos del titular, dando sustento al *principio de proporcionalidad*. Relacionado con este principio está el *principio de minimización de datos,* respecto al cual la empresa se compromete a recoger solo los datos necesarios para la finalidad de su tratamiento. En cuanto al *principio de confidencialidad,* la política establece un compromiso expreso respecto a mantener reserva de los datos de los usuarios y advierte a sus usuarios que solo compartirá sus datos con terceros cuando la ley así lo ha facultado, cuando el titular ha consentido

expresamente o cuando es requerido por la autoridad en cumplimiento de los requisitos legales. Si bien existe un compromiso robusto, el uso del término "cuando la ley así lo ha facultado" resulta bastante abstracto y poco determinado.

El *principio de seguridad* cuenta con su propio apartado, en el cual WOM se compromete a mantener constantemente medidas de seguridad para el tratamiento de tus datos y tomar los resguardos necesarios para que se cumpla el deber de confidencialidad.

El *principio de calidad* también se encuentra recogido, al existir una mención expresa a que los datos personales que almacenen deben ser exactos, completos y actuales en relación con los fines de su tratamiento. Así como el *principio de responsabilidad*, respecto al cual WOM se compromete a responder en caso de incumplir alguno de los principios antes mencionados.

Por último, WOM informa a sus usuarios que en cualquier momento pueden hacer efectivo su derecho a acceder, rectificar, cancelar u oponerse al tratamiento de datos personales, y establece un correo electrónico específico para hacer llegar estas solicitudes de acuerdo a la ley Nº 19.628.

En razón de lo anterior, la empresa obtiene una estrella.

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. En esta sección se encuentran disponibles los informes correspondientes al año 2018 y 2019.[24] El informe de 2019 es bastante más sustantivo que su símil del año anterior.

El informe de 2019 divide la información entregada en dos categorías: 1) Total de interceptaciones año 2018, y 2) Total solicitudes de información año 2018. Respecto a la primera categoría, el informe señala que se realizó un total de 3.850 interceptaciones. Sin embargo, a diferencia del año pasado, el documento sí señala que un total de siete interceptaciones fueron rechazadas por incumplimiento de requisitos legales. Estas luego fueron subsanadas, por lo que se les dio curso.

Respecto a la segunda categoría, WOM declara haber recibido un total de 12.035 "solicitudes de información" durante el año 2018, de las cuales 25 fueron rechazadas por incumplimiento de requisitos legales. Al igual que el año pasado, la categoría no se encuentra definida de

24 WOM. Informe de Transparencia año 2019, disponible en: https://www.wom.cl/documents/20182/1049626039/Informe+de+Transparencia+2019.pdf/a443cf2b-150d-f499-9890-8e7c1d6e3714 [Consultado el 29 de junio de 2018].

forma precisa, y solo se establece 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.

Al contener la misma categoría tipos de información tan variados como datos asociados al RUT del usuario y tráfico asociados a las líneas telefónica no es posible tener una idea clara de qué porcentaje de estas solicitudes son de carácter intrusiva, como aquella contenida en el inciso quinto del artículo 222 del Código Procesal Penal. Sin embargo, el mismo informe establece que para el próximo año pretenden contar con tres categorías: Interceptaciones, Solicitudes de Información (artículo 222, inciso quinto) y Solicitudes de Otros Datos. Lo anterior da cuenta de una intención positiva de mejorar sus niveles de transparencia, especialmente teniendo en consideración que se trata de una empresa relativamente nueva en el mercado.

Por último, el informe cuenta con un desagregado por región respecto a las solicitudes de interceptación, el cual muestra que casi un 50 % de las interceptaciones son realizadas en la región metropolitana.

La compañía recibe una estrella. Si bien la información podría estar mejor categorizada, el informe tiene gran cantidad de información y la empresa se compromete expresamente a mejorar la categorización para la próxima versión de su informe de transparencia.

4.1.3. ¿Notifica la empresa a los usuarios acerca de solicitudes de información del Gobierno?

WOM también presenta avances en esta categoría. En el Protocolo de Entrega de Información a la Autoridad[25] la empresa declara que "*se reserva el derecho a notificar a los usuarios una vez que expire el plazo de reserva de la diligencia de la investigación y cuando el usuario no fuera formalizado luego de cumplido el plazo de investigación, siempre que el éste* [sic] *sea identificable –para efectos de la verificación de identidad– y se cumplan los demás requisitos legales.*" No queda claro en qué casos WOM notificará a los usuarios y en qué casos no, ya que solo se reserva el derecho a realizar dichas notificaciones y no se compromete a hacerlo.

25 WOM. Protocolo de Entrega de Información a la Autoridad. Disponible en: https://www.wom.cl/documents/20182/1049626096/Protocolo+Entrega+Informaci%C3%B3n+Autoridad+2019.pdf/2e6bc2ae-a2bf-0acc-985d-b9fa873e46ca [Consultado el 29 de junio de 2019].

Por otro lado, en el documento que contiene el informe de transparencia 2019 también se hace referencia a esta categoría. WOM señala que "*ha iniciado un diálogo con las autoridades –principalmente con el Ministerio Público–, para explorar la vía por la cual se pueda notificar a los usuarios acerca de las solicitudes de acceso a su información personal y/o interceptaciones, por parte de los organismos autorizados por ley. En el mes de marzo de 2019 se hizo presente el requerimiento al Ministerio Público, por lo que esperamos poder contar con avances antes de que concluya el primer semestre de 2019*". Si bien al momento del cierre de este informe este sistema aún no ha sido implementado, resulta positivo que la empresa esté tomando medidas concretas y tenga entre sus planes establecer un mecanismo para notificar a sus usuarios cuando hayan sido objeto de una diligencia intrusiva.

Por ello, la compañía obtiene media estrella.

4.1.4. ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que el gobierno 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 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 2019, dando a entender que se informará la fecha en que es modificado o actualizado. Este documento es una versión ligeramente modificada de la vigente en el año 2018.

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: Código Procesal Penal (artículos 9, 219, 222 y 223); decreto 142 de 2005 del Ministerio de Transportes y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación; ley Nº 19.974, sobre Sistema Nacional de Inteligencia; entre otras.[26]

Respecto de la interceptación de comunicaciones, el protocolo establece que esta 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

26 ibid.

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 exija explícitamente que se adjunte la autorización judicial que ordena la diligencia de interceptación de comunicaciones, pues es un requisito establecido explícitamente por el Código Procesal Penal. 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, adjuntando la resolución judicial correspondiente. Esto es particularmente positivo, ya que entendemos 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.

La principal modificación de este año es que el documento ya no admite la posibilidad de acceder a una solicitud de acceso a información sin adjuntar la orden judicial de forma previa en casos de urgencia. De esta forma, se señala que "*en casos urgentes, podrá realizar la solicitud siempre desde el correo institucional, poniendo en copia al fiscal de la causa. Sin perjuicio de lo anterior, deberá acompañar la resolución judicial*".

WOM obtiene una estrella en esta categoría.

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

Si bien no existen antecedentes de que WOM haya recurrido a tribunales de justicia para defender la privacidad de sus usuarios, la sec-

27 Cabe interpretar que por "información de tráfico" el protocolo 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.

ción en donde se encuentra su Protocolo de Entrega de Información a la Autoridad hoy transparenta los oficios que la SUBTEL ha realizado a la empresa solicitando información y antecedentes para el año 2018 y 2019.

Junto al enlace correspondiente al mes de mayo de 2019, que redirige al Oficio Ordinario Nº 5714,[28] se encuentra un enlace a una declaración pública. En ella WOM declara que parte importante de lo solicitado por el regulador - en particular información relativa a la ubicación de sus usuarios y el listado detallado del tráfico de datos de sus usuarios - son información de carácter personal y la empresa no se encuentra autorizada para divulgarla, por su carácter confidencial.[29] Esto da cuenta que si bien WOM no ha recurrido a tribunales en la materia, sí ha transparentado al menos un caso en donde ha defendido los datos personales de sus usuarios en procesos administrativos ante el regulador.

WOM obtiene media estrella en esta categoría.

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 pasado, 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 ancha fija para hogares[30] y para el servicio de telefonía móvil y banda ancha móvil.[31]

En esta misma pestaña es posible encontrar las distintas condiciones contractuales. Por ejemplo, se encuentra disponible el documento

28 El oficio puede se encuentra disponible en el siguiente enlace: https://www.wom.cl/documents/20182/1049626057/Oficio+Ord.+5714+de+2019.pdf/63fa6e7f-7b92-bd89-3993-8734eede4beb [Consultado el 29 de junio de 2019].

29 La declaración de WOM se encuentra disponible en el siguiente enlace: https://www.wom.cl/documents/20182/1049626057/Declaraci%C3%B3n+por+Oficio+Ordinario+5714+de+2019.pdf/73d417e6-01d9-eaaa-c64c-b370c12eddca [Consultado el 29 de junio de 2019].

30 Movistar Chile. Condiciones Comerciales y Contractuales de servicio hogar. Disponible en: https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-hogar/ [Consultado el 30 de junio de 2019].

31 Movistar Chile. Condiciones Comerciales y Contractuales de telefonía y banda ancha móvil. Disponible en: https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/ [Consultado el 30 de junio de 2019].

"Condiciones contractuales del servicio telefónico móvil"[32] y el documento "Condiciones contractuales del servicio telefónico fijo".[33] En ambas es posible encontrar una cláusula muy escueta y abstracta, que da cuenta que el tratamiento de datos personales se realizará de acuerdo a lo establecido por la Ley Nº 19.628.[34]

Asimismo, el documento titulado "Política de Privacidad Movistar"[35] no cuenta con una fecha de entrada en vigencia, pero parece no haber sido actualizado desde la publicación de la versión 2017 del presente informe. 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 de la mencionada política, lo que no facilita a los usuarios su conocimiento.

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:

1. Nombre.
2. Apellido paterno.
3. Apellido materno.
4. R.U.T.
5. Nº serie cédula.
6. Fecha de nacimiento.

32 Movistar Chile. Condiciones Contractuales del Servicio de Banda Ancha Fija Prepago. En línea, disponible en: https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/pdf/CondicionesContractualesTelefonicoMovil.pdf [Consultado el 29 de junio de 2019].

33 Movistar Chile. Condiciones Contractuales del Servicio de Banda Ancha Móvil. En línea, disponible en: http://www.movistar.cl/PortalMovistarWeb/ShowDoc/WLP+Repository/Portlets/P030_Generico/Documentos/BAM_1 [Consultado el 23 de marzo de 2018].

34 En ambas se encuentra disponible la siguiente cláusula: "*El Cliente acepta que sus datos personales informados producto de la contratación del Servicio podrán ser tratados y/o utilizados por TCH, de conformidad a lo dispuesto en la Ley N° 19.628, sobre Protección de Datos de Carácter Personal, para su adecuada atención comercial*".

35 Movistar Chile. Política de Privacidad Movistar. En línea, disponible en: https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/pdf/Politica_de_Privacidad_Movistar.pdf [Consultado el 29 de junio de 2019].

7. Número telefónico.
8. Dirección particular y/o comercial.
9. 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 que el artículo 222 del Código Procesal Penal obliga a las empresas a conversar, 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, incorpore menciones a alguna medida destinada a evitar violaciones a la privacidad. En consecuencia, es posible apreciar que 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.

En cuanto a los principios mencionados en la metodología, solo es posible argumentar que Movistar recoge parcialmente el *principio de licitud*, al señalar que se sujetará a las disposiciones de la ley N° 19.628, sobre Protección de datos de carácter personal y el *principio de finalidad* al establecer que la empresa solo va a procesar datos para finalidades permitidas por el ordenamiento jurídico. En otras palabras, Movistar se compromete simplemente a cumplir con la legislación vigente en materia de protección de datos personales.

El hecho de que dentro de los datos recolectados se encuentre el número de serie de la cédula de identidad da cuenta que los términos y condiciones de Movistar no tienen en consideración el *principio de minimización de datos* y el de *proporcionalidad*, ya que la recolección de ese dato no se justifica respecto a la entrega del servicio de telecomunicaciones. De hecho, ninguna otra empresa del informe lo recolecta.

La empresa obtiene un cuarto de estrella en esta categoría.

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, alojado en el sitio web de su matriz internacional.

El informe de sostenibilidad del año 2018 no ha sido publicado a la

36 Telefónica Chile. Informe de Sostenibilidad. En línea, disponible en: http://www.telefonicachile.cl/telefonica-y-sociedad/informe-de-sostenibilidad/[Consultado el 29 de junio de 2019].

fecha de redacción de este informe, por lo que la última versión corresponde al año 2017, la misma que fue analizada en la versión anterior de Quién defiende tus datos.[37] Esta versión no contempla información sobre vigilancia de las comunicaciones, ni ninguno de los demás puntos considerados en la respuesta modelo. Con todo, resulta destacable que dicho informe manifieste el interés de la compañía 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 compañía, pero que están destinados a reflejarse en la relación de ellos con todos 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.

Movistar tampoco ha avanzado en contar con una promoción local de su informe de transparencia. El reporte "Informe de Transparencia en las Comunicaciones" alojado en el sitio internacional de Movistar ha sido actualizado a su versión de 2018.[38] Al igual que en su versión 2017, 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 las solicitudes para suspender temporalmente el servicio.

El informe establece que, en 2018, Movistar Chile recibió 10.382 solicitudes de interceptación de comunicaciones (2.098 menos que en el año 2017),[39] de las cuales 54 fueron rechazadas, 23.889 de acceso

37 Ibíd., 2015. Informe de Sostenibilidad 2015. En línea, disponible en: http://www.telefonicachile.cl/wp-content/uploads/2016/04/informe-2015.pdf [Consultado el 29 de junio de 2019].

38 Documento disponible en: https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2018.pdf/5a54f445-e95f-4b71-e549-e9f6d1eb5b7d [Consultado el 30 de junio de 2019].

39 Este año la cifra se encuentra desagregada entre tipos de acceso: 1.326 de telefonía fija y 9.056 de telefonía móvil.

a metadatos (18.795 menos que en 2017), de las cuales 286 fueron rechazadas y ninguna solicitud para bloqueo y filtrado de determinados contenidos (al igual que el año anterior). El informe de este año busca también dar cuenta del número de personas afectadas y no solo el número de solicitudes, pero llega a la conclusión de que no es posible estimar la cantidad de personas afectadas debido al uso de tarjetas de prepago sin titular registrado.

En definitiva, Movistar todavía publica su informe de transparencia en el sitio web internacional de la empresa, la que liberó estadísticas actualizadas y más específicas relativas a las solicitudes de interceptación, solicitud de información y bloqueo de sitios web respecto de los usuarios chilenos. Sin embargo, estas estadísticas no son publicadas en el sitio chileno de Movistar, por lo cual pueden resultar de difícil acceso para los usuarios nacionales, incluidos sus clientes actuales o potenciales.

A pesar de lo anterior, la información transparentada por Movistar a nivel internacional sigue siendo una de las más precisas en el mercado, por lo que todavía es posible asignar cierto puntaje en este ítem. Es de esperar que Movistar Chile empiece a mostrar el mismo avance en transparencia que su matriz.

Movistar recibe tres cuartos de estrella en esta categoría.

4.2.3. ¿Notifica la empresa a los usuarios acerca de solicitudes de información del Gobierno?

Al igual que en la versión anterior de este informe, no ha sido posible encontrar públicamente información referida a este punto. En los términos contractuales y comerciales de los servicios fijo y móvil –incluidas las políticas de privacidad existentes– no se menciona nada al respecto, 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 información en el sitio web de la empresa.

La empresa no recibe estrella en esta categoría.

4.2.4. ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que el Gobierno 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.

Por ello, la empresa no obtiene estrella en este ítem.

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

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

La empresa no obtiene estrella en este punto.

4.3. *VTR*

4.3.1. ¿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?

Al igual que el año pasado, 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 las modalidades de prepago y plan),[40] los que contienen cláusulas relativas a las políticas de datos personales. El acceso es bastante sencillo e intuitivo, y su contenido no ha cambiado desde el año pasado.

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.

La sección 13.1 del documento se refiere al registro estadístico del uso de los servicios por parte de los clientes, con el fin de mejorar los servicios provistos por VTR. La sección 13.2 alude al registro y análisis de la información personal de cada cliente, con la finalidad de entregar los servicios contratados, como el registro de las llamadas a números móviles o el arriendo de películas en VOD. Se establece qué información será tratada por VTR o por terceros. Por ejemplo, si VTR encarga a una empresa externa el servicio de cobranza.

Por último, la cláusula 13.3 establece que, al momento de contratar,

40 VTR. Revisa las Condiciones Contractuales y Comerciales de los Servicios VTR. En línea, disponible en: http://vtr.com/productos/moviles/contratos [Consultado el 30 de junio de 2019].

41 VTR. Solicitud de Suministros de Servicios de VTR. En línea, disponible en: http://vtr.com/CS/vtr_f3/contrato-de-suministro.pdf y VTR. Condiciones de Suministro de Servicios Móviles. En línea, disponible en: http://vtr.com/CS/vtr_f3/condiciones_de_suministro_de_servicios_moviles1.pdf [Consultado el 30 de junio de 2019].

el cliente autoriza a VTR para tratar sus datos de contacto, servicios y comportamiento, para que VTR o terceros puedan hacerle ofertas comerciales. En caso de ser terceros quienes envíen información comercial al cliente, estos deben informarle la naturaleza de la asociación comercial con VTR.

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.

Al tratarse de un contrato de adhesión, resulta preocupante que la cláusula 13.3 establezca que al momento de contratar el cliente autoriza a que terceros puedan acceder a sus datos de contacto, incluso si se le entregan facultades al cliente para poner término a este tipo de comunicaciones. Esta modalidad contrasta con la de WOM y el Entel, que solo admiten que sus empresas relacionadas utilicen los datos de sus usuarios para actividades comerciales y limitan estas actividades de publicidad a aquella relacionada con la misma empresa que presta el servicio.

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 Nº 19.628. Del contenido del contrato, solo es posible evidenciar que existen referencias indirectas al *principio de finalidad,* al señalarse los usos que VTR le puede dar a los datos de los usuarios, y el *principio de confidencialidad,* al existir un compromiso de VTR que de entregarse información personal a terceros se hará velando porque se apliquen adecuados estándares de confidencialidad.

Por su parte, VTR también tiene publicado un apartado destinado exclusivamente a comunicar su política de privacidad.[42] Este subsitio contiene una introducción, en donde VTR reafirma su compromiso con la privacidad de los usuarios. En este párrafo puede encontrarse una alusión indirecta al principio de licitud, al señalarse que la política rige para la forma en que VTR tratará los datos personales de sus usuarios, a menos que estos entreguen su consentimiento expreso para obrar de forma distinta.

El apartado consiste en distintas pestañas desplegables. La primera define qué entiende VTR por datos personales, realizándose una interpretación amplia del concepto y mencionando explícitamente los datos de tráfico, direcciones IP y uso de internet (registro de navegación) como datos personales.

42 VTR. Política de privacidad del consumidor. En línea, disponible en: https://vtr.com/productos/privacidad [Consultado el 30 de junio de 2019].

La siguiente sección establece cuáles son los datos que VTR recolecta. Entre ellos se señala la información de contacto del usuario (nombres, dirección, números de teléfono, correo electrónico, nombres de usuario, edad, género, preferencias de lenguaje, detalles de envío), la información de la cuenta bancaria del usuario (para efectos de pago), información necesaria para entregar el servicio (versión del software usada, smartcard ID, IP/dirección de Mac, y paquetes de servicio), información estadística respecto de cómo los usuarios están usando los servicios y otra información personal, que puede ser entregada voluntariamente por el usuario u obtenida de fuentes accesibles al público. De esta forma, es posible argumentar que VTR recoge indirectamente el *principio de proporcionalidad* al no recolectar datos excesivos o innecesarios.

La tercera pestaña informa con qué propósito VTR utiliza la información recolectada, abordando directamente el *principio de finalidad*. En el documento, VTR informa que los datos personales de sus usuarios podrán ser utilizados para cumplir su obligaciones legales, mejorar sus servicios y proveer sus productos o servicios. También se informa que se utilizará esta información para gestionar el desempeño de sus servicios y presentar al cliente nuevos productos.

Al igual que en lo establecido en las cláusulas de sus contratos, esta comunicación comercial puede referirse a productos de VTR, pero también de terceros, en este caso, sus "socios estratégicos". Esta entrega de información a terceros parece estar restringida en el siguiente párrafo, en donde se establece que se realizará cuando el cliente elige participar de una oferta o transacción especial presentada por VTR, pero suministrada por alguno de estos socios.

El apartado también cuenta con una pestaña dedicada al principio de seguridad, en donde VTR se compromete a implementar distintas medidas técnicas para el resguardo de la información personal, entre ellas "protección de contraseñas, encriptación, firewalls, antivirus, sistema de detección de intrusos, detección de anomalías y control de accesos para nuestros empleados".

El *principio de calidad* también se encuentra recogido en una pestaña especial, al señalarse que si algún dato se encuentra incompleto, incorrecto, desactualizado o es innecesario, VTR lo corregirá en cuanto les sea posible.

VTR también entrega un correo de contacto específico para que sus usuarios hagan efectivo su derecho a acceso, rectificación, cancelación u oposición. Por último, la política no cuenta con una fecha de publicación o versión que le permita a los usuarios comparar la política actual con aquella que estaba vigente al momento de contratar el servicio.

La empresa recibe media estrella. Si bien cuenta con una política de privacidad, esta no aborda todos los principios contenidos en la metodología y tampoco cuenta con una fecha de publicación.

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

Un aspecto en el que VTR sí ha avanzado es el de publicar un informe de transparencia. Este puede encontrarse en el sitio web de la compañía.[43] A pesar de que el documento no está fechado, puede deducirse que es del año 2019, ya que hace referencia al total de solicitudes del año 2018.

De esta forma, el documento muestra que durante 2018 VTR recibió 144 solicitudes de interceptación telefónica. Resulta positivo que esta información esté desagregada en tipos de comunicación (10 de telefonía fijo y 134 de telefonía móvil). Sí llama la atención el bajo número de solicitudes de información en proporción a la participación de mercado de VTR, mientras que las otras empresas suelen recibir varios miles de solicitudes de interceptación al año.

La segunda categoría es denominada "solicitudes de información", la que se subdivide en dos categorías:

a. Solicitudes de acceso a tráfico telefónico.

1. Tráfico de llamadas Fono Fijo: 35
2. Tráfico de llamadas Fono Móvil: 120
3. Tráfico de antenas: 18
4. Información relativa a IP, MAC, Tráfico de IMEI: 274

b. Solicitudes de otros datos.

1. Información de IMEI de equipos telefónicos móvil: 503
2. Información de clientes: 404
3. Copias de contrato de servicios: 171
4. Copia de grabación de cámaras de seguridad: 3

Es decir, VTR recibió un total de 447 solicitudes de información relativas al tráfico telefónico (incluyendo los datos de tráfico o metadatos de navegación del usuario) y 1081 relativas a información de titularidad del cliente. Resulta interesante la granularidad con que la cantidad de solicitudes de información se encuentra presentada. Un total de nueve categorías de solicitud es informada, lo que entrega una noción muy precisa de los tipos de requerimientos que la autoridad realiza a las empresas de telecomunicaciones.

43 Disponible en: https://vtr.com/img/documents/Informe-de-Transparencia.pdf [Consultado el 3 de julio de 2019].

La información no se encuentra desagregada por región o por mes del año, pero sí da cuenta de la cantidad de solicitudes rechazadas. De acuerdo al documento, la totalidad de las solicitudes cumplían con los requisitos legales, por lo cual no se rechazó ninguna.

En atención a lo lo desagregada que se encuentra la información respecto del tipo de solicitud y que se da cuenta de la cantidad de solicitudes rechazadas, VTR obtiene una estrella en esta categoría.

4.3.3. ¿Notifica la empresa notifica a los usuarios acerca de solicitudes de información del Gobierno?

A diferencia del año pasado, hoy VTR hace referencia explícita a la posibilidad de notificar sus clientes respecto de una medida intrusiva que le haya afectado. De esta forma, en el documento titulado "Protocolo de Entrega de información a la Autoridad, 2019", el último párrafo señala que "*VTR se reserva el derecho de notificar a sus clientes una vez que expire el plazo de reserva de la diligencia de la investigación y cuando el cliente ni fuera formalizado, luego de cumplido el plazo de investigación*".[44]

De esta forma –al igual que con WOM– no queda claro en qué casos VTR notificará a los usuarios y en qué casos no, ya que solo se reserva el derecho a realizar dichas notificaciones, pero no se compromete a hacerlo. Por otro lado, a diferencia de WOM, VTR no ha señalado que se encuentra en proceso de establecer un mecanismo para hacer efectiva esta posibilidad.

Por ello, la compañía obtiene un cuarto de estrella.

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

Otro punto en el que VTR ha avanzado en relación al informe anterior es en la publicación de un Protocolo de Entrega de información a la autoridad, el que se encuentra disponible en su sitio web.

Este documento establece de forma bastante detallada el procedimiento que la autoridad deberá cumplir para solicitar información personal de los usuarios de VTR. A diferencia del informe de transparencia, en este caso los tipos de datos a solicitar se encuentran en tres categorías: 1) solicitudes de interceptación telefónica, 2) solicitudes de información que dice relación con tráficos telefónicos y 3) solicitudes de información que dice relación con otros datos.

44 Documento disponible en: https://vtr.com/img/documents/Protocolo-de-Entrega-de-informaci%C3%B3n-a-la-Autoridad.pdf [Consultado el 3 de julio de 2019].

Resulta positivo el nivel de detalle en los requisitos que la autoridad debe cumplir para que una solicitud resulta válida, estableciéndose un canal oficial para el procesamiento de los requerimientos y exigiendo expresamente que se adjunte una orden judicial previa, tanto para las solicitudes de interceptación telefónica como el acceso a datos de tráfico (metadatos). Del mismo modo, VTR señala que de no cumplirse todos los requisitos, le hará saber las falencias de la solicitud a la autoridad para que sean subsanadas.

Por último, también resulta positivo que al regularse los casos en donde se le debe dar una tramitación urgente a la solicitud de información, también se exija que se adjunte la orden judicial correspondiente.

VTR obtiene una estrella en esta categoría.

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

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

En años anteriores a VTR se le había otorgado un porcentaje de puntuación, ya que su política de privacidad contenía un párrafo en donde se establecía que "VTR se reserva el derecho a cuestionar el acceso a información personal a las autoridades". Sin embargo, hoy son varias las empresas que cuentan con este tipo de declaraciones y también existen empresas que han realizado defensas administrativas y judiciales de la privacidad de sus usuarios.

Por tanto, en base a los cambios en los parámetros metodológicos para la actual versión de este informe, VTR no obtiene estrella.

4.4. Claro Chile

4.4.1. ¿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?

El sitio web de Claro Chile fue modificado este año y hoy concentra toda la información respecto a la privacidad de sus usuario en un enlace denominado "Protección de Datos".[45] En este menú existen pestañas desplegables intuitivas y fáciles de utilizar, que le entregan al usuario acceso a la política de privacidad, su informe de transpa-

45 Disponible en: https://www.clarochile.cl/personas/proteccion-de-datos/ [Consultado el 30 de junio de 2019].

rencia, información sobre la relación de la empresa con la autoridad y demás notificaciones a los clientes de Claro.

En la pestaña de términos y condiciones de privacidad es posible ver que Claro presenta enlaces no solo para la política vigente, sino que también para políticas anteriores, ordenadas por versión y por fecha.

La versión vigente corresponde a la versión número 1.2, de mayo de 2019. El contenido de la política hace referencia explícita a los ocho principios contenidos en la metodología de este informe. Sin embargo, es posible encontrar referencias a la concreción de los mismos en otras disposiciones sustantivas del documento.

Así, el *principio de licitud* es referido al comprometerse la empresa a solo efectuar tratamiento de datos personales respecto de aquellos que han sido entregados voluntariamente por los clientes y/o usuarios a través del sitio web www.clarochile.cl, o de cualquier otro medio de acuerdo a sus políticas de privacidad. Del mismo modo, Claro establece que estos datos podrán ser utilizados exclusivamente para proveer de productos o servicios, personalizar la experiencia del usuarios, entregar información sobre productos y ofertas, y para fines estadísticos, entregando sustento al *principio de finalidad.* Vale la pena mencionar que en el caso de entregar información a terceros para efectos de márketing, esta finalidad se encuentra debidamente circunscrita al objeto de entregar información o beneficios de Claro. Asimismo, se concreta el *principio de minimización de datos* al existir un compromiso expreso de que los datos recolectados serán únicamente aquellos necesarios para el cumplimiento de los fines antes mencionados.

Claro también transparenta la información del usuario que puede ser recolectada, almacenada y procesada. De esta forma el documento menciona "*la información asociada a la cuenta de usuario, información respecto al dispositivo mediante el cual se hace uso del sitio, información sobre la dirección IP del usuario, y aquella recopilada a través del uso de cookies, u otras herramientas analíticas".* Como es posible, toda esta información parece pertinente y relevante, cumpliendo de esta forma con el mandato del *principio de proporcionalidad.*

El *principio de confidencialidad* también es recogido de forma explícita. Claro declara que mantiene estricta reserva y confidencialidad respecto de los datos personales de sus clientes y que los datos personales de sus usuarios solo son entregados a la autoridad cuando se cumplan todos los requisitos legales correspondientes.[46] Relacionado a la confidencialidad, Claro se compromete a establecer las

46 Claro incluso va más allá, al señalar "sin perjuicio de lo anterior, Claro, podrá objetar 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".

debidas políticas de seguridad y controles destinados a velar por la confidencialidad de los datos personales, cumpliendo de esta forma con el *principio de seguridad*.

El *principio de calidad* se menciona en el documento, al señalar que los datos personales que voluntariamente han entregado los clientes deben ser correctos, exactos y completos, debiendo estar actualizados de acuerdo a los fines para los cuales se hayan recopilado. Del mismo modo, Claro da cuenta del *principio de responsabilidad* al señalar que se obliga a mantenerlos actualizados a solicitud del cliente o en caso de que tome conocimiento sobre algún error en los mismos. Además, la empresa señala que es legalmente responsable del cumplimiento de los principios, obligaciones y deberes conforme a la ley.

Respecto al ejercicio de los derechos por parte de los usuarios, el documento establece que en todo momento, y de forma gratuita, podrá solicitar el acceso, rectificación, cancelación y oposición respecto de sus datos personales. Del mismo modo, establece un correo electrónico específico para que los usuarios puedan hacer llegar sus solicitudes.

En cuanto a sus contratos, estos se encuentran disponibles en su sitio web, sin embargo el documento más relevante es el "Anexo de contrato de suministro de servicios de telecomunicaciones".[47] El contenido de este documento se aplica a todos los otros contratos y cuenta con una sección especial sobre protección de datos personales. En ella, se hace referencia específica a que se atiene al contenido de la política de privacidad, pero también menciona el ejercicio del derecho a acceso, rectificación, oposición y cancelación, así como a los principios de legitimidad, acceso, información, calidad de los datos, finalidad, proporcionalidad, transparencia, no discriminación, limitación de uso y seguridad en su tratamiento.

Por último, Claro señala que su política de privacidad puede modificarse a futuro, pero que esta modificación será debidamente notifica al usuario. Del mismo modo, se compromete a mantener en línea las versiones anteriores del documento, de forma tal que los usuarios puedan comparar cómo han sido modificadas sus condiciones de privacidad.

El proveedor obtiene una estrella.

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

A diferencia del año pasado, Claro hoy cuenta con documentos

47 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/SSTMmovil%20personaspyme(1)_20190620.pdf [Consultado el 30 de junio de 2019].

distintos para su informe de transparencia y su protocolo de entrega de información a la autoridad.[48] El informe de transparencia del año 2019 es una versión mucho más acabada y estructurada que su versión anterior.

En el documento, la información entregada se presenta en tres categorías distintas: 1) Solicitud de información general (titularidad, domicilio, IMEI, etcétera), 2) Solicitudes de interceptación telefónica, y 3) Metadatos (IP, tráfico, georreferenciación). Esta forma de categorizar la información es la más rigurosa entre las empresas estudiadas en este informe.

La información se encuentra desagregada por zona (norte, centro y sur) y la información del año 2019 (meses de enero, febrero y marzo) y por región. Asimismo, también se comunican la cantidad de solicitudes rechazadas en cada categoría.

De esta forma, el documento muestra que durante el año 2018 se hicieron un total de 32.288 solicitudes de información general, 5.958 solicitudes de interceptación telefónica y 6.101 solicitudes de acceso a metadatos. Como es posible apreciar, la forma en que se encuentra desagregada la información permite dar cuenta por primera vez que la cantidad de solicitudes de metadatos es un número muy similar a la cantidad de interceptaciones telefónicas. En los informes de transparencia de otras empresas este dato no aparece, al encontrarse esta información mezclada con "otros tipos de solicitudes".

Respecto a la cantidad de solicitudes rechazadas, lamentablemente estas no se encuentran divididas por tipo de solicitud, pero el documento da cuenta de que fue un total de 1783 requerimientos rechazados, una cifra significativa.

Por último, de forma bastante novedosa, Claro muestra cuáles han sido las principales causales para rechazar requerimientos de información o interceptación telefónica, las cuales suelen ser de carácter formal.

Claro Chile obtiene una estrella al contar con el mejor informe de transparencia de las empresas estudiadas.

4.4.3. ¿Notifica la empresa a los usuarios acerca de solicitudes de información del Gobierno?

En el documento titulado "Política de requerimientos de informa-

48 De todas formas, el documento del año 2018 se encuentra disponible en la misma sección. Esto es positivo, ya que permite a los usuarios comparar la cantidad de solicitudes por año. Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/politica-requerimiento-de-informacion-transparencia-2018_20190605.pdf [Consultado el 30 de junio de 2019].

ción", Claro se reserva el derecho de notificar a los usuarios cuando la autoridad ha solicitado datos personales de los mismos, en caso de no existir un deber de confidencialidad o reserva respecto del requerimiento de información, o que el plazo de la misma haya expirado.

Adicionalmente, en la sección "Demás notificaciones a los Usuarios y/o Clientes Claro" la empresa señala expresamente que "*como parte de su política de protección de los datos personales, ha establecido el proceso de notificación a los Usuarios y/o Clientes, que hayan sido objeto de requerimientos de información mediante resolución judicial emitida por parte de los tribunales de justicia (Civiles/Laborales/de Familia, Etc). En cualquier caso, dichas notificaciones se practican siempre y cuando no exista el deber legal de confidencialidad o reserva de la información".*

En la misma sección se encuentra un enlace a una carta tipo que Claro pretende utilizar para notificar a los usuarios.[49] La carta es bastante sencilla, solo señalando el RUC de la causa, la fecha de realización de la diligencia y el hecho de que Claro accedió a la medida por encontrarse legalmente obligado.

Sin embargo, este compromiso de notificar a los usuarios solo es aplicado en causas civiles, laborales y de familia, en donde las solicitudes de información a las empresas de telecomunicaciones suelen ser relativas a datos de titularidad, como RUT, nombre y dirección. Al no incluir las solicitudes de tribunales penales, en donde las diligencias suelen ser de carácter más intrusivo, no es posible asignar a Claro la calificación máxima. No obstante, este compromiso de notificar a los usuarios representa un paso en la dirección correcta y da cuenta que Claro se ha atrevido a avanzar en esta materia más que cualquier otra empresa del mercado.

Claro Chile recibe tres cuartos de estrella en este ítem.

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

Como se había adelantado, este año los requisitos que Claro exige a la autoridad se encuentran en un documento especial, denominado "Política de requerimiento de información", el que tiene fecha de publicación de junio de 2019.

El documento de este año es bastante más específico respecto de los requisitos. De esta forma, para solicitar datos de tráfico o georeferen-

49 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/notificacion-modelo-kgd_20190605.pdf [Consultado el 30 de junio de 2019].

ciación del usuario, la autoridad debe contar con una orden judicial previa, emanada de un Tribunal de la República, en la que se identifique específicamente el tribunal que emite la resolución, la causa con número de RUC o RIT y se individualice claramente al usuario o cliente, la cual deberá siempre adjuntarse al requerimiento. Por otro lado, se exige que sea el Fiscal de la causa y no otro individuo quien realice la solicitud a un correo electrónico especialmente señalado para tal efecto.

Los mismos requisitos son establecidos respecto de la solicitud de interceptación de comunicaciones telefónicas. El mismo documento se reserva el derecho de rechazar las solicitudes cuando no cuenten con todos los requisitos establecidos y a notificar a los usuarios de las diligencias realizadas una vez que haya vencido el plazo de reserva de la diligencia.

Claro Chile obtiene una estrella en este punto.

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

En la sección "Relación con la autoridad" Claro ha disponibilizado una serie de documentos relativos acciones que ha tomado la empresa para proteger la privacidad de sus usuarios. Es posible encontrar dos minutas presentadas a los senadores Harboe e Insulza respectivamente, en que Claro manifiesta su preocupación por el aumento del período de retención de metadatos en el proyecto de ley de delitos informáticos. Esto resulta atingente, ya que ambos senadores son miembros de la Comisión de Seguridad Ciudadana del Senado, comisión que se encuentra tramitando dicho proyecto de ley.[50] En los mismos documentos, Claro propone a ambos senadores la posibilidad de incluir en la Ley Nº 19.628 la exigencia de notificar a los usuarios cuando estos sean objeto de alguna diligencia intrusiva al interior del proceso penal.

La sección también cuenta con tres documentos correspondientes a querellas contra quienes resulten responsables por el delito de estafa, en casos relacionados con suplantación de identidad. Si bien esto puede resultar positivo, no puede considerarse dentro de la evaluación de este ítem, ya que la suplantación de identidad tuvo lugar por la incapacidad del agente de ventas de Claro de verificar rigurosamente la identidad del comprador. De esta forma, no puede conside-

50 Las minutas están disponibles en los siguientes enlaces 1) https://www.clarochile.cl/portal/cl/archivos_generales/senado-1-insulza_20190605.pdf y 2) https://www.clarochile.cl/portal/cl/archivos_generales/senado-2-harboe_20190605.pdf [Consultado el 30 de junio de 2019].

rarse como una forma de defensa de los derechos del usuario. Algo similar sucede con un documento que da cuenta de una respuesta a una solicitud de acceso de un usuario, ya que el deber de contestar las solicitudes de acceso a información personal es una obligación legal contenida en la Ley Nº 19.628, no puede considerarse como una medida de defensa de los derechos del usuario.[51]

Por último, se encuentra disponible la respuesta que Claro dio a los oficios ordinarios Nº 106[52] y Nº 107[53] de 2018, en donde SUBTEL solicitó a distintas empresas de telecomunicaciones información de carácter personal de sus usuarios. Sin embargo –y como veremos más adelante– a diferencia de Entel (otra empresa objeto de solicitud), Claro no se negó a entregar la información solicitada por SUBTEL y se limitó a informar que Claro mantiene consideraciones y reparos relativos a la protección de datos personales de sus clientes en este caso, solicitando la creación de una mesa de trabajo que estudie los procedimientos de entrega de información.

Claro Chile obtiene media estrella en este ítem en atención a las gestiones realizadas en distintos procesos legislativos.

4.5. *Entel*

4.5.1. ¿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?

Todos los documentos relativos a políticas de privacidad, datos personales y términos y condiciones de Entel se encuentran disponibles en una sección especial de su sitio web, la cual puede ser fácilmente identificada desde la portada del mismo.[54] Entre estos documento se encuentra su "Política de Privacidad Clientes Entel", la cual fue actualizada en el mes de junio de 2019.[55] Vale la pena mencionar que el documento establece explícitamente que de ser actualizada, las versiones anteriores seguirán estando disponibles en su sitio web, de forma tal que el usuario pueda comparar los cambios.

Muchos de los principios mencionados en la metodología son reco-

51 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Respuesta-derechos-%20ARCO_20190606.pdf [Consultado el 30 de junio de 2019].

52 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Ord.106_20190605.pdf [Consultado el 30 de junio de 2019].

53 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Ord.107_20190605.pdf [Consultado el 30 de junio de 2019].

54 Disponible en: https://www.entel.cl/legales/ [Consultado el 27 de junio de 2019].

55 Disponible en: https://www.entel.cl/legales/pdf/Pol%C3%ADtica-de-Privacidad-Clientes-Entel.pdf [Consultado el 27 de junio de 2019].

gidos de forma directa o indirecta por la política de privacidad. Por ejemplo, el *principio de licitud* se encuentra en el primer párrafo de los "compromisos Entel", al listar las hipótesis que habilitan a Entel a tratar los datos personales de sus clientes (contar con consentimiento, que se trate de datos contenidos en fuentes accesibles al público, entre otras). En el mismo párrafo se recoge el principio de *minimización de datos,* al declarar que Entel solo solicita los datos estrictamente necesarios para cumplir los fines mencionados. El segundo párrafo recoge el *principio de confidencialidad,* estableciendo el compromiso de la empresa por mantener reserva de los datos personales de sus usuarios y reservándose el derecho a cuestionar las solicitudes de la autoridad cuando no cumplan con los requisitos legales.

El cuarto párrafo de la política recoge el principio de calidad, comprometiéndose a realizar esfuerzos para que los datos almacenados sean exactos, completos y actuales, y modificarlos o eliminarlos cuando dejen de cumplir su función. La segunda sección del documento está titulada "Para qué usamos tus datos" y establece las bases para cumplir con el *principio de finalidad*, señalado que los datos recolectados solo serán utilizados para la celebración y cumplimiento de las obligaciones contractuales, para mejorar y monitorear el servicio entregado y para el envío de comunicaciones comerciales. El último –que puede ser el más controvertido– se encuentra acotado, señalado expresamente que si información personal es entregada a terceros (por ejemplo, si se terceriza el servicio de márketing), estos deberán mantener reserva de ellos y solo podrán ser utilizados para el envío de comunicaciones comerciales en nombre de Entel.

El *principio de proporcionalidad* puede entenderse recogido en la sección titulada "Qué datos tuyos podemos almacenar", donde se detalla taxativamente los datos que Entel recoge de sus usuarios, ninguno de los cuales parece ir más allá de la finalidad establecida en la segunda sección. Por último, el punto tres garantiza el *principio de seguridad,* señalando que se utilizando modelos y estándares de protección de datos a la vanguardia.

El único principio no recogido en el documento es el principio de responsabilidad. Por el contrario, en distintas secciones del documento la política establece causales de responsabilidad del cliente por distintas acciones u omisiones.

Por último, la cuarta sección señala los derechos de los usuarios. Se menciona el derecho a acceso, rectificación y eliminación, pero no se hace mención al derecho a oposición. Por otro lado, no se establece un punto de contacto específico para que los usuarios puedan canalizar sus solicitudes.

En cuanto a los contratos, estos se encuentran disponibles pública-

mente,[56] pero sus secciones sobre protección de datos –aunque no se contradicen con los términos y condiciones de privacidad– son más bien escuetos y no hacen referencia a la política de privacidad con una versión determinada.

Entel obtiene tres cuartos de estrella en este ítem.

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

En el sitio web de Entel es posible encontrar públicamente disponible un informe de transparencia con fecha de 31 de marzo de 2019.[57] Las estadísticas de las solicitudes de información personal por parte de la autoridad están divididas en tres categorías: 1) Solicitudes de interceptaciones solicitadas en estricto cumplimiento de la ley, 2) Otras solicitudes judiciales, y 3) Otros requerimientos.

La primera categoría se encuentra desagregada por mes del año, pero no por zona geográfica. La tabla presentada da cuenta que Entel recibió un total de 7.547 solicitudes de interceptación de comunicaciones, las que probablemente se refieren a interceptaciones telefónicas, aunque el documento no entrega detalles sobre su naturaleza.

El documento da cuenta de que durante el 2018 recibió un total de 68.069 "otras solicitudes judiciales". De acuerdo al documento esta categoría incluye "el resto de solicitudes judiciales distintas de las interceptaciones, tales como solicitudes de tráfico de llamadas y datos, direcciones IP, u otras informaciones que puedan ser solicitadas en el marco de un proceso judicial". Sin embargo, la categoría parece agrupar información de distinta naturaleza, ya que "otras informaciones que puedan ser solicitadas en el marco de un proceso judicial" puede referirse a solicitudes de carácter intrusiva (como el acceso a metadatos del usuario), pero también a solicitudes genéricas de tribunales en donde se solicita información como el RUN o dirección de un individuo en procedimientos laborales o de familia. El hecho de mezclar información de naturaleza tan disímil le resta valor a la estadística presentada.

Por último, la categoría "otros requerimientos" agrupa aquella información solicitada por organismos como la SUBTEL, el Instituto Nacional de Estadísticas, el Banco Central y la Fiscalía Nacional Económica. Durante 2018 recibió un total de 25 solicitudes de este tipo y respondió 24. Es claro que el caso en donde no se entregó la información fue el oficio de SUBTEL que se comenta en el punto 4.5.5.

56 Disponibles en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P63200157451364998548342 [Consultado el 27 de junio de 2019].

57 Disponible en: http://www.entel.cl/legales/pdf/Requerimientos-de-Datos-Personales-2019.pdf [Consultado el 27 de junio de 2019].

Por último, vale la pena mencionar que el documento solo da cuenta de las solicitudes rechazadas en el tercera categoría, pero no para las primeras dos, en donde solo se da cuenta del total de solicitudes recibidas. Un pie de página específicamente señala que las cifras presentadas solo incluye requerimientos realizados cumpliendo las normas procesales que regulan la materia. Todo otro requerimiento es rechazado y no ingresa en las estadísticas.

La compañía obtiene media estrella ya que, a pesar de contar con un informe de transparencia, la información no está presentada de forma clara y no hace mención al porcentaje de solicitudes rechazadas por no cumplir los requisitos legales.

4.5.3. ¿Notifica la empresa a los usuarios acerca de solicitudes de información del Gobierno?

En el documento titulado "Guía informativa acerca de las solicitudes de la autoridad de interceptaciones e información personal" contiene una mención explícita a la posibilidad de notificar a sus clientes respecto de una medida intrusiva que lo haya afectado. De esta forma, el documento sostiene que "*En aquellos casos en que se haya levantado el secreto en la investigación, Entel se reserva el derecho a notificar a sus clientes acerca de las solicitudes de información personal de sus clientes*".[58]

De esta forma –al igual que con WOM y VTR– no queda claro en qué casos Entel notificará a los usuarios y en qué casos no, ya que solo se reserva el derecho a realizar dichas notificaciones y no se compromete a hacerlo. Por otro lado, a diferencia de WOM, Entel no ha señalado que se encuentra en proceso de establecer un mecanismo para hacer efectiva esta posibilidad.

Por lo anterior, Entel recibe un cuarto de estrella en este ítem.

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

Otro aspecto en el que Entel ha avanzado respecto de la evaluación del año 2018 es la publicación de un documento que describe los requisitos que tiene que cumplir la autoridad para que Entel dé curso a una solicitud de acceso o entrega de información de los usuarios.

Este documento se encuentra disponible públicamente en la página web de Entel[59] y detalla los requisitos que Entel exige a la autoridad,

58 Disponible en: http://www.entel.cl/legales/pdf/Guia-judiciales.pdf [Consultado el 2 de julio de 2019].

59 Disponible en: http://www.entel.cl/legales/pdf/Guia-judiciales.pdf [Consultado el 27 de junio de 2019].

tanto para la interceptación de comunicaciones telefónicas, acceso a metadatos o datos de tráfico (registro de conexiones IP) y otros antecedentes. Resulta positivo que Entel señale explícitamente que se requiere una orden judicial previa, tanto para la interceptación de comunicaciones, como para el registro de conexiones IP. Del mismo modo, el documento deja claro los antecedentes que deben ser entregados previamente, entre ellos el RUC de la causa, individualización del afectado, fiscal a cargo de la investigación, fecha de la autorización judicial e individualización del tribunal que otorgó la medida. El documento también señala que la información respecto al registro de conexiones IP será eliminado luego de transcurrido el plazo establecido por la ley (un año). Por último, el documento aclara que es el Ministerio Público quien tiene la facultad exclusiva y excluyente de llevar adelante la persecución penal, y por tanto los datos solicitados solo serán entregados al Fiscal respectivo.

En vista de lo anterior, Entel obtiene una estrella completa en este ítem.

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

A diferencia de los años anteriores, durante 2018 Entel emprendió una importante litigación en defensa de la privacidad y la protección de datos personales de sus usuarios. En mayo de 2018, la SUBTEL envió a todas las empresas de telecomunicaciones dos oficios, solicitando que las empresas entreguen información de sus clientes relativa a los servicios de telefonía móvil y televisión paga. Estos oficios también solicitaban información adicional, como el tipo de plan de prepago o pospago, la comuna y región del cliente, si registra tráfico de dato y/o voz durante los últimos 30 días y si se trata de un cliente que cuenta con multiservicio. El objetivo declarado de esta solicitud de información de datos personales de los usuarios es entregar dicha información CADEM, una empresa que realiza encuestas de satisfacción del usuario.

Esta solicitud resulta preocupante por varias razones. En primer lugar, la información solicitada resulta desproporcionada respecto de la finalidad declarada, ya que un muestreo estadístico no necesariamente requiere la entrega de la totalidad de bases de datos. Por otro lado, los datos de los usuarios fueron recolectados con la finalidad específica de entregar el servicio de telecomunicaciones y no resulta razonable que sean transferidos a otros organismos para fines distintos. Por último, resulta difícil de argumentar que la SUBTEL cuente con las atribuciones legales para exigir que las empresas de telecomunicaciones proporcionen información de sus usuarios para luego

entregarla a otra compañía, con el objetivo de realizar encuestas de satisfacción.[60]

A pesar de que el oficio fue enviado a todas las compañías que son parte de este estudio, Entel fue la única que se negó a entregar toda la información solicitada, recurriendo a tribunales luego de haber sido multada por su negativa. En primera instancia, la Corte de Apelaciones ratificó el incumplimiento de Entel, pero rebajó la multa cursada por SUBTEL de 3.060 UTM (equivalente 149.147.460 de pesos) a un total de solo 10 UTM, en base a que existían fundamentos suficientes por parte de Entel para negarse a la entregar de la información[61].

Al momento del cierre de este informe el proceso judicial no ha concluido, ya que el Consejo de Defensa del Estado presentó un recurso de queja ante la Corte Suprema con el fin de que se mantenga la multa cursada en el monto original definido por la SUBTEL. Este recurso todavía no ha sido fallado.

El caso comentado resulta relevante, puesto que es un ejemplo de cómo una empresa puede recurrir ante tribunales –e incluso arriesgar importantes multas– con el fin de proteger la privacidad y los datos personales de sus clientes. Por otro lado, resulta significativo que de todas las empresas oficiadas, Entel haya sido la única que se haya opuesto a la entrega de información. De hecho, este es el primer caso que defensa de los usuarios ante tribunales que ha sido reportado desde que este informe fue inaugurado en el año 2017.

Por todo lo descrito anteriormente, Entel obtiene una estrella completa en este ítem.

4.6. *GTD Manquehue*

4.6.1. ¿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?

GTD Manquehue pone a disposición del interesado una copia de su contrato de servicios de telecomunicaciones con las condiciones generales de contratación,[62] que aplican a todo servicio contratado con

60 Este caso específico fue analizado por María Paz Canales en la siguiente columna: https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/ [Consultado el 26 de junio de 2019].

61 Las sentencias respectivas corresponden a los roles número 2095-2019 y 2811-2019 de la octava sala de la Corte de Apelaciones de Santiago.

62 GTD Manquehue. Condiciones Generales de Contratación de Servicios de GTD Manquehue S.A. En línea, disponible en: https://nuevo.gtdmanquehue.com/condiciones-comerciales/contratos-de-servicios-gtd-manquehue/condiciones-generales-de-contratacion-gtd-manquehue [Consultado el 23 de marzo de 2018].

la empresa,[63] sin diferencia entre móvil y fijo, prepago o plan.

Ambos documentos cuentan con las mismas disposiciones poco específicas y generales del año pasado.

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 los proveedores 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. Los documentos tampoco hacen mención alguna o abordan de forma sustantiva ninguno de los principios señalados en la metodología de este informe. La única excepción es el *principio de seguridad,* que podría entenderse abordado por la Política de Seguridad de la Información de la empresa, la que busca establecer criterios técnicos para asegurar la disponibilidad, integridad y confidencialidad de la información.[64]

El proveedor obtiene un cuarto de estrella.

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

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

Por ello, GTD Manquehue no recibe estrella.

4.6.3. ¿Notifica la empresa a los usuarios acerca de solicitudes de información del Gobierno?

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

GTD Manquehue no recibe estrella.

63 GTD Manquehue. Solicitud y Contrato de Servicios GTD Manquehue. En línea, disponible en: https://nuevo.gtdmanquehue.com/condiciones-comerciales/contratos-de-servicios-gtd-manquehue/solicitud-y-contrato-de-servicios-gtd-manquehue [Consultado el 23 de marzo de 2018].

64 Disponible en: https://nuevo.gtdmanquehue.com/nuestra-empresa/politica-de-seguridad-de-la-informacion [Consultado el 30 de junio de 2019].

4.6.4. ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que el Gobierno 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 información de un usuario por parte del Gobierno.

GTD Manquehue no recibe estrella.

4.6.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de los usuarios activamente, ya sea 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.

El proveedor no obtiene estrella.

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 el año 2018.

La principal novedad se encuentra en el nivel de disparidad en las puntuaciones obtenidas por las empresas. Esto se puede explicar por el aumento en la exigencia de la metodología, lo que ha acentuado la diferencia entre las empresas que se han preocupado específicamente en mejorar los términos y condiciones de privacidad de sus usuarios y las que no han mostrado interés en esta área.

Por otro lado, el informe de este año muestra un aumento importante en el interés de las empresas por avanzar en dos áreas que en el pasado habían sido vistas con resquemor: la defensa judicial de los usuarios y la notificación de diligencias intrusivas.

Por primera vez desde que comenzamos este proyecto, en el año 2016, tenemos un caso de judicialización de una solicitud de información que se interpretó como desproporcionada: Entel se negó a entregar información que consideró de carácter confidencial a la SUBTEL. Aunque misma solicitud fue entregada al resto de las empresas, ninguna de ellas se negó en los términos que Entel lo hizo.

Claro también avanzó en la materia, a través de gestiones en favor de los derechos de los usuarios en procesos legislativos y WOM al oponerse administrativamente a la entrega de información que consideraba confidencial.

La posibilidad de notificar a los usuarios era el parámetro que las empresas veían con más desconfianza en entregas anteriores, en particular por el miedo de incurrir en alguna infracción legal, lo poco práctico que podía resultar y el miedo a enemistarse con la autoridad. Sin embargo, en el informe de este año tanto WOM como VTR se reservaron el derecho de realizar estas notificaciones y Claro incluso estableció una carta tipo para realizar estas diligencia. Esto, sin duda, significa un avance para los derechos de los usuarios.

Otro aspecto positivo es que la existencia de informes de transparencia parece haberse transformado en un estándar de la industria. De hecho, GTD Manquehue es la única empresa del estudio que no cuenta con uno. El resto de las empresas tienen informes que pueden ser más o menos completos y detallados, pero todas han hecho un

esfuerzo específico para cumplir con este parámetro del informe.

Algo similar ocurre con la publicación de los requisitos que las empresas establecen a la autoridad para acceder a una solicitud de acceso a información personal. Adicionalmente, todos los documentos disponibles muestran que las empresas interpretan que el acceso a los datos de tráfico (o metadatos), establecido en el inciso quinto del artículo 222 del Código Procesal Penal, requiere de una orden judicial previa.

Por último, el análisis de los términos y políticas de privacidad de las empresas estudiadas muestra que algunas compañías se han adelantado a la entrada en vigencia de la nueva ley de datos personales y han decidido proteger la información personal de sus usuarios con un estándar mayor a la legislación vigente. Al menos dos de estas empresas utilizaron explícitamente los principios de este informe, lo que demuestra que la iniciativa ***¿Quién Defiende Tus Datos?*** ha tenido efectos concretos, alentando a mejorar la forma en que se protegen los datos y la privacidad de las usuarias y usuarios.

Resumen de estrellas:

WOM	Movistar	VTR	Claro	Entel	Manquehue GTD
4	**1**	**2**.75	**4**.25	**3**.5	**0**.25
★★★★☆	★☆☆☆☆	★★★☆☆	★★★★☆	★★★☆☆	☆☆☆☆☆


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina