2021

¿QUIÉN DEFIENDE TUS DATOS?

Michelle Bordachar

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

2021

¿QUIÉN DEFIENDE TUS DATOS?

Michelle Bordachar

01101001
01100101
01101110 00100000
01100100 01100101 01100110
01101001 01100101 01101110 01100100
01100101 00100000 01110100 01110101 01110011
00100000 01100100 01100001 01110100 01101111 01110011
00111111 00100000 01101110 01100001 01100100 01101001
0110010111100100 01100101 00100000 01110100 0111010

Portada y diagramación: Constanza Figueroa.
Edición y correcciones: Victoria Verrastro y Vladimir Garay.
Mayo de 2021.

Este informe fue realizado por Derechos Digitales, con el apoyo de EFF

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.

Contenido

1. Introducción

El presente informe corresponde a la cuarta entrega del reporte *¿Quién defiende tus datos?*, una evaluación 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, tanto ante las solicitudes de la autoridad como 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 por última vez en el año 2019,[1] nos proponemos responder las siguientes preguntas: ¿Cuáles son las empresas de telecomunicaciones que tienen las políticas de privacidad y protección de datos más transparentes? ¿Existen procedimientos claros en estos casos? ¿Notifican a sus usuarios de los requerimientos de información realizados por la autoridad? ¿Tienen acuerdos con otras entidades para la entrega de información personal?

Este año, la metodología no ha sufrido modificaciones sustantivas respecto del informe pasado, principalmente con el objetivo de ver el avance que ha tenido la industria desde la realización de la versión anterior de este estudio. Sin embargo, existen algunas novedades. Se incorpora como parámetro adicional (aunque sin contar para la asignación de puntaje) que las empresas hagan explícito el compromiso de que toda solicitud de información acerca de un individuo que contenga datos personales sensibles no solo deberá contar con una orden judicial previa, sino que esta deberá ser de carácter individual, excluyendo la posibilidad de entregar este tipo de información respecto de un conjunto de usuarios.

La metodología también evalúa y mide que exista un compromiso de las empresas en cuanto a que la información relativa a la ubicación de sus usuarios para efectos de políticas públicas (o datos de georreferenciación) solo podrá entregarse a la autoridad de forma anonimizada y agregada, salvo orden judicial fundada y específica. Por último, también se exigirá que las empresas establezcan criterios de transparencia respecto a los convenios que estas firmen con otras instituciones públicas y privadas, con el fin de poner esta información a disposición para efectos de investigación.

Todas esas incorporaciones a la metodología se pueden explicar en gran

1 Disponible en: https://www.derechosdigitales.org/wp-content/uploads/quien-defiende-tus-datos-2019.pdf [Fecha última consulta: 10 de enero de 2021]

medida por la naturaleza del año 2020, bastante distinta a la de cualquier otro año en la historia reciente. El mundo en su totalidad se vio afectado por una pandemia que nos obligó a depender aún más de los medios tecnológicos. La imposibilidad de juntarnos y relacionarnos físicamente con las demás personas nos forzó a replantearnos el *cómo* debemos funcionar para poder seguir subsistiendo. Ello se sumó a un período particularmente turbulento en Chile, donde episodios de protesta, represión policial y persecución penal también eran alcanzados por las tecnologías de comunicación.

Como consecuencia, en un contexto más amplio de renovación del marco mismo de protección de derechos fundamentales a nivel constitucional, la agenda política del último tiempo está marcada por la necesidad apremiante de regular las tecnologías y, consecuentemente, la protección de los datos personales. Llegando a tener que discutirse en sede legislativa situaciones súbitamente generalizadas, como el teletrabajo,[2] el acceso a internet como una necesidad y luego como un derecho para profesores y estudiantes,[3] la actualización de la normativa de persecución de delitos informáticos,[4] entre otras varias leyes y situaciones. Queda plasmada la necesidad de evaluar, sobre todo en el contexto en que la tecnología y las telecomunicaciones son una parte fundamental de nuestra vida, los términos y condiciones del uso de estas, así como políticas de privacidad de las empresas de telecomunicaciones bajo un criterio mucho más exigente que nuestra actual ley de protección de datos (Ley Nº 19.628 de 1999).

¿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 informe periódico 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 ha tomado como base los reportes realizados en años anteriores en Chile y se han recogido experiencias de los informes de otros países latinoamericanos, como Brasil, Colombia y México.

2 Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12518 [Fecha última consulta: 10 de enero de 2021]

3 Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/autores.aspx?prmID=14484&prmBOLETIN=13922-07 [Fecha última consulta: 10 de enero de 2021]

4 Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12715&prmBoletin=12192-25 [Fecha última consulta: 10 de enero de 2021]

2. Metodología

El informe de 2019[5] marcó un salto cualitativo en la forma en que *¿Quién defiende tus datos*? evalúa el nivel de protección que las empresas de telecomunicaciones entregan a los datos de sus usuarios. En esa ocasión, se pasó de un análisis más bien formal sobre la publicidad de sus condiciones de contratación y la publicación de informes de transparencia, a un análisis más sustantivo sobre el contenido de esa documentación. Esto se tradujo en la evaluación del contenido de los términos y condiciones publicados por las distintas empresas, a la luz de una serie de principios contenidos en el proyecto de Ley de Datos Personales que se tramita desde 2017 en el Congreso Nacional.

Producto de lo anterior, el informe del año 2019 mostró un importante avance a nivel de la industria, en términos del nivel de protección que las empresas entregan a sus clientes. El reporte da cuenta de la modificación de los términos y condiciones de muchas empresas, elevando sustantivamente el nivel comprometido de protección de los datos personales y la privacidad de sus usuarios, incluso incorporando explícitamente los principios establecidos en el informe. Pero este nivel de avance no fue homogéneo entre los distintos participantes de la industria. Algunas empresas mejoraron sus niveles de protección, mientras que otras quedaron rezagadas, lo que se vio reflejado en la puntuación otorgada. Por ello, la metodología del informe actual no va a contener modificaciones sustantivas en el mecanismo de evaluación, con el objetivo de poder comparar el nivel de avance de la industria durante este último año.

Un informe de estas características no puede estar ajeno a los distintos avances y acontecimientos que se relacionan con el mercado de las telecomunicaciones. Es el caso del año 2020, marcado por la emergencia sanitaria producida por el virus COVID-19. Entre las propuestas que el gobierno ha barajado para combatir la pandemia se han nombrado varias que se relacionan directamente con las empresas de telecomunicaciones, tales como la utilización de aplicaciones de rastreo, la obtención de acceso a la información de ubicación de las personas infectadas y el análisis de flujo de población a partir de

5 https://www.derechosdigitales.org/qdtd-2019/

la información de antenas telefónicas.[6]

Si bien los estados de excepción constitucional pueden justificar la implementación de medidas intrusivas, estas todavía deben cumplir con los requisitos establecidos en el ordenamiento jurídico y los criterios de necesidad y proporcionalidad. De esta forma, la presente entrega del informe incorporará en su metodología que las empresas hagan explícito que toda solicitud de información acerca de un individuo que contenga datos personales sensibles, tales como la geolocalización, no solo deberá contar con una orden judicial previa, sino que esta deberá ser de carácter individual, excluyendo la posibilidad de que las empresas entreguen este tipo de información respecto de una colectividad de usuarios.

Del mismo modo, la metodología evaluará que exista un compromiso de las empresas respecto de que la información relativa a la ubicación de sus usuarios para efectos de políticas públicas solo podrá entregarse a la autoridad de forma anonimizada y agregada. Por último, también se exigirá que las empresas establezcan criterios de transparencia respecto a los convenios que estas firmen con otras instituciones públicas y privadas, con el fin de poner esta información a disposición para efectos de investigación. Para poder comparar la evaluación actual con la realizada en 2019, estos parámetros no contarán para la asignación de puntaje en esta versión.

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

Manteniendo los parámetros establecidos en el informe anterior, para obtener la máxima puntuación las empresas no solo deberán tener disponibles públicamente sus contratos y sus políticas de privacidad, sino que dichos documentos deben reflejar un compromiso sustantivo con la defensa de los usuarios, su privacidad y la protección de sus datos personales. Con el fin de que las empresas entreguen un nivel de protección que vaya más allá de la ley vigente, se analizarán los términos y condiciones a la luz de los principios contenidos en el proyecto de ley de datos personales que hoy se tramita en el Congreso Nacional.[7]

Ya que el texto del proyecto de ley puede modificarse durante el pro-

6 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 utilizarán para evaluar su desempeño, semanas antes de la versión final.

7 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 [Fecha última consulta: 10 de enero de 2021]

ceso 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 para 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.

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 guardar reserva acerca de los datos personales del titular. Del mismo modo, se compromete a establecer controles y medidas adecuadas para preservar su confidencialidad, entregando acceso a terceros solo cuando el titular lo ha consentido expresamente o cuando es requerido por la autoridad, cumpliendo 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 al momento del cierre de este informe, es el principio de minimización de datos, que, si bien se encuentra relacionado con el de proporcionalidad, nos parece importante considerar 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.

Sin embargo, estos no son los únicos criterios de evaluación, al existir otras vías mediante las cuales las compañías pueden demostrar su nivel de compromiso con la protección de la seguridad y derechos de sus clientes, a través de prácticas regulares que distan de sus documentos públicos de políticas de manejo de datos, por ejemplo, en el caso de las prácticas en el manejo de antecedentes de sus clientes. En específico, la solicitud de fotocopia de cédulas de identidad y, en general, los mecanismos que utilizan para la verificación de identidad de las personas, cuestión que se encuentra directamente relacionada con el cumplimiento de los principios de minimización y seguridad. Esto último, en el contexto de las recientes denuncias[8] realizadas por víctimas de suplantación de identidad o fraudes como el SIM *Swapping*.[9] 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.

2.2 Informe de transparencia

Este parámetro ha sufrido modificaciones menores. Esto se debe a que cinco de las seis empresas evaluadas ya han implementado la publicación de informes periódicos de transparencia, transformándose en una especie de estándar de la industria. Sin embargo, el nivel de granularidad de los informes sigue siendo variado, por lo que se seguirá evaluando que las empresas hagan explícito el número, e

8 https://twitter.com/24HorasTVN/status/1377440045661966337

9 https://www.24horas.cl/nacional/sim-swapping-estafa-telefonos-chip-4714667

idealmente el porcentaje, de las solicitudes que fueron rechazadas por no cumplir con los requisitos legales. Del mismo modo, se exigirá que las empresas presenten la información de forma desagregada, estableciendo el número de solicitudes que solicitan acceso a los metadatos[10] de sus clientes 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.

También se verificará si las empresas de telecomunicaciones informan a sus usuarios el tiempo máximo por el que almacenan sus metadatos de comunicaciones y si estos son eliminados transcurrido el tiempo exigido por la ley.

Por último, si bien no es necesario que conste en el mismo documento del informe, este año se evaluará que las empresas transparenten los convenios suscritos con instituciones públicas y privadas que entreguen acceso a información personal o estadística de sus usuarios para efectos de iniciativas de investigación.

2.3 Notificación a los usuarios

Al igual que el año pasado, la notificación a los usuarios se mantiene como el parámetro con menor cumplimiento. En 2019, solo una empresa implementó un sistema de notificación a sus usuarios, aunque solamente respecto de causas judiciales civiles y de familia, no investigaciones de carácter penal.

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, incluso, que no resulta legalmente posible notificar al usuario de una diligencia intrusiva, ya que el Código Procesal Penal establece un deber de reserva durante 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, si la reserva resulta estrictamente indispensable para la eficacia de la diligencia. La hipótesis implica que la persona

10 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.

investigada no sepa que está siendo objeto de vigilancia mientras esta se ejerce.

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 naturaleza de la diligencia). Una falta de comunicación extendida en el tiempo terminaría produciendo indefensión en las personas afectadas por intrusiones potencialmente abusivas. En los casos en donde se formaliza una investigación en relación con la persona afectada por la medida, se reduce ese riesgo, ya que la defensa tendrá acceso a la carpeta de investigación.[11] Cuando no hay formalización, esa intrusión en la vida privada queda libre de escrutinio.

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 aquellas personas que resultan afectadas por medidas intrusivas de vigilancia de investigaciones que no llegan a la etapa de formalización ante un tribunal, el hecho que la empresa los notifique se transforma en el único mecanismo posible para enterarse 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 expresamente algún mecanismo para notificar a sus usuarios que la autoridad ha solicitado su historial de tráfico (metadatos) o una interceptación de sus comunicaciones privadas. Esta notificación debe realizarse luego que la reserva de la diligencia haya 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 que las empresas notifiquen sin entorpecer o participar innecesariamente en los procedimientos penales.

11 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.

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 al informe de 2019. Se busca constatar que las empresas cuenten con una pauta públicamente disponible que establezca cuáles 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 realizar este tipo de diligencias. Al igual que el año pasado, esta versión del informe 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.

Como novedad, este año el informe evaluará que las empresas hagan explícito que toda solicitud de información que contenga datos personales sensibles, tales como la geolocalización, no solo deberá contar con una orden judicial previa, sino que esta deberá ser de carácter individual. También se exigirá que la información relativa a la ubicación de sus usuarios, para efectos de políticas públicas (por ejemplo, políticas de transporte, de desarrollo social, etcétera) solo podrá entregarse a la autoridad de forma anonimizada y agregada.

2.5 Defensa de la privacidad, en especial ante los tribunales de justicia, el poder legislativo y la administración

El objetivo de este parámetro es dar cuenta del nivel de compromiso que las empresas demuestran efectivamente hacia la protección de los derechos de las personas como con su seguridad, mediante su resguardo, promoción y defensa activa. De esta forma, también buscamos conocer el nivel de concordancia entre las declaraciones y las acciones de las compañías.

Para estos efectos, al igual que en años anteriores, uno de los aspectos relevantes para el análisis es 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. Asimismo, se ha considerado el hecho que la empresa haya efectuado alguna acción comprobable y significativa para oponerse a proyectos de ley, normas legales, políticas públicas o requerimientos de la autoridad que pudieran afectar la privacidad o la protección de los datos personales de sus abonados.

En la presente versión del informe, este punto resulta especialmente sensible. La investigación y persecución penal de los hechos de violencia posteriores al estallido social de octubre de 2019 conlleva a su vez la recogida de antecedentes que, como es de público conocimiento, involucran la recolección de datos de comunicación.

A ello se suma la circunstancia de la pandemia y la implementación de medidas de confinamiento que obligó a mantener atención sobre posibles medidas de la autoridad. Finalmente, el requerimiento de datos personales por entidades administrativas con diversos fines o la creación de nuevas instancias de recolección de información personal de telecomunicaciones, como en el caso de la implementación de la Ley de Velocidad Mínima Garantizada. En algunas ocasiones, la reacción frente a acciones regulatorias no provino necesariamente de las empresas estudiadas individualmente, sino de su agrupación gremial en la Asociación de Telefonía Móvil (ATELMO), de la que son miembros Claro, Entel, GTD, Movistar y VTR. Esta circunstancia es también tomada en consideración.

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, cuando 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, que menoscaba 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 las empresas de las que son clientes, este informe pueda realizar una medición más precisa. De esta forma, se entrega a los usuarios una visualización que les

permite diferenciar de forma más clara los distintos niveles de cumplimiento de los ISP 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.

a) 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 encuentran disponibles 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 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.

b) ¿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 comunicacio-

nes. 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, etcétera).
- El informe se publica, como mínimo, con una frecuencia anual.

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.

c) ¿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 ha tomado acciones (comprobables) para implementar un sistema que le permita notificar al usuario de que ha sido objeto de una medida intrusiva, idealmente 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.

d) ¿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, publicada en su página web y destinada 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 detalla y establece específicamente los requisitos necesarios para responder favorablemente a la solicitud (por ejemplo, una orden judicial; nivel mínimo de especificidad que requiere una solicitud de información para que sea procedente; etc.).
- La empresa es clara respecto al tiempo que guarda la información de los usuarios.
- La empresa es clara respecto a la eliminación de la información de los usuarios, una vez transcurrido el plazo durante el cual la guarda.

El proveedor obtiene media estrella si cuenta con alguna guía publicada en su sitio web para el manejo de los datos de los usuarios, aun 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.

e) ¿La empresa proveedora ha defendido la privacidad y protegido los datos de los usuarios activamente, ya sea públicamente, en sede judicial o administrativa 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. También se otorgará una estrella a aquellos proveedores que, aun cuando no hayan recurrido a la justicia, hayan logrado conseguir el mismo resultado agotando las instancias previas.

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 propuesta de reforma a la ley Nº 19.628 sobre Protección de la vida privada, formulada con el propósito de renovar casi la totalidad del estatuto actual, se presenta como el esfuerzo más ambicioso para actualizar la normativa con más de veinte años de vigencia.[12] Presentado el 13 de marzo de 2017,[13] el proyecto de ley[14] se encuentra en primer trámite constitucional (discusión de su articulado en el Senado), habiéndose aprobado en general en el Senado.

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 ser autorizada previamente por un tribunal[15] 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

12 Fue promulgada el 18 de agosto de 1999, y publicada el 28 de agosto del mismo año.

13 Carey (2017) "Proyecto de Ley que Regula la Protección de Datos Personales y Crea la Agencia de Protección de Datos Personales". Disponible en: https://www.carey.cl/proyecto-de-ley-que-regula-la-proteccion-y-el-tratamiento-de-los-datos-personales-y-crea-la-agencia-de-proteccion-de-datos-personales/ [Fecha última consulta: 10 de enero de 2021]

14 Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07 [Fecha última consulta: 10 de enero de 2021]

15 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.

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,[16] 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 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.[17] 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.

El artículo 224 del Código Procesal Penal señala que la 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 Ministerio Público u otros organismos, en la medida que se cumplan los requisitos establecidos en el artículo mencionado.

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

16 "¿Qué dice el llamado 'Decreto Espía'?", https://www.derechosdigitales.org/11400/que-dice-el-llamado-decreto-espia/ [Fecha última consulta: 10 de enero de 2021]

17 Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25 [Fecha última consulta: 10 de enero de 2021]

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 que 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 blanco de críticas desde su promulgación, 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 personales, ni hace mención al tratamiento transfronterizo de estos. 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 se establecen formas especiales de reparación. La ley 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, tampoco los prohíbe. Por lo mismo, la publicación de este tipo de documentos ha sido considerada una buena práctica para efectos de este informe, en sus distintas versiones.

3.2 Empresas de telecomunicaciones

Como bien sabemos, el año 2020 estuvo marcado por la pandemia COVID-19. Dicha situación hizo crecer fuertemente la importancia y el uso que le daban las personas a los servicios prestados por las empresas de telecomunicaciones, lo que produjo un alza considerable durante el primer semestre del 2020: desde diciembre de 2019 a junio de 2020 el tráfico mensual de datos fijos aumentó un 44%, mientras que

el tráfico de datos móviles aumentó un 22,5% en el mismo periodo.[18]

En cuanto a la participación de mercado de las empresas de telecomunicaciones, el más reciente informe de Subtel[19] muestra cómo el mercado ha evolucionado durante el último año. De acuerdo con las estadísticas de diciembre de 2020,[20] las cuotas de mercado entre los diferentes ISP son las siguientes:

1. *Movistar.* Participación de mercado: 26,9% del mercado de internet fijo y 21,6% del mercado de internet móvil.
2. *VTR.* Participación de mercado: 33,9% del mercado de internet fijo y 1,3% del mercado de internet móvil.
3. *Claro Chile.* Participación de mercado: 12,8% del mercado de internet fijo y 16,7% del mercado de internet móvil.
4. *Entel.* Participación de mercado: 6,7% del mercado de internet fijo y 34,8 % del mercado de internet móvil.
5. *Grupo GTD.* Participación de mercado: 8% del mercado de internet fijo y no cuenta con participación en el mercado de internet móvil.
6. *WOM.* No cuenta con participación en el mercado de internet fijo y un 24,8% del mercado de internet móvil.

Las seis compañías seleccionadas para este estudio representan una parte sustantiva del mercado de internet en Chile: un 88,3% de los servicios fijos y 99,2% de conexiones móviles.

Según cifras de 2019, el 82,3% de la población en Chile usa internet,[21] mayoritariamente a través de servicios móviles,[22] número que se ha mantenido al alza durante los últimos seis años. En consecuencia, los resultados de esta evaluación dan cuenta de una situación que afecta a parte importante de la población chilena.

18 SUBTEL. 2020. Especial Análisis Tráfico Internet enero-junio 2020 de la Subtel. Disponible en: https://www.subtel.gob.cl/wp-content/uploads/2021/01/PPT_Series_JUNIO_2020_V0.pdf Fecha última consulta: 4 de mayo de 2021]

19 SUBTEL. 2020. Sector Telecomunicaciones. Disponible en: https://www.subtel.gob.cl/wp-content/uploads/2021/04/PPT_Series_DICIEMBRE_2020_V0.pptx [Fecha última consulta: 4 de mayo de 2021]

20 Ibíd.

21 https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2019&locations=CL&start=1992&view=chart

22 Según las mismas estadísticas de Subtel, el 60,40% de la población cuenta con internet fija en el hogar.

4. Análisis

4.1 WOM

a) ¿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 sobre términos comerciales, contractuales y transparencia,[23] donde es posible acceder a los modelos de contrato de servicios y sus anexos. El sitio web ha mantenido la presentación de los años anteriores, muestra la información a través de una serie de pestañas que se expanden al hacer clic, resultando claro e intuitivo acceder a ellas, tomando solamente tres clics desde la página principal a los modelos y anexos de contratos.

El contrato tipo para la contratación de servicios hace referencia a la protección de los datos personales de clientes, en su cláusula octava.[24] Si bien en lo sustantivo la última versión de esta cláusula mantiene prácticamente los mismos términos del año anterior (compromiso a dar estricto cuidado a todos los principios considerados en la metodología de este informe; la limitación de la finalidad en el uso de los datos a la entrega del servicio y el envío de publicidad y beneficios, y la referencia al derecho de los clientes a solicitar la modificación o eliminación de sus datos personales y el no envío de información publicitaria, promocional y/o de entretenimiento), se ha introducido una importante mejora en relación a los derechos de los usuarios. Así, como novedad, este año WOM incluyó un contacto directo para que los clientes puedan solicitar la modificación o eliminación de sus datos (datospersonales@wom.cl) y un enlace a un formulario para solicitar el cese de envío de información publicitaria

23 WOM. Términos Comerciales, Contractuales, Modelo de Integridad y Transparencia. Disponible en: https://www.wom.cl/terminos-condiciones/ [Fecha última consulta: 29 de abril de 2021]

24 "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, o discriminación, seguridad, limitación de uso y minimización de datos. En cualquier momento el cliente podrá solicitar la modificación o eliminación de sus datos personales al correo datospersonales@wom.cl y el no envío de información publicitaria, promocional y/o de entretenimiento en https://www.wom.cl/nomasinformacion, acercándose a las sucursales habilitadas o llamando al call center. WOM declara tener una política de privacidad, publicada en https://www.wom.cl/terminos_condiciones, la cual podría modificarse en el futuro, sin perjuicio de que los clientes tendrán acceso a las versiones anteriores". [Fecha última consulta: 5 de enero de 2021]

(http://www.wom.cl/nomasinformacion/). Del mismo modo, pese a que lo anterior estaba señalado en la cláusula pasada, esta se ha modificado, incluyendo un enlace directo a una página habilitada por WOM (http://www.wom.cl/nomasinformacion/) para desuscribirse de sus bases de datos y no recibir más publicidad. Anteriormente, ambas cuestiones solo podían realizarse acercándose a sucursales habilitadas o llamando al centro de atención telefónica de WOM. El cambio introducido por la compañía hace el proceso mucho más intuitivo, fácil y rápido para el ejercicio de este derecho por parte de los usuarios.

Los anexos de "Planes y Tarifas Multimedia", "Planes Solo Voz", "Planes Solo Datos" y "Planes y Tarifas Internet" complementan los contratos tipo, en cada uno de los servicios referidos. Estos anexos contienen información de carácter técnico, especialmente referida a la velocidad y las condiciones de entrega de servicio, y sin hacer referencia a las condiciones relacionas con la privacidad o la protección de datos de los usuarios.

En la pestaña "Políticas de privacidad y de seguridad" existe un menú desplegable, donde se describe en términos sencillos el contenido de la política de privacidad. En ese mismo menú se pueden encontrar tres documentos: la política de privacidad actual (de junio de 2019, ya analizada para la elaboración del informe pasado), las versiones anteriores —todas con fecha— y la política de contactabilidad.

La política de privacidad es aplicable al sitio web de WOM, sus distintos canales de comunicación y todos los servicios que la empresa ofrece.

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 aquellos 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 les advierte que solo compartirá sus datos con terceros cuando la ley así lo ha facultado, cuando el titular lo ha consentido expresamente, o cuando es requerido por la autoridad en cumplimiento de los requisitos legales. Si bien se valora el compromiso expresado respecto de la reserva de los datos, los términos "cuando el titular ha consentido" y "cuando la ley así lo ha facultado" resultan bastante abstractos y poco determinados.

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 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 también 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, entregando un correo electrónico específico para hacer llegar estas solicitudes.

El año pasado la empresa tuvo una estrella completa, por lo cual en base a las últimas mejoras introducidas (incorporación de mecanismos que facilitan a sus clientes el ejercicio de sus derechos) es que este año volverán a tener puntaje máximo.

La empresa obtiene una estrella en este ítem.

b) ¿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 corres-

pondientes a los años 2018,[25] 2019,[26] 2020[27] y 2021;[28] siendo posible reconocer varios avances en estos últimos dos informes.

A partir del informe de 2020, WOM comenzó a reportar tres categorías de solicitudes: 1) total de interceptaciones, 2) total de solicitudes de información, y 3) solicitudes de otros datos. Respecto a la primera categoría, se reportaron un total de 8.700 solicitudes de interceptación durante al año 2019, ninguna de las cuales fue rechazada. Adicionalmente, WOM informa que se encontraron casos con diferencias entre la resolución judicial y la ficha del sistema de registro de intervenciones telefónicas del Ministerio Público ("RESIT"), haciendo prevalecer lo informado en la resolución dictada por el juzgado respectivo.

En cuanto a la segunda categoría, WOM declara haber recibido un total de 17.314 solicitudes de información durante el año 2019, de las cuales 95 fueron rechazadas por incumplimiento de requisitos legales, debido a que los requerimientos respectivos no contaban con antecedentes suficientes que los sustentaran, de acuerdo con la política de WOM de requisitos para el envío de información a la autoridad en respuesta a requerimientos judiciales y de acuerdo con la normativa vigente. A diferencia del año 2019, el informe de 2020 además desglosa esta información en solicitudes relacionadas a tráfico[29] (8.135) y otras solicitudes de información (9.179). Sin embargo, en relación con estas últimas, solo se entregan los siguientes ejemplos del tipo de información de que podría tratarse:

- 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.

No es posible conocer el tipo de información solicitada, dada la amplitud del término "datos asociados", ni tampoco si existe otro tipo de información que les sea solicitada, ni a qué porcentaje del universo de solicitudes recibidas corresponde cada una de estas subcategorías.

25 WOM. Informe de Transparencia año 2018, disponible en: https://www.wom.cl/bases/bases/documents/informe-transparencia-2018.pdf [Fecha última consulta: 29 de abril de 2021]

26 WOM. Informe de Transparencia año 2018, disponible en: https://www.wom.cl/bases/bases/documents/informe-transparencia-2019.pdf [Fecha última consulta: 29 de abril de 2021]

27 WOM. Informe de Transparencia año 2020. Disponible en: https://www.wom.cl/bases/bases/documents/informe-transparencia-2020.pdf [Fecha última consulta: 29 de abril de 2021]

28 WOM. Informe de Transparencia año 2021. Disponible en: https://www.wom.cl/bases/bases/documents/informe-transparencia-2021.pdf [Fecha última consulta: 29 de abril de 2021]

29 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.

Tal como advertimos en nuestro informe anterior, esta falta de precisión hace que no sea posible tener una idea clara de qué porcentaje de estas solicitudes son de carácter intrusivo, como aquella contenida en el inciso quinto del artículo 222 del Código Procesal Penal. Por último, para la tercera categoría de requerimientos, se informan un total de 14 solicitudes. Al igual que en el caso anterior, solo se entregan algunos ejemplos (informaciones asociadas a pagos de cuentas con cheque, envío de facturas asociadas a compras de equipos móviles, datos relacionados con pagos de tarjetas de crédito y respaldo de imágenes de cámaras de seguridad).

Por su parte, el informe de 2021 muestra que en 2020 hubo un total de 8.332 solicitudes de interceptación, 12.563 solicitudes de información (1.186 relacionadas a tráfico y 11.377 correspondientes a "otras solicitudes") y 218 requerimientos distintos de los señalados en el artículo 222 inciso 5º del CPP. En relación con el número de solicitudes rechazadas u observadas, se observa un aumento considerable, con un total de 30 para el caso de las interceptaciones (en comparación a ninguna en 2019) y 1.021 para otras solicitudes de información (en comparación a 95 en 2019).

Adicionalmente, se vuelve a informar sobre casos con diferencias entre la resolución judicial y la ficha del sistema RESIT, prevaleciendo lo informado en la resolución judicial dictada por el juez respectivo, y que el rechazo u observaciones a las solicitudes de información fue debido a que los requerimientos no contaban con los antecedentes suficientes que los sustentaran, de acuerdo con la política de requisitos para el envío de información a la autoridad y a la normativa vigente.

Por último, cabe destacar que los informes de WOM presentan la información desagregada a través de un criterio geográfico por región, dejando en evidencia que la gran mayoría de las interceptaciones son realizadas en la Región Metropolitana.

En síntesis, se reconocen avances tanto en la forma de proceder ante la recepción de solicitudes de información como en la forma de presentar la información relacionada con dichas solicitudes. Sin embargo, creemos que aún es posible alcanzar un mayor nivel de detalle respecto de este último punto.

Por lo anterior, **WOM recibe una estrella**. *Instamos a la compañía a profundizar en la granularidad de sus futuros informes de transparencia.*

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

WOM no presenta avances en esta categoría respecto del informe anterior. En el "Protocolo de Entrega de Información a la Autoridad"[30] 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, sin comprometerse a hacerlo. Tampoco se entrega información sobre la notificación o no a usuarios objeto de solicitudes de información realizadas en procesos que no sean de carácter penal.

Por otra parte, tanto en el informe de transparencia de 2020 como en el de 2021 WOM señala haber iniciado un diálogo con autoridades para explorar la vía por la cual se pueda notificar a los usuarios acerca de las solicitudes de acceso a su información personal o interceptaciones, haciendo referencia a un requerimiento al Ministerio Público realizado en marzo de 2019. Asimismo, en ambos informes señala que desde el Ministerio Público les habrían insistido en que el principal responsable en la disponibilidad de los antecedentes recaería en Tribunales o el Ministerio Público, dado que las compañías no tienen acceso al estatus de las investigaciones y los procesos judiciales. Por último, el informe termina con una declaración en orden a insistir con las autoridades, para que recojan el requerimiento en cuestión y puedan avanzar prontamente en una solución que permita mantener a los usuarios informados y cumplir la legislación vigente.

WOM no participó ni demostró mayor interés en la discusión legislativa de finales de 2020 referida a la notificación de solicitudes de información de autoridades estatales, siendo su apoyo esencial en esta discusión. Con todo, durante la elaboración de este informe la compañía mostró una actitud colaborativa, especialmente con relación a la comprensión del alcance de las solicitudes de información que reciben las distintas compañías.

Por ello, **la compañía obtiene media estrella**. *Este año esperamos*

30 WOM. Protocolo de Entrega de Información a la Autoridad año 2020. Disponible en: http://www.wom.cl/bases/bases/documents/Protocolo-Entrega-Informaci%C3%B3n-Autoridad.pdf [Fecha última consulta: 5 de enero de 2021]
WOM. Protocolo de Entrega de Información a la Autoridad año 2021. Disponible en: https://www.wom.cl/bases/bases/documents/protocolo-entrega-informacion-autoridad.pdf [Fecha última consulta: 30 de abril de 2021]

ver materializadas las intenciones contenidas en sus informes, por ejemplo, mediante su participación en las discusiones legislativas en marcha que incluyen el debate sobre mecanismos de notificación a los afectados por medidas investigativas intrusivas.

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben 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. Desde el informe pasado a la presente versión, WOM ha emitido dos documentos titulados "Protocolo de Entrega de Información a la Autoridad", ambas versiones ligeramente modificadas del respectivo protocolo de 2018. Estos documentos hacen referencia al año y mes de su publicación, siendo el primero de octubre de 2020 y el segundo de enero 2021, y dan a entender que se informará la fecha en que es modificado o actualizado.

El protocolo comienza por dar cuenta de los cuerpos jurídicos que pueden ser invocados por la autoridad para solicitar la interceptación de comunicaciones o la solicitud de información personal de los usuarios. Respecto de la interceptación de comunicaciones, el protocolo establece que esta puede ser solicitada por el Fiscal del Ministerio Público que investiga una causa, por Carabineros o por la Policía de Investigaciones, a través del sistema RESIT del Ministerio Público, que posteriormente derivará el requerimiento a la plataforma de WOM para realizar la gestión respectiva, previa validación de la documentación asociada. Las demás autoridades autorizadas por ley deben contactarse al correo requerimientos_mp@wom.cl, a través de su correo institucional. Para lo anterior se requiere adjuntar la autorización o resolución judicial debidamente firmada y timbrada, velando porque esta 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 y la autorización debe estar íntegramente escaneada y en formato PDF. 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, se señala que esta podrá ser solicitada por el fiscal, miembro de la Policía de Investigaciones o Carabineros, a través de su correo institucional, adjuntando

la resolución judicial correspondiente. Esto es particularmente positivo, ya que se entiende 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. Con todo, a pesar de reconocer este requisito, WOM habría sido la única compañía que entregó información de sus clientes ante el requerimiento masivo de información realizado por el Ministerio Público sin autorización judicial, en enero de 2020, lo que la empresa luego desmintió mediante un comunicado público.[31]

Sin perjuicio de lo anterior, resulta positivo que la empresa haya eliminado de su protocolo la posibilidad de acceder a solicitudes realizadas sin la respectiva orden judicial en casos de urgencia y que exija explícitamente que se adjunte la autorización judicial que ordena la diligencia de interceptación de comunicaciones.

Por ello, **la compañía recibe media estrella** *en esta categoría.*

e) ¿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 existen antecedentes que WOM haya recurrido a los tribunales de justicia para defender la privacidad de sus usuarios. Por el contrario, como hemos dicho, se ha reportado que en enero de 2020 WOM habría entregado información de sus clientes a fiscalía sin autorización judicial previa.[32] Esto resulta particularmente preocupante si consideramos que WOM fue la única de las compañías requeridas que habría entregado así la información solicitada,[33] en circunstancias donde un par de meses antes WOM había modificado su "Protocolo de Entrega de Información a la Autoridad", y una de las principales modificaciones era que ya no se admitiría la posibilidad de acceder a una solicitud de acceso a información sin adjuntar la orden judicial de forma previa en casos de urgencia. Esta última cuestión resultó decisiva en la puntuación otorgada en el informe anterior. Entendiendo que se trata de un solo hecho conocido, entre las miles de solicitudes recibidas anualmente, es un caso especial, dado el contexto sociopolítico de la solicitud y la amplitud de la misma, en que la información

31 "Compañías de teléfono entregaron datos del tráfico de sus antenas a fiscalía por investigación de estaciones de Metro siniestradas", El Desconcierto, 8 de enero de 2020, https://www.eldesconcierto.cl/noticias/2020/01/08/companias-de-telefono-entregaron-datos-del-trafico-de-sus-antenas-a-fiscalia-por-investigacion-de-estaciones-de-metro-siniestradas.html

32 https://www.fayerwayer.com/2020/01/acusan-wom-entregar-datos-personales/

33 https://www.latercera.com/nacional/noticia/fiscalia-pide-levantar-informacion-antenas-celulares-dias-ocurrieron-ataques-al-metro/963909/

solicitada y entregada no correspondía a un solo usuario, sino a un grupo indeterminado de personas, lo que hace que se trate de una situación excepcionalmente grave. El comunicado posterior de la compañía[34] no despejó del todo las dudas al respecto.

En la sección en donde se encuentra su "Protocolo de Entrega de Información a la Autoridad",[35] WOM publica los oficios enviados por Subtel entre los años 2018 y 2020 a la compañía solicitando información, así como las respuestas enviadas por WOM ante dichas solicitudes. Entre estas últimas podemos encontrar una declaración pública de WOM[36] en reacción al Oficio Ordinario Nº 86 de junio de 2020,[37] en la que manifiesta su disconformidad con la solicitud del regulador consistente en el envío del listado de números telefónicos de su base de clientes y, asimismo, haber solicitado a Subtel reconsiderar su solicitud, de manera de no exponer información exhaustiva de números de teléfono a la autoridad. Así, si bien WOM no ha recurrido a tribunales en la materia, ha demostrado al menos una acción en defensa de los datos personales de sus usuarios en procesos administrativos ante el regulador.

WOM obtiene media estrella en esta categoría.

Movistar Chile

a) ¿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 publica en su sitio web distintos contratos, según el servicio ofrecido. Estos se encuentran a un clic de distancia de la página principal, en el apartado "Condiciones Comerciales y Contractuales", divido en servicios móviles[38] u hogar.[39] Tanto en las "Condiciones

34 "Compañías de teléfono entregaron datos del tráfico de sus antenas a fiscalía por investigación de estaciones de Metro siniestradas", El Desconcierto, 8 de enero de 2020, https://www.eldesconcierto.cl/noticias/2020/01/08/companias-de-telefono-entregaron-datos-del-trafico-de-sus-antenas-a-fiscalia-por-investigacion-de-estaciones-de-metro-siniestradas.html

35 https://www.wom.cl/terminos-condiciones/

36 La declaración de WOM se encuentra disponible en el siguiente enlace: https://www.wom.cl/bases/bases/documents/neutralidad_condiciones/respuesta_oficio_circular_86.pdf [Fecha última consulta: 15 febrero de 2021].

37 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 [Fecha última consulta: 19 de enero de 2021].

38 https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/ [Fecha última consulta: 28 de abril de 2021]

39 https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-hogar/ [Fecha última consulta: 28 de abril de 2021]

contractuales del servicio telefónico móvil"[40] como en el documento "Condiciones contractuales del servicio telefónico fijo"[41] es posible encontrar una cláusula referida a la privacidad, la misma de años anteriores, que se limita a señalar que el tratamiento de datos personales ha de ser realizado conforme a lo establecido por la ley Nº 19.628.

Sin perjuicio de lo anterior, no deja de llamar la atención una sutil diferencia en la redacción de las respectivas secciones sobre datos personales en las condiciones contractuales del servicio telefónico fijo y las del servicio telefónico móvil. Mientras en el primero solo se autoriza el tratamiento de datos personales informados producto de la contratación del servicio, en el último dicha autorización se extiende a aquellos datos que se deriven de la contratación y uso del servicio.

Otra cuestión que vemos con preocupación es que la política de privacidad de Movistar[42] no cuenta con una fecha de entrada en vigor y que, aparentemente, el texto no ha sido modificado desde 2017.

Entre los aspectos positivos, a diferencia de años anteriores, ahora Movistar cuenta con una sola política de privacidad, eliminado la disparidad que existía en las pasadas versiones. Asimismo, vemos como positivo que la "Política de Privacidad y Seguridad" establezca 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 de serie cédula.
6. Fecha de nacimiento.
7. Número telefónico.
8. Dirección particular y/o comercial.
9. Dirección de correo electrónico.

Al mismo tiempo, vemos con preocupación que la política señale que se tratarán "todos los datos personales que se originan a consecuencia de la prestación de los servicios de telecomunicaciones contratados". Esto último, además de ser incoherente con el listado taxativo

40 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 [Fecha última consulta: 28 de abril de 2021]

41 Movistar Chile. Condiciones Contractuales del Servicio Banda Ancha Fija y Banda Ancha Satelital. En línea, disponible en: https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-hogar/pdf/BAF_3.pdf [Fecha última consulta: 28 de abril de 2021]

42 Movistar Chile. Política de Privacidad Movistar. En línea, disponible en: https://ww2.movistar.cl/centro-de-transparencia/politica.html [Fecha última consulta: 28 de abril de 2021]

referido precedentemente, no cumple con el principio de minimización de datos.

En cuanto a los principios mencionados en la metodología, es posible destacar que Movistar recoge el principio de seguridad al señalar que se adoptarán medidas de protección adecuadas, aunque no profundiza en cómo se protegen específicamente los datos de los usuarios. Señala también que actuará en forma responsable si la información se ve comprometida, recogiendo el principio de responsabilidad. También podemos ver parcialmente recogido el principio de licitud, al señalar que se sujetará a las disposiciones de la ley Nº 19.628, sobre Protección de datos de carácter personal, y el principio de finalidad, al establecer que la empresa solo va a procesar datos permitidos por el ordenamiento jurídico. En otras palabras, Movistar se compromete simplemente a cumplir con la legislación vigente en materia de protección de datos personales. Finalmente, no encontramos ninguna referencia ni compromiso en relación con el principio de calidad (para verificar que los datos recabados sean exactos y completos).

Por último, felicitamos la iniciativa de Movistar de crear una página especial para que las personas puedan ejercer sus derechos ARCO,[43] donde encontramos una plataforma intuitiva que hace mucho más fácil el ejercicio de estos derechos. Asimismo, destacamos que Movistar haya eliminado de su política de privacidad la referencia a un costo asociado al ejercicio del derecho a la modificación de datos personales.

La empresa obtiene media estrella en esta categoría. *Instamos a la compañía, nuevamente, a incluir la fecha de entrada en vigor de las respectivas políticas de privacidad, mantener a disposición del público las versiones anteriores y unificar los criterios de recolección de información.*

b) ¿Cuenta la empresa proveedora con un informe de transparencia?

Movistar cuenta con dos informes, uno de sostenibilidad publicado en el sitio web de Telefónica Chile, y otro de transparencia alojado en el sitio web de su matriz internacional.

El informe integrado de sostenibilidad del año 2020 fue recientemente publicado.[44] A diferencia de las versiones anteriores, el informe de este año no es específico para Chile. En cuanto al informe de transparencia, encontramos una versión actualizada a 2020 en el reporte

43 Movistar Chile. Política de Privacidad Movistar. En línea, disponible en: https://ww2.movistar.cl/centro-de-transparencia/politica.html [Fecha última consulta: 28 de abril de 2021]

44 Documento disponible en: https://www.telefonica.com/es/web/negocio-responsable/informe-2020 [Fecha última consulta: 6 de enero de 2021]

"Informe de Transparencia en las Comunicaciones" el que, a diferencia de años anteriores, ha sido publicado en el sitio internacional de Movistar, y también en su "Centro de Transparencia"[45] del sitio web local, haciendo más fácil el acceso a los usuarios chilenos.

Al igual que en su versión 2019, el informe incluye información de distintos países, entre ellos Chile, y no se limita a requerimientos de información de clientes, sino que incluye también información relativa a solicitudes para bloquear el acceso a sitios web, para bloquear o filtrar contenido y para suspender temporalmente el servicio. De conformidad con este informe, en 2019 Movistar Chile recibió 11.491 solicitudes de interceptación de comunicaciones, de las cuales 163 fueron rechazadas; 32.276 solicitudes de acceso a metadatos, de las cuales 675 fueron rechazadas, y ninguna solicitud para bloqueo y filtrado de determinados contenidos.

Recientemente Movistar publicó su informe de transparencia de 2021, el que muestra que en 2020 Movistar Chile recibió 12.433 solicitudes de interceptación de comunicaciones, de las cuales 772 fueron rechazadas; 42.639 solicitudes de acceso a metadatos, de las cuales 867 fueron rechazadas, y ninguna solicitud para bloqueo y filtrado de determinados contenidos y suspensiones geográficas o temporales de servicios.

Lamentablemente, el informe de transparencia solo se encuentra publicado en la página de la matriz de Telefónica,[46] y la información no se encuentra desagregada conforme a un criterio geográfico, ni señala el tiempo durante el cual almacenan metadatos.

Sin perjuicio de lo anterior, destacamos la forma en que Movistar presenta su información, de manera sumamente clara e ilustrativa. Asimismo, que sea la primera y única compañía que pública las alianzas que mantiene con instituciones públicas y privadas para la comunicación o análisis de datos.[47]

Movistar recibe una estrella en esta categoría. Instamos a la compañía a profundizar el nivel de detalles con que entrega su información, por ejemplo, desagregándola mediante un criterio geográfico en sus futuros informes, y a publicar sus informes de transparencia en la página que consultan mayormente sus clientes chilenos, de manera de hacer más accesible la información para estos últimos.

45 Documento disponible en: https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2020.pdf/296b9c6a-92f2-df9c-6abb-6c0cb37c248f [Fecha última consulta: 6 de enero de 2021]

46 Documento disponible en: https://www.telefonica.com/es/web/negocio-responsable/informe-de-transparencia-en-las-comunicaciones [Fecha última consulta: 4 de mayo de 2021].

47 Documento disponible en: https://telefonicachile.cl/el-big-data-al-servicio-de-la-investigacion-conoce-nuestras-alianzas/ [Fecha última consulta: 4 de mayo de 2021].

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

A diferencia de los años anteriores, Movistar comenta y señala la postura que va a tener en cuanto a las notificaciones a sus usuarios. Dicha información la podemos encontrar dentro del "Protocolo de entrega de datos a autoridades competentes".[48]

Ahora bien, pese a que es un avance positivo, de dicho documento se desprende que la compañía está apuntando en dirección contraria a la que buscamos. En el documento, Movistar explícitamente señala: "(...) Movistar Chile no da aviso al usuario o cliente afectado una vez que termina la medida de interceptación, ya que consideramos que la notificación de una medida intrusiva debe ser formalizada dentro del proceso penal y no por una vía alternativa, al objeto de cautelar el ejercicio de los derechos de todos los intervinientes".

En relación con lo anterior, hacemos presente que desde Derechos Digitales creemos necesario encontrar mecanismos que permitan cumplir con la ley vigente en cuanto a la notificación de los afectados por medidas investigativas intrusivas, cuestión por la cual abogamos activamente en el Congreso, pero que difícilmente podría ser tomada en consideración sin el apoyo de las empresas de telecomunicaciones. Por lo demás, los compromisos demostrados por las otras empresas dan cuenta de la posibilidad de insistir en la información útil para las personas eventualmente sujetas a medidas lesivas de su privacidad y su autodeterminación informativa.

Por las razones expuestas, **la empresa recibe un cuarto de estrella en esta categoría.** *Para este año esperamos ver materializada su preocupación por la privacidad y la protección de la información de sus clientes, mediante la defensa activa del respeto de sus derechos y garantías, por ejemplo, mediante su participación en las discusiones legislativas sobre cumplimiento del deber de notificación a los afectados por medidas investigativas intrusivas.*

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?

En comparación con los reportes anteriores, Movistar presenta un gran avance en esta materia. Hoy es posible encontrar información específica dentro de su "Centro para la Transparencia", donde ahora se encuentra disponible el "Protocolo de entrega de datos a autoridades

48 Documento disponible en: https://ww2.movistar.cl/centro-de-transparencia/protocolo.html [Fecha última consulta: 6 de enero de 2021].

competentes".[49] En este protocolo, Movistar da a conocer la política de Movistar Chile en relación a las solicitudes de información por parte de la autoridad, así como el tipo de datos que es suministrado y el procedimiento que siguen dichas solicitudes hasta su materialización.

El protocolo parte afirmando que Movistar es custodio de la información confidencial de sus clientes y usuarios, siempre velando por sus derechos fundamentales y garantías. Por ello, señala que se apegará estrictamente a los procedimientos establecidos tanto en la Constitución como en el ordenamiento jurídico en general, llegando incluso a hacer un examen previo a cada solicitud.

Más adelante en el protocolo, Movistar indica que entrega la información a las autoridades judiciales y administrativas de acuerdo con sus competencias y para el cumplimiento legal de sus funciones. Pone como ejemplo al Ministerio Público, los tribunales, la Agencia de Inteligencia del Estado y la Fiscalía Nacional Económica.

En el apartado "Tipo de información que se entrega a las Autoridades", Movistar indica que "las Autoridades pueden solicitar una amplia tipología de informaciones respecto de un usuario en particular", señalando, "a modo meramente ejemplar", que pueden ser objeto de requerimiento de información los datos personales recabados directamente de su titular, los datos de carácter comercial que a consecuencia del comportamiento contractual del usuario hayan obtenido (tales como líneas de teléfono contratadas, marca y modelo del equipo terminal móvil habilitado, número IMEI del equipo terminal móvil habilitado, planes contratados, servicios adicionales contratados, entre otros). Incluye la información originada a consecuencia de la prestación de los servicios contratados y que se registran en las redes de telecomunicaciones de Movistar, tales como registros de tráficos de llamadas, fecha, hora y duración de una comunicación, tipo de comunicación realizada y registros de números IP, entre otros.

En síntesis, se trata de un documento de fácil acceso, en que se detalla el procedimiento establecido para dar respuesta a las peticiones de entrega de información.

Adicionalmente, cabe destacar que, dentro del mismo "Centro para la Transparencia", Movistar ha publicado información en la que da a conocer públicamente las alianzas públicas y privadas que tiene en materia de investigación y los términos en que se desarrollan dichas iniciativas.

Por ello, **la empresa obtiene tres cuartos de estrella** *en este ítem. Ins-*

49 Disponible en: https://ww2.movistar.cl/centro-de-transparencia/protocolo.html [Fecha última consulta: 6 de enero de 2021]

tamos a la compañía a entregar mayor detalle sobre el tipo de información que puede ser objeto de requerimiento, en lugar de entregar información de forma meramente ejemplar.

e) ¿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?

Durante el año 2019, Movistar Chile llevó a cabo acciones en defensa de los derechos de sus clientes, específicamente en el proceso de cargo iniciado por Subtel, en el expediente Rol Nº 12699-2019, aún en tramitación. Este proceso sancionatorio tiene origen en el Oficio Ordinario Nº 11.027 del 20 de agosto de 2019, a través del cual Subtel requirió a Telefónica Móviles Chile S.A. "enviar el detalle de los nuevos clientes de contrato (364.509) con los campos: número telefónico, fecha de contrato y plan asociado, a través de almacenamiento digital".

A través de carta Nº 559 del 6 de septiembre de 2019, Movistar Chile respondió el requerimiento, aludiendo una evidente colisión normativa entre la ley Nº 18.168 General de Telecomunicaciones y el decreto ley Nº 1.762 de 1977, que establece las facultades fiscalizadoras de Subtel y la garantía constitucional contenida en el artículo 19, numeral 4, conforme al texto vigente fijado por ley Nº 21.096, y la ley Nº 19.628, sobre protección a la vida privada. En vista de dicho conflicto normativo, Movistar Chile solicitó a Subtel que fuera eximida de enviar los antecedentes requeridos, por cuanto no cuenta con autorización expresa de sus clientes para compartir con la información requerida. Lo anterior trajo como consecuencia la formulación del Cargo Rol Nº 12699-2019, el cual se encuentra pendiente de fallo por parte del Ministro de Transportes y Telecomunicaciones.

La empresa obtiene tres cuartos de estrella en este punto. *Esperamos ver un rol más activo por parte de Movistar en cuanto a la defensa de la privacidad y protección de los datos de sus clientes, por ejemplo, mediante su participación en las discusiones legislativas en marcha, que incluyen el debate sobre mecanismos de notificación a los afectados por medidas investigativas intrusivas.*

VTR

a) ¿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?

En el apartado "Contrato de Servicios VTR", contenido en la página principal de su sitio web, están disponibles las copias de los contratos

tipo y las condiciones comerciales de sus servicios de internet, fijos y móviles (sin distinción entre las modalidades de prepago y plan),[50] los que contienen cláusulas relativas a las políticas de datos personales. El acceso es bastante sencillo e intuitivo.

El contrato de suministro de internet fijo y móvil[51] es prácticamente el mismo que se encontraba vigente cuando se publicó la versión anterior de este informe y, con relación a los aspectos que se analizan aquí, no presenta ninguna innovación. De manera prácticamente idéntica para las modalidades fija y móvil, se establece que la empresa registra y analiza el uso de los servicios y las interacciones que los usuarios tienen con la compañía.

La sección 13.1 del documento para internet fijo (11.1 para servicios móviles) se refiere al registro y análisis de información estadística. En esta sección se informa sobre la utilización de mecanismos automatizados que registran el uso de los servicios y la interacción de los clientes con la compañía, explicando que dicha información solo es registrada y analizada en forma estadística, con la finalidad de usarla para mejorar los servicios, procedimientos de atención e iniciativas comerciales. Asimismo, VTR se compromete a no realizar operaciones que impliquen asociar dicha información a algún cliente identificado o identificable.

La sección 13.2 del documento para internet fijo (11.2 para servicios móviles) alude al registro y análisis de información individual de cada cliente relativa al uso de los servicios y su interacción con VTR; por ejemplo, la fecha y duración de sus llamadas telefónicas, las películas contratadas a través del servicio VOD y la fecha de pago de la cuenta mensual, con la finalidad de entregar adecuadamente los servicios contratados. En la misma sección se informa que, con la finalidad indicada precedentemente, dicha información será procesada directamente por VTR o por terceros proveedores de esta, velando para que se apliquen adecuados estándares de confidencialidad, sin perjuicio del deber de VTR de informar a terceros algunos de estos datos, de acuerdo con la normativa vigente o a requerimiento de una autoridad competente.

La sección 13.3 (11.3 para servicios móviles) establece que, al momento de contratar, el cliente autoriza a VTR para tratar, analizar y correlacionar sus datos personales relativos a sus antecedentes de

50 VTR. Revisa las Condiciones Contractuales y Comerciales de los Servicios VTR. En línea, disponible en: https://www.vtr.com/moviles_contratos [Fecha última consulta: 6 de enero de 2021]

51 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 [Fecha última consulta: 30 de agosto de 2016]

contacto, servicios contratados y/o comportamiento de pago, para que VTR o terceros autorizados por esta puedan remitirle comunicaciones publicitarias o comerciales y/o de entretenimiento. En caso de ser terceros quienes envíen las comunicaciones publicitarias, estos deberán informar a los clientes la naturaleza de la asociación comercial con VTR para que puedan ejercer su facultad de revocar dicha autorización.

Finalmente, se informa a los clientes que podrán solicitar en cualquier momento el cambio de sus datos personales y que el procedimiento para efectuar dicha solicitud estará publicado en www.vtr.com.

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, servicios contratados y/o comportamiento de pago. Además, aun cuando se establezca el deber de los terceros de informar a los clientes la naturaleza de la asociación comercial con VTR para que estos puedan ejercer su derecho a revocación, ello significa que, a menos que exista una comunicación del tercero con el cliente –y el tercero cumpla dicho deber– el cliente no tiene forma de saber con cuántos terceros VTR comparte su información, ni quiénes son estos. Esta modalidad contrasta con la de otras compañías, 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.

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.[52] Este sub-sitio contiene una introducción a la que le siguen distintas pestañas desplegables. El apartado primero define qué entiende VTR por información personal, 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.

La siguiente sección del sub-sitio 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,

52 VTR. Política de privacidad del consumidor. En línea, disponible en: https://vtr.com/productos/privacidad [Fecha última consulta: 13 de diciembre de 2020]

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 a 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 propósitos 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 sus obligaciones legales, mejorar sus servicios y proveer sus productos o servicios. También 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 pareciera 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 se encuentra recogido en la pestaña "¿Cuáles son tus derechos?". En ella VTR entrega un correo de contacto específico para que sus usuarios puedan hacer efectivos sus derechos de acceso, rectificación, cancelación u oposición.

Si bien la empresa cuenta con una política de privacidad, esta no aborda todos los principios contenidos en la metodología y sería idéntica a la analizada en años anteriores, sin las modificaciones necesarias para superar los reparos realizados en el estudio de 2019, que a su vez eran una repetición de los contenidos en el informe del 2018. En particular, no ha subsanado su falta de especificidad respecto de las entidades con las cuales puede compartir la información personal de sus clientes para efectos de comunicación comercial, ni ha puesto fecha a su política de privacidad, ambas cuestiones que

también fueron advertidas en los informes de 2017 y 2018.

En definitiva, VTR no presenta avances en esta materia respecto a ninguno de los años anteriores, lo que demuestra una falta de interés en mejorar y proteger la privacidad de sus clientes.

La empresa obtiene un cuarto de estrella en esta categoría.

b) ¿Cuenta la empresa proveedora con un informe de transparencia?

VTR no muestra ningún avance en esta materia respecto de los años anteriores. El informe de privacidad contenido en su página web es de mayo de 2019.[53]

Debido a la falta de avance en la materia, **la compañía recibe cero estrella en esta categoría.**

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

VTR se refiere a este tema en su protocolo de entrega de información a la autoridad, que data de 2019.[54] Si bien VTR hace referencia explícita a la posibilidad de notificar a sus clientes respecto de una medida intrusiva que le haya afectado, solo se reserva el derecho de hacer la notificación, sin comprometerse a ello ni señalar en qué casos notificará a sus clientes y en cuáles no. Por otro lado, tampoco muestra señales de encontrarse en algún proceso con la autoridad para establecer un mecanismo de notificación efectiva, como lo han hecho otras compañías.

Vemos con preocupación la falta de actualización en la materia, especialmente considerando que durante 2019 y 2020 se llevaron a cabo múltiples discusiones en el ámbito público y legislativo sobre este punto.

Debido a la falta de avances, **la compañía recibe cero estrella en esta categoría**.

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?

VTR cuenta con un protocolo de entrega de información a la autori-

53 Disponible en: https://vtr.com/img/documents/Informe-de-Transparencia.pdf [Fecha última consulta: 7 de enero de 2021]

54 Documento disponible en: https://vtr.com/img/documents/Protocolo-de-Entrega-de-informaci%C3%B3n-a-la-Autoridad.pdf [Fecha última consulta: 4 de mayo de 2021].

dad, publicado en su página web, que data de 2019.[55] Allí se menciona la posibilidad que las autoridades hagan requerimientos de datos, indicando el procedimiento que deberán seguir para dicho propósito y bajo qué circunstancias una solicitud podría ser rechazada. Asimismo, VTR informa que mantendrá el registro de los metadatos de comunicaciones de sus clientes por un plazo no inferior a un año y que, transcurridos 2 años, los datos serán eliminados, aunque no especifica la modalidad de eliminación de estos.

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

Resulta positivo que VTR detalle los requisitos que la autoridad debe cumplir para que una solicitud resulte 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.

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.

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

En un sentido similar, en sus "Condiciones de uso" la compañía establece medidas para la administración eficiente de sus redes, aduciendo razones de seguridad informática, la prevención de *spam* y la propagación de virus. Entre las medidas contempladas se encuentra el bloqueo transitorio de ciertos puertos. Estas medidas son aplicables

55 Documento disponible en: https://vtr.com/img/documents/Protocolo-de-Entrega-de-informaci%C3%B3n-a-la-Autoridad.pdf [Fecha última consulta: 4 de mayo de 2021].

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

Finalmente, cabe consignar que en las condiciones comerciales aplicables a los "servicios hogar", documento que entrega información anexa a los contratos, se contemplan normas sobre bloqueo de contenidos. A propósito de la gestión de la red, se menciona el bloqueo de acceso a sitios de abuso infantil y el mecanismo para levantar dicha medida, en caso que sea improcedente. Si bien este documento fue actualizado en abril de 2021, no cuenta con modificaciones sustantivas.

VTR obtiene una estrella en esta categoría.

e) ¿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 los años anteriores, 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". En primer lugar, como vimos anteriormente, dicha política de privacidad se mantiene inalterada respecto de los años anteriores. En segundo lugar, dicha afirmación sin ninguna acción concreta que lo respalde queda solamente en una declaración de principios que no protege en nada a sus clientes, sin contar que 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 los motivos anteriores, **VTR no obtiene estrella en esta categoría**.

Claro Chile

a) ¿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?

La página de inicio del sitio web de Claro Chile[56] cuenta con una sección llamada "Claro Transparente", dentro de la cual se encuentran, entre otras, las secciones "Protección al Usuario" y "Normativa legal". En la primera aparecen los enlaces de acceso a las secciones "Derechos de los usuarios" y "Transparencia, privacidad y protección de datos personales". En la segunda, a "Condiciones contractuales", donde podemos encontrar los distintos contratos que Claro Chile ofrece,[57] divididos en servicios móviles y servicios fijos. Entre los primeros está el "Contrato de suministro de servicios de telecomunicaciones",[58] que cuenta con una sección especial sobre protección de datos personales donde —sin perjuicio de señalar que se sujeta a lo dispuesto por la política de privacidad— hace mención al ejercicio de los derechos de 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.

En cuanto a la protección de los datos personales de sus usuarios, la información ofrecida por Claro en la sección "Protección de Datos",[59] parece bastante completa y detallada, siendo su acceso bastante intuitivo gracias a los cuatro apartados que la componen: 1) "Nuestra Política de privacidad y protección de datos", 2) "Informe de Transparencia", 3) "Relación con la autoridad", y 4)"Demás notificaciones a los Usuarios y/o Clientes Claro". En relación a otras compañías, una de las ventajas del sitio de Claro es que mantiene publicadas las políticas de privacidad de los años anteriores, lo que permite apreciar más fácilmente las diferencias entre una versión y otra.

La versión actualmente vigente corresponde al número 1.3 de octubre de 2020.[60] Como novedad, este año se incorpora expresamente el principio de minimización; aunque se encontrara incluido en la

56 Disponible en: https://www.clarochile.cl/personas/ [Fecha última consulta: 18 de enero de 2021]

57 Disponible en: https://www.clarochile.cl/portal/cl/legal-regulatorio/lightbox/descripcion-ED-188.html [Fecha última consulta: 18 de enero de 2021].

58 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/SSTMmovil%20personaspyme(1)_20190620.pdf [Fecha última consulta: 18 de enero de 2021]

59 Disponible en: https://www.clarochile.cl/personas/proteccion-de-datos/ [Fecha última consulta: 18 de enero de 2021]

60 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Politica-privacidad-y-Proteccion-de-datos-1.3_20201105.pdf [Fecha última consulta: 18 de enero de 2021]

versión anterior, ahora hay un compromiso expreso por parte de la compañía a que los datos recolectados serían únicamente aquellos necesarios para el cumplimiento de los fines informados. Así, en la actualidad la política hace referencia explícita a todos los principios contenidos en la metodología de este informe, siendo además posible encontrar referencias a la concreción de estos en otras disposiciones sustantivas del documento.

Así, el principio de licitud es referido al comprometerse la empresa a solo tratar aquellos datos personales que han sido entregados voluntariamente por los clientes o usuarios a través de su sitio web o cualquier otro medio de acuerdo con sus políticas de privacidad. Del mismo modo, Claro establece que estos datos podrán ser utilizados exclusivamente para proveer productos o servicios, personalizar la experiencia de los usuarios, entregar información sobre productos y ofertas, y con fines estadísticos, entregando sustento al principio de finalidad. Vale la pena mencionar que, para la hipótesis de comunicación de datos a terceros, dicha comunicación se encuentra circunscrita a los objetivos allí señalados.

Entre los cambios realizados por Claro en relación con el año anterior, destacamos la inclusión del siguiente párrafo dedicado a los datos personales de menores de edad:

“Los clientes y/o usuarios solo podrán comunicar datos personales de terceros de acuerdo con lo dispuesto en la Ley 19.628, sobre protección de la vida privada. CLARO no tiene por finalidad recopilar o recolectar datos personales de menores de edad y será responsabilidad de los padres, tutores o representantes la autorización que los menores de edad que se encuentren bajo su cuidado proporcionen”.

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”. 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 cuan-

do se cumplan todos los requisitos legales correspondientes.[61] Relacionado a la confidencialidad, Claro se compromete a establecer las 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 con 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, podrán 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.

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

Claro obtiene **una estrella** *en esta categoría.*

b) ¿Cuenta la empresa proveedora con un informe de transparencia?

A diferencia del año pasado, Claro además de presentar su informe de transparencia en español, también cuenta con una versión traducida al inglés.

La información entregada en el documento 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), en los casos del año 2019 (ambos semestres) y la del primer

61 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".

semestre del 2020, además de estar dividida por región. Asimismo, también se comunican la cantidad de solicitudes rechazadas en cada categoría. De esta forma, el documento muestra que durante el año 2019 se hicieron un total de 39.196 solicitudes de información general, 12.523 solicitudes de interceptación telefónica y 6.091 solicitudes de acceso a metadatos.

Respecto a la cantidad de solicitudes rechazadas, hacemos presente que durante la elaboración del presente informe observamos que la documentación no mostraba información desagregada por tipo de solicitud. Asimismo, si bien daba cuenta de un total de 4.332 requerimientos rechazados —cifra bastante significativa, más del doble que el año anterior—, no se acompañaba de un gráfico que mostrara las estadísticas de dichos rechazos, a diferencia del informe del año anterior. Claro actualizó su informe de transparencia, clasificando también las solicitudes rechazadas e incorporando las solicitudes recibidas de parte de tribunales civiles, familia y laborales.

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

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

En el documento titulado "Política de requerimientos de información", 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 esta haya expirado.

Adicionalmente, dentro de la sección "Claro Transparente", podemos encontrar una sub-sección específica llamada "Demás notificaciones a los Usuarios y/o Clientes Claro",[62] donde 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

62 Disponible en: https://www.clarochile.cl/personas/proteccion-de-datos/ [Fecha última consulta: 18 de enero de 2021]

Claro pretende utilizar para notificar a los usuarios.[63] La carta es bastante sencilla, solo señalando el RUC de la causa, la fecha de realización de la diligencia y el hecho 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. Claro no incluye el deber de notificación en sede penal; con relación a lo anterior, la empresa en comunicación directa con la autora del estudio, declara haber explorado junto al Ministerio Público la posibilidad de notificar a aquellos usuarios o clientes que hayan sido objeto de medidas intrusivas en el contexto de una investigación penal, una vez que haya cesado el deber de confidencialidad o reserva respecto de esta, pero no hace público el resultado de dicho diálogo. No obstante, este compromiso de notificar a los usuarios e intentar comunicarse con el Ministerio Público representa un paso en la dirección correcta.

Claro recibe una estrella en este ítem, *al ser la única compañía que realiza algún tipo de notificación a sus usuarios en causas judiciales (civiles, laborales y de familia) y por haber insistido con la autoridad, durante el año 2020, para encontrar una forma de cumplir con el deber de notificación contenido en el artículo 224 del Código Procesal Penal.*

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?

Al igual que el año pasado, uno de los requisitos que se habían establecido en la metodología es la publicación de las exigencias que debe cumplir la autoridad para solicitar información a Claro. En su página web, la empresa cuenta con la "Política de requerimiento de información".

Durante la elaboración del presente informe advertimos que la política de Claro no había sido modificada desde 2019. Claro, haciéndose cargo de esta observación, actualizó su política y además incorporó nuevos requisitos en relación con al bloqueo de páginas web o direcciones IP.

El documento, como se señaló en el informe pasado, es bastante específico respecto de los requisitos. De esta forma, para solicitar datos de tráfico o georreferenciación del usuario, la autoridad debe contar

63 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/notificacion-modelo-kgd_20190605.pdf [Fecha última consulta: 7 de enero de 2021]

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, lo que 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 documento se reserva el derecho de rechazar las solicitudes cuando no cuenten con todos las exigencias establecidas y a notificar a los usuarios de las diligencias realizadas una vez que haya vencido el plazo de reserva de la diligencia.

Claro obtiene una estrella en esta categoría.

e) ¿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" del sitio web, Claro ha puesto a disposición una serie de documentos relativos a 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.[64] 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 de un agente de ventas de verificar rigurosamente la identidad del comprador. De esta forma, no puede considerarse como una forma de defensa de los derechos del usuario. Algo similar suce-

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

de 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, y no puede considerarse como una medida de defensa de los derechos del usuario.[65]

Adicionalmente, Claro ha puesto a disposición del público información referente a dos oficios recibidos por parte del Sernac, correspondiente a la negación a entregar los datos personales de sus clientes, cuestión que no fue reparada por parte del Sernac.

Por último, hacemos presente que se han tenido a la vista las ultimas minutas de relacionamiento con la autoridad que dan cuenta de ciertas acciones desplegadas por Claro en relación con la ley de protección de datos personales.

Sin perjuicio de todo lo anterior, instamos a Claro Chile a tomar una posición más activa en el debate legislativo sobre notificación a los afectados por medidas de investigación intrusivas.

Claro obtiene tres cuartos de estrella en este ítem, *en atención a las gestiones realizadas.*

Entel

a) ¿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.[66]

Entre estos documentos encontramos las versiones de su "Política de Privacidad Clientes Entel" de junio 2019, noviembre 2020 y marzo 2021. Consideramos una ventaja poder ver las políticas de privacidad de años anteriores, permitiendo con ello comparar con mayor facilidad los cambios efectuados entre uno y otro documento.

Entre los cambios realizados es posible encontrar mejoras, pero también retrocesos. Entre los primeros, destacamos las mejoras progresivas realizadas en relación con los principios mencionados en la metodología, muchos de los que se encontraban recogidos de forma más o menos directa por la política de privacidad de 2020, pero

65 Documento disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Respuesta-derechos-%20ARCO_20190606.pdf [Última fecha de revisión, 30 de junio de 2019].

66 Disponible en: https://www.entel.cl/legales/ [Fecha última consulta: 28 de abril de 2021]

que la política de 2021 ha incorporado en su totalidad y de manera expresa, aunque con algunos matices. Asimismo, celebramos el haber incorporado un punto de contacto específico para que los usuarios puedan canalizar toda solicitud e inquietud en relación con sus datos personales.

Además, hacemos presente el interés mostrado por Entel en mejorar su política de privacidad. Por ejemplo, durante la preparación del presente informe, advertimos a Entel nuestra preocupación por el hecho que la política de 2020 eliminara la referencia al deber de Entel de modificar o eliminar aquellos datos que dejaran de cumplir su función. La empresa, haciendo suya la observación, reincorporó dicha oración en la política de 2021. Asimismo, se comprometió a vincular la política de privacidad en los modelos de contratos de suministro.[67]

Como contrapartida, vemos como un retroceso la eliminación del compromiso de Entel de reservarse el derecho a cuestionar las solicitudes de la autoridad cuando no cumplan con los requisitos legales. Si bien su eliminación no significa necesariamente una renuncia a dicho derecho, consideramos que la declaración eliminada marcaba una postura más celosa de los derechos de sus clientes.

También vemos con preocupación los cambios realizados a la sección "Para qué usamos tus datos". En las versiones de la política de 2019 y 2020, Entel se comprometía de forma expresa a no compartir los datos de sus clientes con terceros, excepto para comunicaciones comerciales, quienes en todo caso debían usar los datos exclusivamente para el envío de dichas comunicaciones. Como contraste, en la política de 2020 se ampliaron significativamente los casos en que los datos podrían ser comunicados (para fines autorizados), y se eliminó la limitación referida al uso que los terceros pueden hacer de los datos que Entel les comunique.

Por último, advertimos que, a pesar de los cambios realizados, se mantiene un error en cuanto a las hipótesis que le habilitan para tratar datos personales sin el consentimiento de las personas en virtud del artículo 4 de la ley Nº 19.628. La redacción del primer párrafo de la sección "Compromisos Entel" da a entender que dicho artículo contendría cuatro hipótesis habilitantes distintas, en circunstancias en que la ley es clara en que no se trata de cuatro hipótesis distintas, sino que todas se encuentran circunscritas al hecho de tratarse de datos provenientes de fuentes accesibles al público. En otras palabras, no es correcto decir (ni dar a entender) que la ley autoriza al tratamiento —sin consentimiento— de datos de carácter económico,

67 Disponibles en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P63200157451364998548342 [Fecha última consulta: 10 de enero de 2021]

financiero, bancario o comercial, sin más; por el contrario, estos datos solo podrán ser tratados sin consentimiento en la medida que se encuentren en fuentes accesibles al público.

Entel obtiene tres cuartos de estrella en este ítem. Instamos a la compañía a modificar la redacción de la cláusula referida al artículo 4 de la ley 19.628, de manera de reflejar el verdadero sentido de dicha norma.

b) ¿Cuenta la empresa proveedora con un informe de transparencia?

En el sitio web de Entel es posible encontrar públicamente disponible un informe de transparencia revisado en marzo de 2021.[68] A diferencia de los otros años, este informe presenta, a modo de resumen, dos gráficos distintos: 1) solicitudes judiciales y 2) solicitudes de interceptación. 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 84.447 de solicitudes de información, lo que presenta un alza de 32% en relación al número de solicitudes recibidas el año 2019. Por el otro lado, en 2019 recibió un total de 57.207 de solicitudes de información, lo que presenta un alza de 8,7% en relación con el número de solicitudes recibidas el año 2018. Como punto destacable es que, pese a que no se puede acceder directamente al informe de transparencia del año pasado, el gráfico señala específicamente cuántas solicitudes hubo en los años 2018 y 2019.

En cuanto a las solicitudes de interceptación, el documento da cuenta que durante el 2020 se recibieron 11.212 solicitudes de interceptación telefónica, lo que presenta un alza de 22% en relación con el total de solicitudes de interceptación recibidas el año 2019. Durante el 2019 recibieron un total 8.749 solicitudes de interceptación telefónica, lo que presenta un alza de 8,2% en relación con el total de solicitudes de interceptación recibidas el año 2018. Y, al igual que el gráfico anterior, se pueden apreciar los números de interceptaciones de años anteriores.

68 Disponible en: https://www.entel.cl/legales/public/pdf/Informe-de-Transparencia-Requerimientos_de_Datos_Personales_2021.pdf [Fecha última consulta: 28 de abril de 2021] .
Este último informe de transparencia corresponde a un informe corregido, luego que durante la realización de este proyecto se advirtiera a Entel sobre la discrepancia existente entre los datos presentados en los informes de 2019 y 2020, específicamente en la sección de solicitudes de información. Así, el informe del 2019 (disponible hasta enero de 2021 en el sitio web de Entel) mostraba que en enero del 2018 se realizaron 4.965 solicitudes de información, en circunstancias que el informe de 2020 señalaba que en enero de 2018 se realizaron 4.090 solicitudes. Por otra parte, el informe de 2019 indicaba que en febrero hubo 3.570, y el de 2020 3.445. Asimismo, el informe de 2019 mostraba 7.665 solicitudes en marzo, y el de 2020 4.346. Valoramos la corrección del informe de transparencia y el compromiso manifestado por Entel en orden mejorar sus procesos internos para la generación de los informes, para evitar que este tipo de errores vuelvan a ocurrir.

Entel obtiene tres cuartos de estrella. *Instamos a la compañía profundizar en el nivel de detalles que entrega, desagregando la información de sus futuros informes, por ejemplo, mediante un criterio geográfico.*

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

En la "Guía informativa acerca de las solicitudes de la autoridad de interceptaciones e información personal", publicada el 27 de noviembre de 2020, Entel declara que tiene el deber legal de resguardar la confidencialidad y reserva de la información de sus clientes y que, en caso de ser requerido por resolución judicial, deberá evaluar según las circunstancias de proceder a la notificación a sus clientes. Sin embargo, no queda claro en qué casos Entel podría considerar procedente dicha notificación y en qué casos no, y solo se reserva el derecho a realizar dichas notificaciones, más no se compromete a hacerlo en aquellos casos que fuera procedente.

Por otro lado, Entel no participó ni mostró interés en la discusión legislativa de finales de 2020, sobre notificación de solicitudes de información de autoridades estatales.

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

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?

Entel cuenta con una guía bastante completa respecto a los procedimientos y requisitos que debe cumplir la autoridad para que la empresa dé curso a una solicitud de acceso o entrega de información de los usuarios.

Este documento, que se encuentra disponible públicamente en la página web[69] de Entel, ha tenido mínimos cambios respecto del año pasado y detalla los requisitos que Entel exige a la autoridad, 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,

69 Documento disponible en: https://www.entel.cl/legales/public/pdf/guia_solicitud_judiciales.pdf [Fecha última consulta: 4 de mayo de 2021].

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, 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.

Dicha guía fue modificada solo en un punto para darle mayor protección a los clientes, declarando Entel que se encuentra comprometido con la fiel e íntegra protección de los datos personales de sus clientes, velando por el resguardo y la confidencialidad de estos.

Entel obtiene una estrella en este ítem.

e) ¿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?

Sobre este punto, el suceso más relevante desde la última versión de este informe está representado por un avance en una causa judicial cuya resolución final se encontraba entonces pendiente. 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 postpago, 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 a CADEM, una empresa que realiza encuestas de satisfacción de usuarios.

Como expresamos en la última versión de este informe, esta solicitud es preocupante por varias razones y 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.[70] A pesar que el oficio fue enviado a todas las compañías que son parte de este estudio, Entel fue la úni-

70 Este caso específico fue analizado por María Paz Canales en la siguiente columna: https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/ [Fecha última consulta: 18 de enero de 2021].

ca 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 entrega de la información.[71]

Fallado lo anterior, el Consejo de Defensa del Estado, en representación del Ministerio de Transporte y Telecomunicaciones y de la Subsecretaría de Telecomunicaciones, interpuso un recurso de queja, el que fue desechado con fecha 12 de noviembre de 2019 por la Corte Suprema. No obstante, actuando de oficio, la Corte Suprema dejó sin efecto la sentencia de la Corte de Apelaciones y en su lugar confirmó las sanciones originalmente impuestas por la Ministra de Transporte y Telecomunicaciones, pero estableciendo que la multa de 0.25 UTM por cada día transcurrido sin que Entel hubiera dado cumplimiento a la orden de Subtel solo podría computarse desde que se haya notificado el fallo que la establece de manera definitiva.

El caso comentado resulta relevante, al ser el primer caso de defensa de los usuarios ante tribunales que ha sido reportado desde que este informe fue inaugurado en 2017 y es un ejemplo de cómo una empresa puede recurrir ante tribunales de justicia –arriesgando importantes multas– con el fin de proteger la privacidad y los datos personales de sus clientes. Cabe destacar que Entel fue la única de las empresas requeridas por Subtel que se opuso a la entrega de la información de sus usuarios.

Por todo lo descrito anteriormente, **Entel obtiene tres cuartos de estrella en este ítem.** *Esperamos que para una próxima versión existan nuevas actuaciones que apunten en la misma dirección que la causa culminada en 2019.*

GTD Manquehue

a) ¿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?

En su página web GTD Manquehue pone a disposición tres contratos generales. El primero es una copia de su contrato de servicios de

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

telecomunicaciones con las condiciones generales de contratación;[72] el segundo es sobre condiciones de solicitud y contrato de servicios,[73] sin diferencia entre móvil y fijo, prepago o plan; y finalmente uno referido a las condiciones generales de contratación de suministro de servicio telefónico móvil.[74]

En relación con este último documento, hacemos presente que durante la elaboración del presente informe se advirtió a GTD Manquehue sobre la ausencia de toda referencia a la ley N.º 19.628 y a la protección de los datos personales de sus clientes a los derechos ARCO,[75] con la sola excepción de la información que se entregaba a los clientes para que pudieran realizar cambios respecto de sus datos personales, dentro de la sección sobre atención al cliente. Frente a lo anterior, GTD Manquehue tomó una actitud activa y constructiva, modificando el documento en cuestión, por lo que actualmente es posible encontrar información relativa a la protección de los datos personales, específicamente en el numeral 13 del documento.

En el contrato de condiciones de la solicitud y el contrato de servicios GTD Manquehue en su punto número 11 insinúa que el tratamiento de los datos se hará conforme a dos reglamentos, tanto una política de privacidad que se encuentra en la web de GTD Manquehue, a la cual se enlaza, y al punto número 10 de las condiciones generales de contratación.

Y es en estas condiciones generales donde la empresa contempla una cláusula específica (punto número 10) para el tratamiento de los datos personales. Dicha disposición afirma que todos los datos personales proporcionados por el suscriptor serán tratados, almacenados y resguardados conforme a las condiciones estipuladas en la ley Nº 19.628, sobre la "Protección de Datos de Carácter Personal y la Política de Privacidad" de GTD Manquehue.

En el segundo párrafo podemos ver establecido el principio de finalidad, al afirmar GTD Manquehue que el tratamiento y utilización de los datos personales entregados por el cliente a GTD Manquehue ten-

72 GTD MANQUEHUE. Condiciones Generales de Contratación de Servicios de GTD MANQUEHUE S.A. En línea, disponible en: https://www.gtd.cl/condiciones-comerciales/contratos-de-servicios-gtd/condiciones-generales-de-contratacion-gtd-manquehue [Fecha última consulta: 17 de enero de 2021]

73 GTD MANQUEHUE. Solicitud y Contrato de Servicios GTD MANQUEHUE. En línea, disponible en: https://www.gtd.cl/condiciones-comerciales/contratos-de-servicios-gtd/solicitud-y-contrato-de-servicios-gtd-manquehue [Fecha última consulta: 7 de enero de 2021]

74 Disponible en: https://www.GTD Manquehue.cl/condiciones-comerciales/contratos-de-servicios-GTD Manquehue/condiciones-generales-de-contratacion-GTD Manquehue-movil [Fecha última consulta: 7 de enero de 2021]

75 El cambio de datos personales el suscriptor podrá realizarlo en cualquiera de las oficinas comerciales de la compañía, o a través de la plataforma de atención telefónica, previa verificación de identidad.

drá por finalidad "asegurar la correcta prestación de los servicios, y el envío de noticias, novedades, ofertas, promociones e información comercial al cliente". En el contrato, GTD Manquehue explica el procedimiento para poder modificar datos y para dejar de recibir información comercial, publicitaria, promociones u ofertas de entretenimiento.

Por último, celebramos uno de los mayores progresos alcanzados este año en que, a diferencia de los años anteriores, GTD Manquehue ahora cuenta con una política de privacidad. Destacamos, asimismo, que la política tenga fecha y cumpla con todos los estándares propuestos en la metodología de este informe, los que buscan que la industria avance hacia la protección permanente y efectiva los derechos de los titulares de los datos personales.

Dado lo anterior, y especialmente considerando los avances y el interés demostrado por la compañía en mejorar sus prácticas, **GTD Manquehue obtiene una estrella en este ítem.**

b) ¿Cuenta la empresa proveedora con un informe de transparencia?

Este año, por primera vez, GTD Manquehue entrega un informe de transparencia,[76] pero con fecha de 2019. En dicho informe se señala cuál es el marco normativo aplicable y entrega la información separada según tipo de solicitud recibida, señalando que el año 2019 fue requerida, por distintas autoridades, mediante un total de:

- Cero solicitudes de interceptación telefónica.
- Nueve solicitudes de información general.
- 27 solicitud de metadatos.

De dichas solicitudes, tres —casi un 10% — fueron rechazadas u objetadas, ya sea por antecedentes incompletos o incorrectos en el requerimiento, no adjuntar resolución judicial en los casos que aplica y, en general, el no cumplimiento de las exigencias establecidas en la normativa para proceder con la entrega de información.

Dado que aún no se encuentra publicada la información sobre las solicitudes de autoridad recibidas durante el año 2020, **GTD Manquehue recibe media estrella en esta categoría.** *Instamos a la compañía a actualizar la información disponible al público y a realizar avances en cuanto al detalle de la información que entrega y la forma en que la presenta.*

76 Disponible en: https://www.GTD Manquehue.cl/normativa/privacidad-y-proteccion-de-datos-personales/informe-de-transparencia [Fecha última consulta: 18 de enero de 2021]

c) ¿Notifica la empresa a los usuarios acerca de solicitudes de información de las autoridades estatales?

Al igual que muchas compañías que aparecen en este informe, GTD Manquehue establece la posibilidad de notificar a los clientes en caso de que hayan sido objeto de una solicitud de información por parte de la autoridad. Esta posibilidad está contemplada en el "Protocolo de requerimiento de información",[77] que señala que GTD Manquehue "se reserva el derecho de notificar a los clientes en caso de no existir deber de confidencialidad o reserva respecto del requerimiento de información, o haya expirado el plazo de reserva de la diligencia de investigación, siempre que esto sea posible y se cumplan los requisitos legales aplicables".

El problema se repite, entonces, porque no hay un criterio claro de cuándo se va a notificar a los clientes la existencia de una vulneración a su privacidad.

GTD Manquehue recibe **un cuarto de estrella** *en esta categoría.*

d) ¿La empresa publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?

Como se adelantó, GTD Manquehue ahora cuenta con un protocolo de requerimiento de información.[78] Dicho documento parte declarando el compromiso que adoptó GTD Manquehue con la privacidad y protección de los datos de sus clientes y está dividido según el tipo de información que se quiera solicitar: de registro de tráfico telefónico, de interceptación telefónica o de metadatos.

Tanto en las solicitudes de registro de tráfico telefónico, como en las de interceptaciones telefónicas y solicitud de informe de metadatos, GTD Manquehue exige que se adjunte la resolución judicial correspondiente, entre otros antecedentes. Hacemos presente que la mención expresa al requisito de una orden judicial a efectos de solicitar metadatos es una novedad surgida en el transcurso de elaboración del presente informe, por lo que reconocemos, una vez más, el interés demostrado por GTD Manquehue para mejorar sus políticas de tratamiento y protección de datos personales.

Con todo, aún hay aspectos que podrían mejorar. Por ejemplo, la información entregada no es clara respecto al tiempo durante el cual guarda la información de los clientes, así como de la eliminación de

77 Disponible en: https://www.GTD Manquehue.cl/normativa/privacidad-y-proteccion-de-datos-personales/requerimientos-de-informacion [Fecha consulta: 18 de enero de 2021]

78 Ibíd.

esta, cosa que sí hacen otras compañías.

En síntesis, GTD Manquehue no solo cuenta por primera vez con un protocolo de requerimiento de información y un informe de transparencia, sino que durante la elaboración del presente informe mostró avances significativos en esta materia. Sin embargo, aún quedan aspectos que deben ser mejorados, especialmente cuando se trata de aspectos básicos a cuya necesidad nos hemos referido en los informes anteriores, cuestión que no puede ser obviada.

Considerando lo anterior, **GTD Manquehue recibe tres cuartos de estrella**.

e) ¿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 acciones haya tenido lugar.

En relación con las acciones llevadas a cabo por ATELMO en defensa de los derechos de las personas, por ejemplo, en discusiones en torno a la protección de los datos personales ante el Consejo para la Transparencia y ante Contraloría, valoramos y felicitamos la participación de GTD Manquehue al ser parte de dicha organización. Sin embargo, para efectos de este parámetro, solo se toman en consideración aquellas acciones llevadas a cabo en forma individual por las compañías.

El proveedor no obtiene estrella en esta categoría. *Instamos a GTD Manquehue a tomar un rol más activo en la defensa y protección de los derechos de sus clientes.*

5. Tabla de **resultados**

¿QUIÉN DEFIENDE TUS DATOS? 2021

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

LA EMPRESA PROVEEDORA DE INTERNET	WOM	Movistar	VTR	Claro	Entel	GTD
¿Tiene publicado 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 de las autoridades estatales?	★	☆	☆	★	☆	☆
¿Publica el procedimiento, los requisitos y las obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios?	★	★	★	★	★	★
¿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?	★	★	☆	★	★	☆
*De un máximo de **5 estrellas,** obtiene:*	**3,5** ★★★½☆	**3,25** ★★★☆☆	**1,25** ★☆☆☆☆	**4,75** ★★★★★	**3,5** ★★★½☆	**2,5** ★★½☆☆

La escala de medición indica que:

★ cumple todos los parámetros

★ cumple casi satisfactoriamente

★ cumple parcialmente

★ cumple de forma insuficiente

☆ no cumple :(


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina