2022

¿QUIÉN DEFIENDE TUS DATOS?

Michelle Bordachar

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

¿QUIÉN DEFIENDE TUS DATOS?

Chile 2021-2022

Portada y diagramación: **Catalina Viera**
Edición y correcciones: **Belén Roca**

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

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales.

Septiembre, 2022.

Contenido

1. Introducción

El presente informe corresponde a la quinta 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, pero también en relación con las prácticas de tratamiento de datos personales de las propias empresas.

¿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 la información disponible al público de los proveedores de servicios de telecomunicación más grandes de Chile: Claro, Entel, GTD Manquehue, Movistar, VTR y WOM.

El énfasis está puesto en evaluar hasta qué punto las empresas defienden la privacidad de sus usuarios ante las solicitudes de la autoridad y frente al tratamiento indebido de datos personales que terceros pudieran pretender hacer, así como la transparencia con la que las propias compañías tratan los datos personales de sus usuarios. Considerando los buenos resultados que ha tenido este informe, nos propusimos ir más allá y subir el estándar en relación con la evaluación realizada por última vez en el año 2021.[1] En esta quinta edición buscamos responder las siguientes preguntas: ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias? ¿Cuentan las empresas proveedoras con un informe de transparencia actualizado que entrega información de calidad? ¿Notifican a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, han realizado esfuerzos concretos para ello? ¿Cuentan con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias? ¿Han defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

1 Disponible en: https://www.derechosdigitales.org/wp-content/uploads/quien-defiende-tus-datos-2019.pdf [Fecha última consulta: 29 de mayo de 2021]

Estas preguntas se traducen en algunos cambios cualitativos en la metodología respecto de los años anteriores. Estas novedades en la metodología son posibles gracias a los avances mostrados por la industria desde los inicios de este estudio, haciendo que varios de los criterios de evaluación iniciales pasarán a formar parte de un piso mínimo, lo que dio espacio a la incorporación de otros criterios de evaluación que permiten un análisis más exhaustivo de las prácticas y documentos de las empresas;[2] pero también se explican en gran medida por los desafíos planteados por dos situaciones específicas de los últimos años. En primer lugar, las protestas sociales desplegadas durante el año 2019, que aumentaron en forma drástica la vigilancia estatal y persecución penal con ayuda de las tecnologías de comunicación; en segundo lugar, por la pandemia por Covid que nos afecta desde el año 2020, aumentando nuestra dependencia a los medios tecnológicos y, por tanto, la comunicación de nuestros datos personales. Estas situaciones evidencian cómo la tecnología y las telecomunicaciones forman parte fundamental de nuestra vida, haciendo necesario evaluar 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).

Entre las novedades, este año sí se asignará puntaje al criterio a evaluar incorporado en la metodología del informe pasado, referido a si las empresas hacen explícito que toda solicitud de información acerca de un individuo que contenga datos personales sensibles, tales como la geolocalización, requiere no solo de una orden judicial previa, sino que además debe referirse a personas determinadas, excluyendo la posibilidad de solicitar este tipo de información respecto de una colectividad de usuarios indeterminados, y que para el caso de requerimientos de autoridad para el desarrollo de políticas públicas, la información relativa a la ubicación de las usuarias solo puede ser entregada a la autoridad competente y de forma anonimizada y agregada. Otra de las novedades es la evaluación del grado de compromiso de las empresas con el resguardo de la información de sus usuarios, con especial enfoque en el manejo seguro de los datos, lo que se traduce en la exigencia a las empresas de criterios de transparencia respecto a los convenios suscritos con instituciones públicas y privadas para comunicación y transferencia de información personal o estadística de sus usuarios, y si explican claramente a sus usuarios los casos en que sus datos han sido administrados por terceros, así como las medidas que han tomado para su protección,

2 El informe del año 2019 mostró que todas las empresas cumplen con publicar sus contratos y políticas de privacidad, así como la guía referida al procedimiento, requisitos y obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de las usuarias. Asimismo, todas las empresas analizadas cumplieron con hacer esta documentación de fácil acceso, y —con la sola excepción de VTR— con publicar informes de transparencia actualizados.

los usos dados a los datos de las usuarias, la forma cómo estos se manejan y almacenan, y la comunicación al público sobre la existencia de flujo transfronterizo de datos.

Por otra parte, considerando que la modificación constitucional —de mediados de 2018— que incorporó la protección de los datos personales al catálogo chileno de derechos fundamentales, junto con la agenda política del último tiempo, marcada por la necesidad apremiante de regular las tecnologías, han impulsado una serie de discusiones legislativas referidas a diversos temas que impactan de una u otra manera la protección de la privacidad y de los datos personales de las personas (v.gr.: teletrabajo,[3] acceso a internet como una necesidad y luego como un derecho para profesores y estudiantes,[4] actualización de la normativa sobre delitos informáticos,[5] etc.), se ha hecho necesario también evaluar la participación que las compañías han tenido en estas discusiones.

En línea con lo anterior, nuestro informe nunca ha estado ajeno a los distintos desarrollos y acontecimientos que se relacionan con el mercado de las telecomunicaciones, y el año 2021 sin duda estuvo marcado por el avance de proyectos de ley que buscan propiciar políticas públicas de vigilancia y ampliar las hipótesis de aplicación de medidas intrusivas de investigación; y por distintos casos de interceptaciones ilegales, siendo los más graves el del periodista Mauricio Weibel,[6] a nivel local, y el de Pegasus a nivel internacional.[7] Este último salió a la luz gracias a una iniciativa internacional de periodismo de investigación que reveló cómo algunos gobiernos vigilaban a periodistas, políticos de la oposición, activistas, empresarios y otras personas mediante un software privado de espionaje llamado Pegasus, desarrollado por NSO Group, una empresa de tecnología y ciberarmas de origen israelí.[8] Casos como los señalados demuestran que la interceptación ilegal de comunicaciones es una realidad y no una preocupación infundada, poniendo de manifiesto la necesidad de velar porque este tipo de medidas —en aquellos casos en que sean legales— no sean utilizadas en forma abusiva o para fines distintos a los establecidos por el legislador para consagrarlas legalmente.

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

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

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

6 **https://www.ciperchile.cl/2021/04/30/interceptacion-telefonica-y-espionaje-del-que-ha-sido-objeto-el-periodista-mauricio-weibel-y-otros-profesionales-lesiona-la-democracia/** [Fecha última consulta: 19 de agosto de 2022]

7 Ver: **https://oas-org.zoom.us/rec/play/Do3mn9kfW-iyPHTEUkRRjB7oZoA-4pkLpY_JMvOovX2ilDnlj7SEJ8iN5z1qrKV8ic-z169OK_eJ2jiqZ.jQT6iWVjG7b0JYvc** [Fecha última consulta: 19 de agosto de 2022]

8 Un informe de Amnistía Internacional sobre la información filtrada acerca de este programa mostró que hubo más de 50 países involucrados y más de 50.000 números telefónicos interceptados. Disponible en: **https://www.amnesty.org/es/latest/news/2021/07/the-pegasus-project/** [Fecha última consulta: 10 de enero de 2021]

2. Metodología

La metodología para la elaboración del informe QDTD 2021[9] no tuvo cambios significativos en relación con los criterios de la versión que le antecedió. Ello, con el objeto de poder comparar los avances de la industria de las telecomunicaciones, que durante el año 2019 mostró resultados muy dispares, producto del salto cualitativo en la forma en que **Quien Defiende Tus Datos** evaluó el nivel de protección que las empresas de telecomunicaciones entregan a los datos de sus usuarios.

En relación con la protección y defensa de los derechos de sus usuarios, especialmente en materia de privacidad y protección de datos personales, en 2019 por primera vez pasamos de un análisis más bien formal (publicación de términos y condiciones, informes de transparencia, etc.) a un análisis más profundo, que evaluará el contenido de los términos y condiciones ofrecidos por las distintas empresas de telecomunicaciones a sus usuarios.

La última versión de este informe tuvo un enfoque en las políticas públicas, en virtud de las excepcionales circunstancias por las que atravesaba el país para volver a una normalidad controlada, tras la pandemia que nos sigue afectando. Por esto, se agregaron varios criterios nuevos como, por ejemplo, la exigencia de que toda solicitud de información acerca de un individuo que contenga datos personales sensibles, tales como la geolocalización, no solo debe contar con una orden judicial previa, sino que también ser de carácter individual, y el compromiso de que la información relativa a la ubicación de las usuarias que sea requerida para efectos de políticas públicas solo sea entregada a la autoridad de forma anonimizada y agregada. Otro criterio evaluado es si las empresas transparentan el tiempo de almacenamiento junto con el proceso de eliminación que se aplica a los metadatos transcurridos los plazos respectivos. Si bien en la última edición de este informe estos criterios no fueron considerados para la asignación de puntaje, felizmente muchas de las empresas decidieron incorporarlos expresamente en sus distintas políticas y protocolos. Dado lo anterior, este año sí evaluamos estos criterios para incentivar mejoras transversales entre las distintas empresas.

Si bien no hemos vuelto completamente a la normalidad, la población ya no se encuentra sometida a políticas públicas tan agresivas como las que marcaron el enfoque de la última versión del informe QDTD. Con la llegada de la (nueva) normalidad, el informe QDTD vuelve a su enfoque original, exigiendo un rol más activo de los actores evaluados, buscando que las empresas aboguen por los derechos de sus usuarios.

9 Disponible en: **https://www.derechosdigitales.org/wp-content/uploads/QDTD-2021.pdf** [Fecha última consulta: 10 de enero de 2021]

Los años 2021 y 2022 han mostrado un aumento significativo de las iniciativas y políticas públicas relacionadas con el acceso a datos personales, al tiempo que la apertura digital que vivió el país a raíz de la pandemia aumentó la información que compartimos mediados por el uso de las telecomunicaciones. Por ello, una de las principales novedades de este informe es la introducción de nuevos criterios que buscan incentivar un rol más activo por parte de las empresas de telecomunicaciones en la defensa los derechos de sus usuarios, por ejemplo, mediante su participación en instancias legislativas, especialmente en aquellos proyectos de ley que amenazan el derecho a la privacidad y a la protección de los datos personales (vgr.: el proyecto de ley de Delitos Informáticos, el de Prepago, entre otros).

Por otra parte, durante el tiempo transcurrido desde la primera versión de QDTD Chile a la fecha, hemos visto cómo las empresas han fortalecido sus políticas internas para adecuarlas a un estándar cada vez más alto, sin embargo, la protección de la información de las usuarias escapa del ámbito de control de las compañías cuando es compartida con terceras partes. Por ello, este año también decidimos considerar la forma como las empresas de telecomunicaciones cuidan la seguridad del tratamiento de datos, y los resguardos que toman cuando comunican a terceros tanto dentro como fuera del territorio nacional. Por último, este año seguimos evaluando si las empresas comunican los cambios que introducen en sus contratos y políticas de privacidad, pero con un mayor nivel de exigencia, tomando en consideración la existencia de un compromiso de notificar dichos cambios, si los documentos señalan la fecha de entrada en vigor de los documentos publicados, si las empresas mantienen a disposición del público las versiones anteriores de sus contratos y políticas de privacidad, etc.

En otra arista, los informes de transparencia también han mostrado grandes avances durante los años que hemos realizado QDTD. Para continuar mejorando la calidad de estos informes, y en orden a contar con información más clara acerca de cómo operan los requerimientos de información que las distintas autoridades hacen a las empresas, este año hemos solicitado conocer en mayor detalle el tipo de datos que son entregados.

Finalmente, volvemos a hacer hincapié en la importancia del rol que pueden cumplir las empresas de telecomunicaciones en la generación de un sistema de notificaciones en orden a asegurar que las autoridades respectivas cumplan con su obligación de notificar a las personas afectados por medidas investigativas intrusivas en los casos y conforme a los términos establecidos en la ley. Esto, pues, como bien es sabido por las empresas de telecomunicaciones, en la actualidad las autoridades no dan cumplimiento a la obligación de notificación establecida en el artículo 224 del Código Procesal Penal, bajo pretexto de ser un trámite de difícil ejecución.

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

Siguiendo el espíritu del informe pasado, las políticas de privacidad y contratos de las empresas deben reflejar un compromiso sustantivo con la defensa de las usuarias, su privacidad y la protección de sus datos personales. Para que las empresas cumplan con el estándar de protección que se espera, se tendrán en cuenta elementos que van 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,[10] sumados a dos principios que no se encuentran en la legislación actual: el principio de minimización de datos y el principio de lealtad. Para ello, se analizarán los términos y condiciones a la luz de los principios contenidos en el texto del proyecto de ley de datos personales que se encuentra en segundo trámite constitucional en nuestro Congreso[11] aunque, al igual que en la edición pasada y teniendo en cuenta las posibles modificaciones que puede sufrir el proyecto de ley, hemos optado por una versión más genérica de estos principios que, por lo demás, son ampliamente 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 transparencia: exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

Principio de lealtad: la empresa se compromete a tratar los datos no solo de forma transparente y lícita, sino también de un modo leal, que demuestre un compromiso ético, que va más allá del estricto cumplimiento de la ley.

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.

10 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]

11 El texto del proyecto se encuentra disponible en: **https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07** [Fecha última consulta: 14 de junio de 2022]

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 medidas técnicas y organizativas que estén a su alcance, 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, solo entregando acceso a terceros cuando el titular haya consentido expresamente en ello o sea requerido por la autoridad cumpliendo los requisitos legales establecidos por el ordenamiento jurídico para dicho tipo de requerimientos.

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.

Por último, es importante recalcar que, para cumplir con estos principios, no será necesario que las políticas de privacidad o protección de datos de las empresas los mencionen explícitamente —aunque ello será valorado positivamente—.

Por otra parte, hacemos presente que, para la última versión de QDTD, todas las empresas analizadas cumplieron con el criterio de publicar en su página web los borradores de sus contratos, y la respectiva política de privacidad, aunque algunas no mantienen publicadas las versiones anteriores de sus contratos y políticas de privacidad, ni incluyen la fecha de su entrada en vigor o vigencia, especialmente en aquellos casos en que las compañías se reservan el derecho de introducir modificaciones sin previo aviso e incluyen una cláusula de aceptación tácita, en virtud de la cual todo cambio se entiende aceptado por el solo hecho de continuar utilizando los servicios. Consideramos que una cláusula como la señalada es abusiva, pero, además, si a las usuarias no se les otorga acceso a las versiones anteriores de la documentación que suscriben, ni se les informa de la fecha de entrada en vigor, resulta prácticamente imposible que puedan conocer las condiciones que les son impuestas.

Por ello, en adelante, la publicación de los contratos y la política de privacidad será considerada un piso mínimo y común de evaluación, con el cual todas las compañías deberán cumplir, y así dar paso a la incorporación de nuevos criterios de evaluación, derivados de la aplicación del principio de transparencia, a saber:

* **La empresa realiza una mención expresa a la existencia —o no— de flujo transfronterizo de datos, y bajo qué resguardos.**

* **La empresa informa a sus usuarios si comunica sus datos a terceros (o los casos en que dicha comunicación ocurre), la base jurídica y finalidades de dicha comunicación, así como los resguardos que ha tomado para que dichos terceros traten los datos con igual o mayor nivel de cuidado.**

* **La empresa informa con claridad sobre el tratamiento que hace de los datos de las usuarias, especialmente, informando en detalle las categorías de datos recolectados, las finalidades para las cuales podría tratar cada categoría de dato que recopila; el tiempo máximo de almacenamiento de los datos, y la forma de eliminación de esta información una vez transcurrido el plazo de almacenamiento.**

* **La empresa mantiene a disposición del público las versiones anteriores de sus contratos y políticas de privacidad, toda la documentación tiene consignada su fecha de entrada en vigor, y la carga de revisar las modificaciones no es traspasada a las usuarias.**

2.2. Informe de transparencia

Por segundo año consecutivo, este parámetro solo ha sufrido modificaciones menores. Durante el año 2020, todos los proveedores analizados, con la sola excepción de VTR, contaron con un informe de transparencia actualizado. Por ello, de manera similar al caso anterior, dicho criterio pasó a formar parte de un piso mínimo común con el que todas las encuestadas deberán cumplir. Sin embargo, el nivel de granularidad de los informes sigue siendo difícil, por lo que seguiremos evaluando que las empresas expliciten el número y porcentaje de las solicitudes que fueron rechazadas por no cumplir con los requisitos legales, así como también el número de órdenes judiciales que recibe, con indicación de cuántas de estas se refieren a una pluralidad de individuos.

Del mismo modo, se agregan los siguientes nuevos criterios para evaluar de mejor manera la calidad de la información entregada por los proveedores:

Se tendrá en consideración si las empresas desglosan la información relativa a las solicitudes recibidas, diferenciando aquellas solicitudes que provienen de alguna autoridad fuera del contexto de un proceso penal o sin contar con una orden judicial, de aquellas que provienen de órdenes judiciales; y detalla las categorías de datos que le han sido requeridas al proveedor, así como todas las categorías de datos que ha comunicado a terceros.

Se exigirá que las empresas presenten la información de forma desagregada, estableciendo el número de solicitudes que solicitan acceso a los metadatos[12] 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.

Igualmente, evaluamos si el informe de transparencia desglosa la información según si las solicitudes de información recibidas se refieren a un individuo en particular o a una colectividad (v.gr.: información de todos los teléfonos celulares conectados a una antena determinada, durante un periodo de tiempo determinado); el número de órdenes judiciales rechazadas y el motivo del rechazo.

También evaluamos si las empresas de telecomunicaciones informan a sus usuarios por cuanto tiempo máximo almacenan sus metadatos de comunicaciones y si estos son eliminados transcurrido el tiempo exigido por la ley para su retención por parte de las ISP.

12 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.

Además, este año solicitamos a las empresas incluir información sobre las solicitudes que hayan recibido para bloquear o filtrar contenido, bloquear acceso a sitios web, o suspender temporalmente el servicio.

Por último, si bien no es necesario que conste en el mismo documento del informe, este año también valoramos que las empresas transparenten la existencia de convenios suscritos con instituciones públicas y/o privadas para la comunicación de información personal o estadística de sus usuarios (incluso para efectos de iniciativas de investigación).

2.3. Notificación a las usuarias

La notificación a las usuarias sigue siendo el parámetro de menor cumplimiento. En la versión anterior del informe QDTD solo una empresa implementó un sistema de notificación a sus usuarios, y limitado respecto de causas civiles y de familia, más no de carácter penal.

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

Atendido el interés demostrado por las compañías, y especialmente que el secreto de las diligencias judiciales es la excepción en nuestro ordenamiento jurídico, que tal secreto extendido en el tiempo terminaría produciendo indefensión en las personas afectadas; y la obligación legal de notificar a la persona afectada por una medida intrusiva cumplidos los requisitos establecidos en la propia ley, la metodología de este año continuará evaluando positivamente a aquellas empresas que establezcan algún mecanismo de notificación para sus usuarios que hayan sido objeto de medidas intrusivas respecto de las cuales no tengan obligación de secreto (v.gr.: en causas de familia o laborales). También volveremos a evaluar si las empresas han tenido iniciativas concretas para implementar un sistema que a futuro permita notificar a las usuarias que han sido objeto de medidas intrusivas de investigación en el marco de un proceso penal, ya sea que estas acciones se hayan desarrollado a través de un diálogo con las autoridades pertinentes, mediante su participación en instancias legislativas, o de otra manera. Aquellas empresas que hayan hecho público este interés obtendrán una fracción de estrella adicional.

Por todo lo señalado precedentemente, y en especial consideración de la discusión legislativa sobre la obligación legal de notificar a las personas afectadas por medidas investigativas intrusivas, que se dio tanto en el marco del proyecto de ley de Delitos Informáticos, como en el Proyecto de ley Prepago, este año pusimos especial atención en el interés demostrado por las empresas encuestadas en la defensa de los derechos de sus usuarios en estas instancias legislativas.

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

Con este parámetro se busca constatar que las empresas cuenten con una pauta públicamente disponible que establezca cuales son los requisitos que la autoridad debe cumplir para que una solicitud de información o de interceptación de comunicaciones sea considerada legítima, es decir, con apego a la ley.

En la actualidad todos los proveedores cumplen con hacer públicos y de fácil acceso los documentos referidos a los procedimientos, requisitos y obligaciones legales que las autoridades estatales deben cumplir al requerir información personal de sus usuarios. En virtud de este gran avance demostrado por la industria, en adelante dichos criterios forman parte del piso mínimo y común con que deberán cumplir todas las ISP, para así poder dar lugar a nuevos criterios de evaluación.

Así, si bien seguimos valorando la exigencia de una orden judicial previa para entregar información de sus usuarios, ahora también se evaluará si la empresa hace explícita la obligación legal de notificar a las personas afectadas por una medida investigativa intrusiva, en los términos señalados en el artículo 224 del código procesal penal[13].

Asimismo, este año nuevamente se 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 referirse a personas determinadas, pero además se exigirá que la empresa explicite que cuando se trate de información relativa a la ubicación de sus usuarios para efectos de políticas públicas, esta solo podrá entregarse a la autoridad de forma anonimizada y agregada.

Por último, este año también evaluaremos que las empresas informen sobre el tiempo máximo durante el cual almacena metadatos, y la forma de eliminación de esta información una vez el tiempo durante el cual la guarda.

13 Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=176595&idParte=8646783 [Fecha última consulta 14 de junio 2022]

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

Una empresa que defiende la privacidad y la protección de los datos de sus usuarios debe demostrar una conducta activa para la defensa y protección de aquella información que recolectan y a cuyo resguardo y seguridad están obligadas. Para conocer el verdadero nivel de compromiso de las empresas con la protección de los derechos y la seguridad de sus usuarios, en este parámetro tomamos en consideración aquellas acciones llevadas a cabo por las compañías para el resguardo, promoción y defensa activa de los derechos de sus usuarios, que muestran una coherencia entre las declaraciones y las acciones de las compañías.

Desde que, a raíz del estallido social de octubre de 2019, se evidenciara el uso intensivo de datos de comunicación para la investigación y persecución penal, este punto se volvió de especial relevancia. A ello se suma la circunstancia de la pandemia y la implementación de medidas de confinamiento, que obligó a mantener atención sobre la realización de posibles actos de vigilancia por parte 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.

Para estos efectos, entre los aspectos que son evaluados positivamente para el análisis están 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; y, en general, cualquier acción comprobable y significativa, entre las que destacamos toda participación en la esfera legislativa 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. Esta última resulta esencial, dado que muchas de las medidas investigativas intrusivas que contempla nuestro ordenamiento jurídico y los respectivos proyectos de ley, se relacionan directamente con las empresas de telecomunicaciones, al ser estas las que han de proveer parte de los medios para llevar a cabo dichas medidas.

En cuanto a los mencionados proyectos de ley, destacamos el **Boletín 12042-15**, que modifica la ley N° 18.168, General de Telecomunicaciones, en materia de individualización y registro de datos de las usuarias de servicios de telefonía en la modalidad de prepago

(Proyecto de ley Prepago), que busca realizar estas modificaciones con el objetivo de obligar a las usuarias de telefonía móvil en modalidad de prepago a proporcionar información que permita su individualización en un registro que haga posible la identificación de las usuarias (y el bloqueo de aquellos equipos y números telefónicos que no hayan sido registrado en los plazos fijados por ley); y el proyecto de ley **Boletín 12192-25** que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest (el proyecto de ley de Delitos Informáticos).

2.6. Aspectos generales de la evaluación

Al igual que en el informe anterior, en ciertos casos excepcionales podríamos asignar una puntuación mayor a la estrictamente correspondiente en aquellos casos en que consideramos que una empresa se encuentra notoriamente cercana a satisfacer los indicadores fijados para un parámetro. Intentamos así reflejar de mejor forma los matices de cumplimiento entre distintas compañías, evitando modificar la escala de calificaciones de una forma que menoscabe la claridad de la información. Cuando así suceda, se dejará constancia de las oportunidades de mejora que existan 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 se subdivide en distintos criterios, cada uno de los cuales tiene asignada una puntuación, de manera que la calificación no estará limitada a media estrella o una estrella completa, siendo posible también obtener ¼ o ¾ de estrella. Nos parece importante que, a medida que aumente el nivel de exigencia de las usuarias respecto de las condiciones de protección de sus derechos que ofrecen las empresas, este informe pueda realizar una medición más precisa, que entregue a las usuarias una visión más detallada los distintos niveles de cumplimiento y las condiciones ofrecidas por las ISP chilenas.

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

a) ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

Parámetros de la respuesta:

* La política de protección de datos coincide con la normativa nacional, y ofrece mecanismos para el ejercicio de los derechos, estableciendo un punto de contacto para hacer llegar la solicitud respectiva.

* La política cumple con los principios señalados en la metodología.

* La política transparenta con claridad si los datos de las usuarias han sido o están siendo administrados por, o comunicados a terceros, para lo cual la empresa deberá:

  – informar sobre la existencia de convenios y/o contratos suscritos con terceros (v.gr.: proveedores de servicios, instituciones públicas y/o privadas) en virtud de los cuales la empresa comunica información personal o estadística de sus usuarios (por ejemplo, para efectos de políticas públicas, iniciativas de investigación, cobro de deudas, etc.)

  – la(s) finalidad(es) con que comunica la información,

  – la base de legalidad que justifica tal comunicación, y

  – las medidas implementadas para la protección de la información objeto de comunicación.

* La política menciona expresamente la existencia o no de flujo transfronterizo de datos, y de existir, cumple al menos con estándares mínimos de resguardo para los datos tratados.

* La política informa claramente sobre el tratamiento que la empresa hace o puede hacer de los datos que recolecta de sus usuarios, especialmente, informando en detalle las categorías de datos recolectados, las finalidades para las cuales podría tratar cada categoría de dato que recopila, y la base de legalidad para cada tipo de tratamiento.

* La empresa informa el tiempo máximo de almacenamiento de los datos, y su forma de eliminación una vez transcurrido el plazo señalado para el almacenamiento.

* La empresa mantiene a disposición del público las versiones anteriores de sus contratos y políticas de privacidad y toda la documentación tiene consignada su fecha de entrada en vigor.

* La empresa no traspasa a sus usuarios la carga de revisar las modificaciones que hace en su documentación, obligándose a notificar debidamente cualquier cambio que incorpore en sus contratos, políticas de privacidad, u otros.

★ **La empresa recibe una estrella completa cuando cumple con todos los parámetros.**

★ **La empresa recibe ¾ de estrella cuando cumple con la mayor parte de los parámetros.**

★ **La empresa recibe ½ estrella cuando cumple parcialmente (de 3 a 5 parámetros).**

☆ **La empresa recibe ¼ de estrella cuando cumple con una mínima parte de los parámetros (de 1 a 2 parámetros).**

☆ **La empresa recibe estrella vacía si no tiene publicada la documentación pertinente en su página web o no cumple con ninguno de los criterios señalados.**

b) ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

Parámetros de la respuesta:

El proveedor obtiene una estrella si cuenta con un informe de transparencia que permita conocer las prácticas de vigilancia de las comunicaciones, explicitando la siguiente información:

* número total de solicitudes de información recibidas;

* información sobre las solicitudes recibidas, desglosada con el siguiente detalle:

  – solicitudes que provienen de alguna autoridad fuera del contexto de un proceso penal o sin contar con una orden judicial, con indicación de la autoridad específica de que se trata;

  – solicitudes que provienen de órdenes judiciales;

  – solicitudes que se refieren a un individuo en particular;

  – solicitudes que se refieren a una colectividad (v.gr.: información de todos los teléfonos celulares conectados a una antena determinada, durante un periodo de tiempo determinado);

* oportunidades en que se ha rechazado una solicitud de acceso a información personal o de interceptación de comunicaciones,

* motivo por el cual han sido rechazadas solicitudes de información;

* 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 y aquellas solicitudes relativas a la realización de interceptación de comunicaciones;

* desagrega el número de solicitudes a través de un criterio geográfico (comuna, región, etc.);

* incluye información sobre solicitudes recibidas para bloquear el acceso a sitios web, para bloquear o filtrar contenido y las solicitudes para suspender temporalmente el servicio;

* detalla todas las categorías de datos que han sido requeridas al proveedor; y todas las categorías de datos que han sido comunicadas por el proveedor. Para cumplir con este criterio las compañías deberán entregar el detalle completo de las categorías de información que les han sido solicitadas, no siendo suficiente las enumeraciones a modo meramente ejemplar.

★ **La empresa recibe una estrella completa cuando cumple con todos los parámetros.**

★ **La empresa recibe ¾ de estrella cuando cumple con la mayor parte de los parámetros.**

★ **La empresa recibe ½ estrella cuando cumple parcialmente (de 3 a 5 parámetros).**

★ **La empresa recibe ¼ de estrella cuando cumple con una mínima parte de los parámetros (2 o menos).**

☆ **La empresa recibe estrella vacía si no tiene publicada la documentación pertinente en su página web o no cumple con ninguno de los criterios señalados.**

c) ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

Parámetros de la respuesta:

* El proveedor cuenta con algún sistema de notificación que permita informar a sus usuarios sobre la realización de alguna diligencia intrusiva (una vez que pueda legalmente realizar tal comunicación), ya sea en sede penal, laboral, de familia, u otra.

* El proveedor ha tomado acciones (comprobables) para implementar un sistema que le permita notificar a sus usuarios que han sido objeto de una medida intrusiva, mediante su participación en el Congreso, por sí o a través de asociaciones gremiales.

* El proveedor ha tomado acciones (comprobables) para implementar un sistema que le permita notificar a sus usuarios que han sido objeto de una medida intrusiva, a través de algún mecanismo de cooperación con la autoridad, o de algún otro modo distinto a los señalados precedentemente.

* El proveedor ha hecho pública una o más de las acciones señaladas precedentemente.

★ **La empresa recibe una estrella completa cuando cumple con todos los parámetros.**

☆ **El proveedor obtendrá ¼ de estrella por cada parámetro cumplido.**

d) ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

Parámetros de la respuesta:

* La empresa informa el tiempo máximo durante el cual almacena metadatos, e informa sobre la forma de eliminación de esta información una vez el tiempo durante el cual la guarda.

* La empresa hace explícita la obligación legal de notificar a las personas afectadas por una medida investigativa intrusiva, en los términos señalados en el artículo 224 del código procesal penal.

* La empresa especifica los procedimientos que tiene para responder a las solicitudes de información de las usuarias por parte de la autoridad.

* La empresa detalla y establece específicamente los requisitos necesarios para responder favorablemente a una solicitud (por ejemplo, una orden judicial; nivel mínimo de especificidad que requiere una solicitud de información para que sea procedente; etc.), entre los cuales contempla que, para el caso de requerimientos de autoridad para el desarrollo de políticas públicas, la información relativa a la ubicación de las usuarias solo puede ser entregada a la autoridad competente y de forma anonimizada y agregada.

* La guía hace explícito que toda solicitud de información que contenga datos personales sensibles (i.e.: geolocalización), además de requerir una orden judicial previa, deberá referirse a individuos determinados, excluyendo la posibilidad de entregar este tipo de información respecto de una colectividad de usuarios que no fueron identificados en la respectiva solicitud.

* La empresa informa el tiempo máximo durante el cual almacena aquella información que le puede ser requerida, detallando el tipo de información de que se trata, y la forma de eliminación una vez transcurrido el tiempo de almacenamiento.

★ **La empresa recibe una estrella completa cuando cumple con todos los parámetros.**

★ **La empresa recibe ¾ de estrella cuando cumple con la mayor parte de los parámetros.**

★ **La empresa recibe ½ estrella cuando cumple parcialmente (de 3 a 5 parámetros).**

★ **La empresa recibe ¼ de estrella cuando cumple con una mínima parte de los parámetros (2 o menos).**

☆ **La empresa recibe estrella vacía si no tiene publicada la documentación pertinente en su página web o no cumple con ninguno de los criterios señalados.**

e) ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias 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 ha efectuado algún tipo de defensa de sus usuarios en instancias de carácter administrativo, o en la discusión de políticas públicas que puedan afectar los derechos de las usuarias.

* El proveedor ha efectuado algún tipo de defensa de sus usuarios mediante su participación en la tramitación legislativa de proyectos de ley.

* El proveedor ha emitido declaraciones públicas condenando iniciativas legales, administrativas o judiciales que afecten o amenacen con afectar la privacidad de sus usuarios, o ha hecho públicas una o más de las iniciativas anteriores.

* El proveedor forma parte de coaliciones o iniciativas multisectoriales donde existen intercambios con usuarios o representantes del interés público.

* El proveedor se ha negado ante solicitudes de información que no se refieran a individuos determinados, como exige la ley.

* El proveedor recurrió a la justicia u otra autoridad competente, para denunciar y/o dejar sin efecto requerimientos de datos por considerarlos excesivos o potencialmente vulneratorios de los derechos de sus usuarios.

★ **La empresa recibe una estrella completa cuando cumple con todos los parámetros.**

La empresa recibe ¾ de estrella cuando cumple con la mayor parte de los parámetros (de 4 a 5).

La empresa recibe ½ estrella cuando cumple parcialmente (3 de los parámetros).

La empresa recibe ¼ de estrella cuando cumple con una mínima parte de los parámetros (de 1 a 2).

☆ **La empresa recibe estrella vacía cuando no cumple ninguno de los parámetros**.

3. Contexto Nacional

3.1. Marco regulatorio

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[14] a solicitud del Ministerio Público, órgano a cargo de la investigación y persecución criminal. Si la recolección de información tiene fines de inteligencia, procede a través de las direcciones de inteligencia de las Fuerzas Armadas y de las policías.

El 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, sin embargo, no existen antecedentes que acrediten que dicha obligación es cumplida en la actualidad.

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),[15] que se refiere a la obligación contenida en el Código Procesal Penal para que los proveedores de servicios de telecomunicaciones conserven un registro, al menos por un año, de los datos de las conexiones que hagan las direcciones IP asociadas a su servicio. Dicha información solamente puede ser dada a conocer a los órganos que la ley indique, resguardando la privacidad de sus abonados.

14 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.

15 Disponible en: **https://www.bcn.cl/leychile/navegar?idNorma=242261** [Fecha última consulta: 20 de julio de 2022].

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[16] 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.

Con todo, actualmente se discute en el Congreso un proyecto de ley[17] que busca renovar casi la totalidad del estatuto actual. El proyecto fue presentado en 2017 y se encuentra en segundo trámite constitucional (discusión de su articulado en la Cámara de Diputados), tras su aprobación en general y en particular en el Senado. Adicionalmente, cabe destacar que desde la publicación de la primera versión de este informe hubo una modificación legal relevante en materia de datos personales: a mediados del año 2018 se publicó en el Diario Oficial la ley Nº 21.096 que consagra el derecho a la protección de datos personales a nivel constitucional. Esta reforma al numeral 4° del artículo 19 de la Constitución Política de la República, agrega además que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

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.

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

17 Disponible en: **https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07** [Fecha última consulta: 20 de julio de 2022].

En cuanto a la publicación de informes de transparencia y políticas de privacidad por parte de las empresas de telecomunicaciones, 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, hasta convertirse en un piso mínimo con el que todas las compañías cumplen en la actualidad.

3.2. Empresas de telecomunicaciones

El año 2021 estuvo marcado en gran parte por la pandemia COVID-19 y el paulatino regreso a la presencialidad. La pandemia obligó a explorar muchas nuevas formas de trabajo, entretención y conexión. Pese a que las restricciones a la movilidad se han ido eliminando progresivamente y la realización de actividades presenciales vuelve a ser posible, muchas de las prácticas desarrolladas durante la pandemia se mantienen vigentes. En este contexto, los servicios prestados por las empresas de telecomunicaciones son más relevantes que nunca. Desde junio de 2020 a junio de 2021 el tráfico mensual de datos fijos aumentó un 34.5%. En el mismo periodo, el tráfico de datos móviles aumentó un 31.67%.[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 septiembre de 2021, las cuotas de mercado entre los diferentes ISP son las siguientes:

— **Movistar**. Participación de mercado: 28% del mercado de internet fijo y 21,5% del mercado de internet móvil.

— **VTR**. Participación de mercado: 31% del mercado de internet fijo y 1,2% del mercado de internet móvil.

— **Claro Chile**. Participación de mercado: 11,6% del mercado de internet fijo y 18,3 % del mercado de internet móvil.

— **Entel**. Participación de mercado: 6,5% del mercado de internet fijo y 34,7 % del mercado de internet móvil.

18 SUBTEL. 2021. Especial Análisis Tráfico Internet Marzo 2020 - Junio 2021. Disponible en: **https://www.subtel.gob.cl/wp-content/uploads/2021/09/PPT_Series_JUNIO_2021_VO.pdf** Fecha última consulta: 4 de mayo de 2021]

19 Disponible en: **https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2019&locations=CL&start=1992&view=chart** [Fecha última consulta: 27 de mayo de 2022]

— **Grupo GTD**. Participación de mercado: 7,8% del mercado de internet fijo y no cuenta con participación en el mercado de internet móvil.

— **WOM**. No cuenta con participación en el mercado de internet fijo y un 23,6% del mercado de internet móvil.[20]

Las seis compañías seleccionadas para este estudio representan una parte sustantiva del mercado de internet en Chile: un 97,7% de los servicios fijos y 99,9% de conexiones móviles.

Según cifras de 2020, el 88,4% de la población en Chile usa internet, mayoritariamente (84,1%) a través de servicios móviles,[21] 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.

20 Disponible en: **https://www.subtel.gob.cl/wp-content/uploads/2021/09/PPT_Series_JUNIO_2021_V0.pdf** [Fecha última consulta: 14 de junio de 2022]

21 Según las mismas estadísticas de Subtel, en septiembre de 2021 el 67.48% de la población chilena cuenta con internet fija en el hogar. Disponible en: **https://www.subtel.gob.cl/hogares-con-acceso-a-internet-fijo-alcanzan-el-67-y-usuarios-aumentan-preferencia-por-redes-de-alta-velocidad/#:~:text=Respecto%20al%20consumo%20de%20datos,Mundo%20(13%2C5%25)**.
[Fecha última consulta: 14 de junio de 2022]

4.1. Claro Chile

4.1.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

La página de inicio del sitio web de Claro Chile[22] mantiene un formato amigable que permite al usuario llegar rápidamente a la política de privacidad y a los contratos que la compañía mantiene publicados en su sitio web, en la pestaña Claro Transparente. Esta pestaña cuenta con las secciones "Protección al Usuario" y "Normativa legal", a las que ahora se suma una de "Reclamos", que facilita a las usuarias el ejercicio de sus derechos.

Bajo el título de protección al usuario encontramos —entre otras— la subsección "Transparencia, privacidad y protección de datos personales", que lleva a su "Portal de Privacidad y Protección de Datos", una nueva página dedicada especialmente a entregar información relacionada con la protección de la privacidad y de los datos de sus usuarios, lo que se traduce en una nueva muestra del compromiso de Claro en esta materia.

Por su parte, los distintos contratos tipo existentes pueden ser encontrados en la sección Normativa Legal, bajo el título "Condiciones contractuales",[23] separados según se refieren a servicios móviles o a servicios fijos.

El primero que figura en servicios móviles es el "Contrato de suministro de servicios de telecomunicaciones",[24] que cuenta con una sección especial sobre protección de datos personales, donde señala que protegerá los datos de sus clientes según lo dispone la ley 19.628; menciona expresamente los principios de licitud, finalidad, calidad de los datos, proporcionalidad, responsabilidad, transparencia, no discriminación, confidencialidad, limitación de uso y seguridad en su tratamiento (conforme nuestra metodología, solo faltarían los principios de lealtad y minimización de datos); se sujeta a la correspondiente política de protección de datos de la empresa; y, por último, explica cómo ejercer los derechos de acceso, rectificación, oposición y cancelación, mejor conocidos como derechos ARCO.

22 Disponible en: https://www.clarochile.cl/personas/ [Fecha última consulta: 26 de mayo de 2022]

23 Disponible en: https://www.clarochile.cl/portal/cl/legal-regulatorio/lightbox/descripcion-ED-188.html [Fecha última consulta: 26 de mayo de 2022]

24 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/SSMT_PersonaEmpresa_29012021_20210129.pdf [Fecha última consulta: 26 de mayo de 2022]

Luego, bajo el mismo título, encontramos el Contrato de Arrendamiento de Equipo(s) y Accesorio(s) Telefónico(s) con opción de compra,[25] que cuenta con una cláusula similar a la descrita precedentemente, con la diferencia de no mencionar que se atiende a la política de protección de datos.

En la sección "Contratos Servicios Fijos", encontramos el Contrato Productos por Cable Pyme,[26] el cual no cuenta con ninguna cláusula de protección de datos.

En cuanto al "Portal de Privacidad y Protección de Datos",[27] es importante reconocer que se trata de un sitio que destaca por su claridad, con un diseño simple que facilita la experiencia del usuario al mostrar es una misma página las secciones referidas a los siguientes temas:

1. Política de Protección de Datos y Privacidad, dónde encontramos una breve explicación de su contenido y las distintas versiones existentes.

2. Política de privacidad y protección de datos de América Móvil, política general de la empresa a la que pertenece Claro.

3. Conceptos de datos personales, acá encontramos breves definiciones de conceptos importantes en materia de datos.

4. Política de Requerimientos de Información donde, junto a una definición breve, se ubica la sección "documentos" en la que se encuentran tanto la versión actual como los archivos históricos, correspondientes a los años 2018, 2019 y 2021.

5. Informe de Transparencia, que también cuenta con una definición y todas las versiones existentes, una de las cuales está disponible en inglés.

6. Relación con la Autoridad, donde Claro expone las distintas instancias en las cuales ha defendido o buscado defender de alguna forma los derechos de sus usuarios, dividiéndolas en "Relacionamiento público" y "Acciones adoptadas en resguardo de los datos de nuestros clientes".

25 Disponible en: **https://www2.clarochile.cl/portal/cl/archivos_generales/contrato-de-arriendo-de-equipo-con-opcion-de-compra_20220218.pdf** [Fecha última consulta: 26 de mayo de 2022]

26 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/-2-Contrato-Productos-por-Cable-PYME_20180403.pdf** [Fecha última consulta: 26 de mayo de 2022]

27 Disponible en: **https://www.clarochile.cl/personas/proteccion-de-datos/** [Fecha última consulta: 29 de mayo de 2022]

7. Demás notificaciones a las usuarias y/o Clientes Claro donde, además de comprometerse con un proceso de notificación a las usuarias y/o Clientes que hayan sido objeto de requerimientos de información mediante resolución judicial emitida por parte de los tribunales de justicia (siempre y cuando no lo impida un deber legal de confidencialidad o reserva de la información), publica el modelo de notificación que serviría para notificar a los afectados.

8. Requerimientos de no envío de publicidad y Políticas de Contactabilidad, sección que contiene un formulario para solicitar el cese de envío de comunicaciones publicitarias o promocionales y un breve documento que hace referencia a su política de contactabilidad, mediante la cual asume un compromiso de autorregulación con la comunidad para disminuir los llamados publicitarios y promocionales regulando, entre otros aspectos, los horarios y el máximo de llamados.

9. Un formulario para hacer valer los derechos ARCO (Acceso, Rectificación, Cancelación u Oposición).

10. Tips en protección de datos para sus usuarios, relacionados con *phishing, smishing,* ciberdelincuentes e internet y seguridad.

11. Noticias sobre protección de datos y privacidad, entre las cuales se encuentra información sobre la declaración conjunta de Derechos Digitales, ACTI y el Centro de Estudios en Derecho Informático de la Universidad de Chile, entre otros, realizada durante el 2022 para mostrar el rechazo transversal generado por el proyecto de ley que pretendía autorizar el acceso a metadatos sin autorización judicial.

La política de privacidad y protección de datos actual corresponde a la versión número 1.5 de julio de 2022.[28] En esta nueva política se han incorporado títulos que facilitan su lectura y, entre otras novedades, encontramos la mención expresa al principio de lealtad (cumpliendo, así, con todos los principios exigidos en la metodología de este informe); el detalle de los tipos de datos recolectados y las finalidades de su tratamiento, presentados en su mayoría mediante una tabla que hace mucho más fácil su comprensión; la inclusión de descripciones de los derechos ARCO y la manera de ejercerlos; el compromiso de no almacenar datos de sus usuarios por plazos mayores a los establecidos por la ley; la especificación de los medios mediante los cuales se informará cualquier modificación a la política de privacidad, cuyas distintas versiones se compromete a mantener

28 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/politica-de-privacidad-y-proteccion-de-datos-1-5.pdf** [Fecha última consulta: 25 de julio de 2022]

disponibles en su página web; el compromiso de adoptar técnicas adicionales para la protección de la información, tales como la anonimización de los datos personales, para reducir el riesgo de un tratamiento no autorizado de estos siempre que sea posible; y la inclusión de una sección sobre dudas o consultas respecto de su política de protección de datos personales, que invita a sus usuarios a escribir al correo electrónico **datos.personales@clarochile.cl** en caso de dudas, consultas o recomendaciones.

Entre las categorías de datos que Claro transparenta recolectar, almacenar y procesar se encuentra 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, además expresa que la participación en concursos, promociones o encuestas es totalmente voluntaria y tiene el único propósito de conocer la experiencia en los servicios otorgados, siendo los resultados comunicados de forma general, anonimizada y estadística.

Claro expresa que, al utilizar herramientas de procesamiento masivo de datos para realizar determinadas actividades de análisis de tendencias de consumo y preferencias sobre uso de productos y servicios, predicción de comportamiento y tendencias de consumo, o de análisis de información para fines técnicos y de mejora de sus productos y servicios, establecerán controles para respetar la privacidad de las personas.

En una versión preliminar de este informe se solicitó a la compañía referirse a la existencia de flujo transfronterizo de datos. En respuesta a esto, la empresa aclaró en su política actualizada que solo comunica datos debidamente anonimizados a sus aliados comerciales, los cuales deberán cumplir estrictamente con la normativa sobre protección de datos, debiendo el destinatario contar con las medidas de protección de los derechos de los titulares y niveles de seguridad al menos equivalentes a los de Claro. Además, en respuesta a la recomendación de expresar el tiempo máximo de almacenamiento de los datos, y la forma de eliminación de la información una vez transcurrido el plazo de almacenamiento, Claro agregó un título nuevo a su política de privacidad denominado “Tiempo de almacenamiento de datos”. En este título, Claro aclara que almacenará los datos de sus clientes por el tiempo necesario para el cumplimiento de los fines para los cuales son tratados, el cual no puede exceder de 5 años desde el término del contrato o desde que las correspondientes obligaciones se hagan exigibles. Continúa diciendo que los rangos autorizados de direcciones IP y los números IP de las conexiones serán almacenados por los plazos que dispone

el código procesal penal en sus artículos 222 y 218 bis. En los casos que el Ministerio Público no haga uso de sus facultades del artículo 218 bis, los datos serán almacenados por un máximo de 2 años.

De las novedades presentadas por Claro, destacamos especialmente la mayor transparencia en relación con el tratamiento de datos que realiza, y felicitamos la adopción voluntaria de compromisos y responsabilidades relacionados con la privacidad y protección de los datos de sus usuarios, así como su rápida reacción ante las recomendaciones realizadas en el informe preliminar de QDTD.

En consideración de lo anterior, ***la empresa recibe 1 estrella****.*

4.1.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

Claro cuenta con informes de transparencia actualizados, al mismo tiempo que mantiene publicados los informes de años anteriores, entregando estadísticas de requerimientos de información y de interceptación por parte de las autoridades desde el año 2019 en adelante.

En su informe de transparencia del año 2021[29] Claro mantiene la forma de presentación general de la información, separada en semestres, por zona (norte, centro y sur), y, a su vez, en tres categorías distintas según el tipo de requerimiento:

1. Solicitud de información general (titularidad, domicilio, IMEI, etcétera),
2. Solicitudes de interceptación telefónica y
3. Metadatos (IP, tráfico, georreferenciación).

Asimismo, el informe del 2021 mantiene el formato de los gráficos estadísticos en materia de requerimientos de información y metadatos (divididos por región y según el tipo de requerimiento), pero sin incluir la información sobre interceptaciones, que ahora es presentada en un gráfico aparte.

Otra novedad del informe de 2021 es la nueva forma de presentar la información relativa a los macro motivos de rechazo de los distintos requerimientos, y la incorporación de un cuadro explicativo de las causales de los referidos macro motivos, más detallado que el del año anterior, dónde es posible encontrar la siguiente información:

29 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/politica-de-privacidad-y-proteccion-de-datos-28-04-22.pdf** última consulta: 26 de mayo de 2022]

* **Error de requerimiento**: esta causal de rechazo implica que el número PCS cuyos datos se solicitan resultan errados, falta un dígito, no indica el RUT de la persona sujeta al requerimiento, no se adjunta el oficio debidamente suscrito, no se individualiza correctamente el dato a consultar, no indica rango de fechas y/o no indica IMEI o rango a consultar asociado al requerimiento.

* **No adjunta Excel**: La planilla no cumple con los estándares de claridad y/o precisión, o no se condice con las especificaciones del requerimiento judicial.

* **No adjunta orden**: Esta causal implica que en el requerimiento de información (tráfico Voz, Datos e IMEI) no se adjunta resolución judicial que autorice expresamente la entrega de la información.

* **No copia fiscal**: Esta causal implica que el funcionario policial a cargo de la diligencia investigativa no copió en su requerimiento a el o la Fiscal que tiene asociada la investigación de la causa.

* **Sin RUC**: Esta causal de rechazo implica que el requerimiento judicial no se indica expresamente el RUC o RIT de la causa, en virtud del cual se solicitan los antecedentes.

* **Correo no institucional**: Esta causal de rechazo implica que el funcionario policial hace uso de un correo no institucional para solicitar requerimientos de información.

Como se puede notar, esta tabla explica con mayores detalles las causales de cada uno de los referidos macro motivos. En relación con la información estadística sobre los requerimientos de información recibidos de otros entes jurisdiccionales, el gráfico cambia de diseño y ahora no se encuentra información sobre tribunales de familia, pero sí de tribunales militares, no siendo posible determinar si lo anterior significa que en 2021 no recibieron solicitudes por parte de tribunales de familia, o si la modificación se debe a un cambio de criterio. Con todo, esta última duda no subsiste para el año 2022, toda vez que el informe presentado para el primer trimestre muestra tanto a los juzgados de familia como a los militares, junto a Corte de Apelaciones y juzgados de policía local, laborales y civiles.

En síntesis, durante el año 2021 Claro recibió un total de 9.640 requerimientos, de los cuales se procedió a objetar, aclarar y/o rectificar 2.944, según el detalle que muestra el gráfico estadístico en materia de requerimientos de información y de interceptación por parte de las autoridades divididos por región:

* Hubo 8.452 solicitudes de interceptación telefónica, de las cuales 92 fueron rechazadas, según el siguiente detalle:
  - Error RESIT: 55
  - Resolución sin firma del juez: 1
  - Prórroga fuera de plazo: 15
  - No adjunta carta de portabilidad: 14
  - Numero a interceptar errado: 5

* Hubo un total de 25.527 solicitudes de información general, de las cuales 2.044 fueron rechazadas.

* 3.551 solicitudes de acceso a metadatos, de las cuales 808 fueron rechazadas.

* En cuanto a estos últimos dos tipos de requerimientos, la gráfica acompañada por Claro muestra los siguientes motivos de rechazo:
  - No copia al fiscal: 60%
  - Correo no institucional: 1%
  - Error de requerimiento: 11%
  - No adjunta Excel: 7%
  - No adjunta orden: 20%
  - No indica RUC: 1%

Por su parte, el informe del primer trimestre de 2022 también trae cambios en comparación al informe de 2021 y su forma de mostrar la información. Para el año 2022 la presentación general de la información, además de estar desagregada por zona y según el tipo de requerimiento, también es separada en dos tablas distintas, según se trata de requerimientos respondidos o rechazados; e incluye una nueva tabla con el detalle del número de requerimientos recibidos, respondidos y rechazados, por región.

Otra de las novedades de este último informe es la incorporación de dos nuevos contenidos: una gráfica de los requerimientos recibidos por los derechos ARCO, y una sección referida a los requerimientos para bloquear o filtrar contenido, bloquear acceso a sitios web, o suspender temporalmente el servicio. En esta última, Claro hace presente que, durante el primer trimestre de 2022,[30] únicamente recibió una solicitud de bloqueo del acceso a página web, realizada por particulares en virtud de lo dispuesto en el artículo 85 U de la Ley 17.336. Dicha solicitud se refería al sitio **www.ailoo.cl**, y fue rechazada por no haberse acreditado el cumplimiento de los requisitos establecidos en las letras b) y e) de la citada disposición.

30 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/informe-de-transparencia-del-primer-trimestre-2022.pdf** [Fecha última consulta: 24 de mayo de 2022]

Finalmente, Claro recogió varias de las recomendaciones realizadas en el informe preliminar, introduciendo cambios que mejoraron la calidad de su informe, al agregar un nuevo gráfico en el cual indican que recibieron únicamente una solicitud por parte de entes gubernamentales fuera de un proceso penal, siendo esta solicitud por parte de la Subtel la cual contaba con una resolución judicial, además especificaron que la solicitud era de carácter colectivo y tenía por objeto saber el número de conexiones con respecto a una antena o estación base. Adicionalmente, incluyeron una nueva tabla donde detallan las categorías de datos que son recolectados y las finalidades con que son utilizados.

En síntesis, durante el primer trimestre de 2022 Claro recibió un total de 7.680 requerimientos, siendo 6.962 respondidos, de los cuales 718 fueron rechazados, según el siguiente detalle:

* Hubo 2.704 solicitudes de interceptación telefónica respondidas, de las cuales 31 fueron rechazadas, según el siguiente detalle:
  - Error RESIT: 18
  - Resolución sin firma de juez: 0
  - RUC de la causa errado: 0
  - Prórroga fuera de plazo: 6
  - No adjunta carta de portabilidad: 5
  - Numero a interceptar errado: 2

* Hubo un total de 6.258 solicitudes de información general respondidas, de las cuales 532 fueron rechazadas.

* 704 solicitudes de acceso a metadatos respondidas, de las cuales 186 fueron rechazadas.

  En cuanto a estos últimos dos tipos de requerimientos, la gráfica acompañada por Claro muestra los siguientes motivos de rechazo:
  - No copia al fiscal: 468
  - Correo no institucional: 7
  - Error de requerimiento: 74
  - No adjunta Excel: 23
  - No adjunta orden: 140
  - No indica RUC: 6

El documento muestra que, durante el primer trimestre del año 2022, se respondieron un total de 6.258 solicitudes de información general y se rechazaron 532 requerimientos. Se respondieron 2.704 solicitudes de interceptación telefónica y se rechazaron 31 de estas solicitudes y finalmente, serespondieron 704 solicitudes de acceso a metadatos mientras que se rechazaron 186 de estas.

Claro ha continuado mejorando la forma de presentar la información de su informe de transparencia, así como la calidad de la misma, siendo una de las compañías con el informe más completo. Claro se hizo cargo de las observaciones realizadas en el informe preliminar y subsanó las falencias de su informe para agregar referencias a las solicitudes que tienen como objeto una colectividad de individuos y el detalle de todas las categorías de datos que les han sido requeridas. En vista de lo anterior se le otorga a Claro el máximo puntaje.

La empresa recibe 1 estrella.

4.1.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

En lo relacionado a este punto, el documento titulado "Política de requerimientos de información"[31] se mantiene prácticamente inalterado en comparación a su versión anterior, indicando que Claro se reserva el derecho de notificar a las usuarias 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.

Si bien reservarse el derecho a notificar no se traduce necesariamente en su notificación efectiva, dentro del Portal de Privacidad y Protección de Datos,[32] en la sección "Demás notificaciones a las usuarias y/o Clientes Claro", la empresa declara que como parte de su política de protección de los datos personales, ha establecido el proceso de notificación a las usuarias 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.) siempre y cuando no exista el deber legal de confidencialidad o reserva de la información. En la misma sección es posible encontrar la carta tipo que Claro utilizaría para realizar estas notificaciones.[33] En ella se señala 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, siendo la primera compañía en publicar un documento de este tipo.

31 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/politica-de-requerimientos-de-informacion-abril-2022.pdf** [Fecha última consulta: 17 de mayo de 2022]

32 Disponible en: **https://www.clarochile.cl/personas/proteccion-de-datos/** [Fecha última consulta: 18 de mayo de 2022]

33 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/notificacion-modelo-kgd_20190605.pdf** [Fecha última consulta: 18 de mayo de 2022]

Por otra parte, destacamos el rol activo adoptado por Claro en esta materia durante los años 2019, 2020 y 2022, mediante la realización de acciones tanto en el Congreso, como también ante el Ministerio Público, demostrando preocupación para buscar una forma de cumplir con el deber de notificación contemplado en artículo 224 del Código Procesal Penal. Se valora muy positivamente que, en mayo de este año, hayan insistido ante el Ministerio Público para revisar nuevamente la posibilidad de notificar a las personas que han sido objeto de un requerimiento de interceptación o solicitud de datos personales, destacando enfáticamente que se haya planteado la posibilidad de implementar un plan piloto a la fiscalía.[34]

Por contemplar un sistema de notificación, hacer públicas las acciones realizadas para la notificación de sus usuarios, y ser la única compañía que ha realizado acciones concretas en orden a conseguir que la autoridad cumpla con su obligación legal de notificar a las personas afectadas por medidas investigativas intrusivas, ***la compañía recibe 1 estrella****.*

4.1.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

En su Portal de Privacidad y Protección de Datos, Claro mantiene publicada su política de requerimiento de información[35] de abril de 2022 junto a las versiones de 2018, 2019 y 2020. En relación con la versión precedente, este documento no ha sido objeto de modificaciones sustantivas, pero contiene algunas modificaciones que consideramos positivas, por ejemplo, el hacer explícito que, tratándose de geolocalización o información que sea considerada por la Ley 19.628 como "Dato Personal Sensible", será necesario que el requerimiento se refiera a personas determinadas, no siendo en consecuencia admisibles requerimientos de carácter general y/o relacionados a personas indeterminadas. 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. Además, al igual que en el resto de sus políticas, se hace presente un canal de contacto (**datos.personales@clarochile.cl**) para quienes tuviesen dudas o comentarios con respecto a la política de protección de datos.

34 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/minuta-minesterio-publico-07-22%20(2).pdf** [Fecha última consulta: 25 de julio de 2022]

35 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/politica-de-requerimientos-de-informacion-abril-2022.pdf** [Fecha última consulta: 18 de mayo de 2022]

Felicitamos a la empresa por incluir una referencia al artículo 224 del Código Procesal Penal en su política de requerimiento de información. Atendido el incumplimiento por parte de la autoridad de esta importante obligación legal, nos parece sumamente importante que la misma esté reflejada de manera expresa en la guía pública destinada a la autoridad.

La empresa recibe 1 estrella.

4.1.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

En la sección "Relación con la autoridad"[36] del sitio web, Claro expone una serie de documentos que dan cuenta de sus acciones para defender la privacidad y la protección de los datos de sus usuarios.

En el ámbito legislativo, Claro envió una minuta en 2021 al Senador Jorge Pizarro,[37] para manifestar su preocupación acerca del proyecto de ley boletín número.11.144-07, que modifica la ley N° 19.628, con el fin de regular la protección y el tratamiento de los datos personales. En específico, Claro hizo presente su preocupación en relación con las solicitudes de información que reciben por parte de organismos públicos, sugiriendo que los estándares y controles en la gestión de protección de los datos personales que aplicarán a las empresas también fueran aplicables a la Administración del Estado, así como establecer controles preventivos y la instauración de oficiales de cumplimiento por cada servicio público.

Este año Claro se pronunció acerca del proyecto de ley de delitos informáticos[38] y sobre el proyecto de ley "prepago".[39] En minuta enviada al entonces Senador José Miguel Insulza,[40] Claro manifestó su preocupación respecto a la debida protección de los datos personales en los proyectos de ley recién nombrados, sin mayores especificaciones.

36 Disponible en: https://www.clarochile.cl/personas/proteccion-de-datos/relacionamiento-publico/ [Fecha última consulta: 28 de mayo de 2022]

37 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/minuta-de-relacionamiento_h_senador-pizarro_20210331.pdf [Fecha última consulta: 19 de mayo de 2022]

38 Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12715&prmBOLETIN=12192-25 [Fecha última consulta: 14 de junio de 2022]

39 Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12563&prmBOLETIN=12042-15 [Fecha última consulta: 14 de junio de 2022]

40 Disponible en: https://www.clarochile.cl/portal/cl/archivos_generales/Minuta-Senador-Insulza-2022.pdf [Fecha última consulta: 19 de mayo de 2022]

En sede administrativa, es posible encontrar una solicitud de reconsideración a la Autoridad Administrativa,[41] mediante la cual Claro solicitó a la Subtel reconsiderar los términos y alcance de su requerimiento sobre la base de datos de clientes de internet fija para un estudio de satisfacción de usuarios de telecomunicaciones. Claro fundamenta esta solicitud de reconsideración expresando que el requerimiento de la "muestra" de la base de clientes realizado por la empresa consultora es desmedido e implica un claro desconocimiento al principio de proporcionalidad. Asimismo, es posible encontrar la respuesta a un requerimiento de la Subtel[42] mediante el cual dicho organismo solicitaba el envío de 10 documentos de cobro correspondientes a servicios móviles contratados por personas naturales. En su respuesta, Claro indicó que estos documentos contienen información de carácter personal y/o privada, solicitando a la autoridad su más estricta reserva y, además, envían los documentos de cobro, pero tachando los datos de los clientes.

Otra acción destacable es la respuesta dada por Claro al oficio 6863[43] de Sernac, mediante el cual este le solicitaba diversos datos para un estudio exploratorio, entre ellos los reclamos ingresados por sus clientes entre el 1 de enero de 2019 y el 31 de agosto de 2020, junto con datos para identificar a los reclamantes (RUT, género, fecha de nacimiento, comuna y región de residencia). Claro respondió a esta solicitud en carácter colectivo, haciendo presente que no era posible entregar la información que se refiere a datos de carácter personal (RUT del cliente, género y fecha de nacimiento del consumidor).

Otro de los elementos tomados en consideración para la asignación de puntaje en este parámetro es la participación de Claro en Atelmo.

La empresa recibe 1 estrella.

41 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/SolicitaReconsideracionAutoridadAdministrativaOficio388.pdf** [Fecha última consulta: 19 de mayo de 2022]

42 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/OF-CIRC-N-105-Respuesta.pdf** [Fecha última consulta: 19 de mayo de 2022]

43 Disponible en: **https://www.clarochile.cl/portal/cl/archivos_generales/oficio-sernac-6863_20210331.pdf** [Fecha última consulta: 30 de mayo de 2022]

4.2. Entel

4.2.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

En la sección "Privacidad y Seguridad de Datos Personales" ubicada al final del sitio web de Entel encontramos diversa información de interés,[44] ordenada en las siguientes categorías:

- Contratos,
- Políticas, Normativas, Reglamento y Leyes,
- Protección de datos,
- Términos y Condiciones,
- Comparador de Ofertas conjuntas y
- Política y tips de ciberseguridad.
- Último *phishing* reportado

En la sección "Políticas, Normativas, Reglamento y Leyes" es posible consultar las distintas versiones de la Política de Privacidad Clientes Entel, siendo la última de ella de junio de 2021.[45] Entel es una de las empresas que introdujo más modificaciones a su política de privacidad con relación al año anterior, entre las cuales destacamos especialmente las correcciones introducidas a la redacción de la cláusula referida al artículo 4 de la ley 19.628, reflejando ahora su verdadero sentido y alcance; y la reincorporación del párrafo en que se compromete a revisar los antecedentes asociados a los requerimientos de la autoridad para la protección de sus usuarios, tal como fuera recomendado en el informe QDTD 2021.

Valoramos también que la política actual de Entel tenga una sección especialmente dedicada a los principios aplicables, dónde se recogen la mayoría de los principios contemplados por nuestra metodología, con excepción del principio de lealtad, minimización y transparencia, aunque consideramos que este último se encuentra recogido implícitamente, toda vez que la política de privacidad de Entel es una de las que entrega mayores detalles sobre el tratamiento de datos que realiza y, por tanto, una de las más transparentes.

Otro cambio ocurre en la sección "Para qué y cómo usamos tus datos", donde Entel ahora declara que no compartirá los datos personales de sus usuarios con terceros para fines distintos a los que hayan sido autorizados. También informa que al realizar análisis sobre grandes volúmenes de datos

44 Disponible en: **https://www.entel.cl/legales/** [Fecha última consulta: 13 de junio de 2022]

45 Disponible en: **https://www.entel.cl/legales/public/pdf/politica-privacidad-clientes-junio%202021.pdf** [Fecha última consulta: 26 de mayo de 2022]

solo utilizará datos anonimizados y agregados. En la sección referida a los datos personales que Entel trata, se agrega una nueva categoría: los datos de geolocalización, cuyo tratamiento se realizaría previo consentimiento y con la finalidad de ofrecer servicios personalizados (v.gr. comunicaciones comerciales de bienes o servicios de Entel o sus asociados comerciales) de acuerdo con la geolocalización de las usuarias.

En cuanto al tiempo de almacenamiento, Entel se compromete a mantener los datos "solamente por el tiempo necesario para la prestación de los servicios, su cobro y facturación", salvo que la ley exigiera algo diferente; y en relación con los rangos autorizados de direcciones IP y los números IP de las conexiones que realicen sus abonados, se compromete a almacenarlos por máximo un año.

Si bien Entel no se refiere expresamente al flujo transfronterizo de datos, informa que podrá comunicar datos de sus usuarios a proveedores y socios comerciales, nacionales e internacionales, encargados del tratamiento de datos.

En cuanto a la protección y seguridad de la información, Entel se compromete a adoptar las medidas adecuadas en cumplimiento a la legislación aplicable para proteger los datos y que estos serán utilizados únicamente para los fines informados en su política de privacidad.

Por último, si bien reconocemos los esfuerzos realizados por Entel para adaptar su política de privacidad a los estándares de esta metodología, advertimos que no existe ningún compromiso expreso para notificar a las usuarias de los cambios que pueda sufrir dicha política. Instamos a Entel a adoptar un mecanismo que permita a las usuarias conocer los cambios que ocurran en relación con el tratamiento de sus datos sin necesidad de consultar permanentemente la política de privacidad vigente en búsqueda de potenciales cambios.

En lo que a los contratos se refiere,[46] tanto los "Contratos Planes de Telefonía móvil" como los "Contratos planes Hogar" y los "Contrato Planes Banda Ancha Móvil" contienen la misma cláusula sobre tratamiento de datos personales. En ella, se establece que el Cliente autoriza expresamente a Entel a tratar sus datos personales en los términos señalados en su Política de Privacidad de Clientes; pero, además, indica que faculta a la compañía "para solicitar, recolectar, almacenar y en general realizar cualquier tipo de operación sobre los siguientes datos personales...". Resulta preocupante la ambigüedad de los términos de la cláusula, donde se autorizaría "cualquier tipo de operación" para el tratamiento de distintos datos, entre ellos datos sensibles como la imagen, voz, datos biométricos, datos de geolocalización y hábitos de consumo.

46 Disponible en: **https://www.entel.cl/contratos/** [Fecha última consulta: 10 de mayo de 2022]

Además, Entel se reserva el derecho a tratar "cualquier otro que sea necesario para la ejecución del presente contrato, sus anexos o el mejoramiento de las experiencias de consumo y de la política ya referida", y agrega que el usuario autoriza que Entel pueda transmitir o comunicar sus datos personales a terceros relacionados o no, ya sea en forma nacional o transfronteriza para el cumplimiento de los fines señalados en este contrato. En definitiva, se trata de una cláusula en la que se pide consentimiento el titular para realizar distintos tratamientos cuyas condiciones no son del todo informadas y, por lo tanto, difícilmente podríamos hablar de un consentimiento informado.

Hacemos presente que, en reacción al preinforme, Entel hizo sus descargos señalando que la cláusula se ajusta a ley, toda vez que menciona los tipos de datos y las finalidades y tiene una extensión adecuada en proporción al resto de las cláusulas del contrato. Señalando, además, que la información más detallada y extensa está en la Política. Sin embargo, la política aludida señala, en términos amplios, que los datos personales serán utilizados "para el cumplimiento de los fines para los cuáles hemos solicitado tu consentimiento".[47] El problema está en que, al momento de solicitar el consentimiento, no se informan los fines para los cuales se autoriza a Entel para solicitar, recolectar, almacenar y, en general, realizar cualquier tipo de operación sobre los datos personales.

La cláusula establece que los estándares de seguridad para la transmisión nacional y transfronteriza de los datos personales están señalados en el documento denominado Política Corporativa de Seguridad de la Información,[48] que puede ser encontrado en la sección "Política y tips de ciberseguridad",[49] cuya última versión es de septiembre de 2020, a pesar de que el mismo documento indica que deberá ser revisada anualmente. Conforme a esta política, todo el personal de Entel —sea este permanente o temporal— tiene la obligación de proteger los activos de información físicos o digitales, los sistemas y la infraestructura tecnológica de la organización. En temas de Seguridad de la Información, Entel establece cadenas de responsabilidad sobre los activos, así como la obligatoriedad de sensibilización y capacitación de sus empleados. Finalmente establece que, en caso de incumplimiento de las normas de Seguridad de la Información por parte de un empleado, este se sujetará a las medidas y procedimientos previstos en un reglamento interno que establece sanciones.

47 Disponible en: **https://www.entel.cl/legales/centro-privacidad/public/pdf/Politica%20Privacidad%20Entel.pdf** [Fecha última consulta: 22 de agosto de 2022]

48 Disponible en: **https://www.entel.cl/legales/public/pdf/SGSI-01-00-PO-Pol%C3%ADtica-Corporativa-de-Seguridad-de-la-Informaci%C3%B3n-Web-p%C3%BAblica.pdf** [Fecha última consulta: 26 de mayo de 2022]

49 Disponible en: **https://www.entel.cl/legales/** [Fecha última consulta: 26 de mayo de 2022]

Por último, al hacer clic en la sección "Sobre el uso del sitio web" de la categoría "Términos y Condiciones", el usuario es dirigido a la página web sobre "Condiciones generales de uso Sitio web Entel", la que contiene seis subsecciones: "Datos personales del usuario o cliente y uso de claves", "Veracidad de la información", "Uso de los datos personales registrados en el sitio", "Propiedad intelectual y propiedad industrial" y "Sobre sitios web e internet". La pestaña denominada "Datos personales del usuario o cliente y uso de claves"[50] expresa que las cookies utilizadas por Entel seguirán los principios de finalidad y minimización de datos, ya que se comprometen a no ser utilizadas para la lectura de otros datos almacenados en el disco duro de las usuarias, ni de los archivos cookie creados por otros proveedores de servicios de internet.

Se valoran positivamente gran parte de las modificaciones introducidas por Entel a sus documentos contractuales y el nivel de detalle que entrega respecto de determinados tratamientos de datos, incluso aquellos que realiza mediante el uso de cookies. Asimismo, felicitamos a Entel por su Política Corporativa de Seguridad de la Información.

Lamentablemente, todos los esfuerzos y avances mostrados por Entel se ven eclipsados por la ambigüedad de la cláusula sobre tratamiento de datos personales contenida en los contratos "Planes de Telefonía móvil", "Planes Hogar" y "Planes Banda Ancha Móvil", y por la ausencia de una política de notificación de sus usuarios para informar cambios a los términos de sus contratos, especialmente considerando que se reserva el derecho de revisar y modificar los términos, como en el caso de las Condiciones Generales de Uso (que, conforme lo informado en la página, producirían efectos legales a contar del quinto día hábil desde la fecha de publicación de la modificación en el sitio web).

La empresa recibe ¾ de estrella.

4.2.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

En el sitio web de Entel está públicamente disponible un informe de transparencia revisado en julio de 2022.[51] A diferencia de años anteriores, este informe presenta, a modo de resumen, dos gráficos distintos: 1) solicitudes judiciales y 2) solicitudes de interceptación. La primera categoría nos muestra información desde el año 2018 a 2021, desagregada por mes del año y por zona geográfica. La segunda categoría muestra el mismo rango temporal de muestra, pero sin desagregarla por zona geográfica.

50 Disponible en: **https://www.entel.cl/condiciones-generales-uso/datos-personales-del-usuario/** [Fecha última consulta: 26 de mayo de 2022]

51 Disponible en: **https://www.entel.cl/legales/centro-privacidad/public/pdf/Informe_de_Transparencia-Requerimientos_de_Datos_Personales.pdf?v=5** [Fecha última consulta: 23 de agosto de 2022]

La tabla presentada da cuenta de que, durante 2021, Entel recibió un total de 82.479 solicitudes de información, lo que significa una disminución de 2,39% en relación con el número de solicitudes recibidas en 2020. El 3% de estas solicitudes fueron devueltas sin respuesta al organismo requirente, debido a que no cumplían con los requisitos legales mínimos. En comparación, durante 2020 Entel recibió 84.447 solicitudes de información, un alza del 32% en relación con el número de solicitudes de información recibidas el año 2019.

Durante 2021 se recibieron 11.113 solicitudes de interceptación de las comunicaciones, una disminución del 0,71% en relación con 2020. Todas las solicitudes fueron admitidas. En comparación, durante 2020 Entel recibió 11.212 solicitudes de interceptación telefónica, un alza del 22% en relación con el total de solicitudes de interceptación recibidas el año 2019.

Además, Entel recibió y consideró nuestro preinforme con aspectos a mejorar acerca de su reporte de transparencia. Ante esto, la empresa agregó los motivos más comunes por los cuales han sido rechazadas las solicitudes de información, siendo estos:

* Tráfico de llamadas sin Resolución Judicial o con resoluciones que no cuenten con los requisitos mínimos de este tipo de documentos.

* Tráfico de llamadas con autorización del propietario a solicitud del Fiscal adjuntando la carta y RUT del cliente, que en las validaciones internas el móvil NO se encuentra bajo el RUT cliente.

* Solicitudes de información de Organismos Policiales sin adjuntar Orden de Investigar.

* Solicitudes de Organismos Policiales sin copiar al Fiscal a cargo de la investigación.

* Solicitudes sin información mínima para realizar búsquedas en nuestros sistemas.

* Requerimientos realizados a través de correos electrónicos no institucionales.

Sin embargo, falta enunciar cuantas solicitudes de información fueron rechazadas por qué motivos, así como los motivos de rechazo del resto de solicitudes.

Continuando con los cambios realizados, se agregó una nueva sección con un gráfico que muestra el porcentaje de solicitudes realizada por la entidad. Además, hay una nueva sección que nos muestra que durante 2021 hubo 10.268 solicitudes asociadas a metadatos las cuales comprenden solicitudes de información de IP y tráfico de llamadas y por sitios. Durante 2021 solo hubo una solicitud para bloquear el acceso a sitios web en virtud de la ley de propiedad intelectual.

Reconocemos y valoramos las mejoras introducidas por Entel a su informe de transparencia, sin embargo, en comparación con otras compañías y en relación a los criterios de la metodología, siguen faltando algunos detalles: primero, explicitar todas las categorías de datos que han sido requeridas o informadas a las autoridades, además de indicar cuántas solicitudes fueron rechazadas por cada motivo nombrado; igualmente, falta indicar la existencia (o no) de solicitudes de información referidas a colectividades (v.gr. información de los teléfonos conectados a una antena determinada, durante un periodo de tiempo).

Tomando en consideración tanto las exigencias de la metodología actual como el nivel de detalle alcanzado por otras compañías en sus respectivos informes, ***la empresa recibe ¾ de estrella.***

4.2.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

En la versión anterior de nuestro informe analizamos en esta sección la "Guía informativa acerca de las solicitudes de la autoridad de interceptaciones e información personal" de abril de 2020. La guía actual[52] no ha sufrido importantes modificaciones. Por tanto, no podemos sino llegar a las mismas conclusiones, esto es, que la empresa no es clara respecto de los casos en que podría considerar procedente notificar a sus usuarios (y en qué casos no). Solo se limita a reservarse el derecho de hacerlo, lo que no se traduce en un compromiso concreto. Tampoco existen otros antecedentes que muestren que Entel haya realizado esfuerzos para notificar a sus usuarios, ni publicaciones o declaraciones de la compañía en relación con su postura respecto de las notificaciones de este tipo de medidas intrusivas.

La empresa recibe 0 estrellas.

52 Disponible en: **https://www.entel.cl/legales/centro-privacidad/public/pdf/guia%20solicitud%20judiciales.pdf?v=10** [Fecha última consulta: 29 de mayo de 2022]

4.2.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

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 las usuarias.[53] Si bien este documento no presenta mayores variaciones con respecto a la versión anterior, hay ciertos cambios que vale la pena destacar. En primer lugar, se modificó el preámbulo de la Guía, agregando un estándar más exigente frente a requerimientos que pudieran afectar la privacidad de sus clientes, al indicar que se asegurarán de que las medidas intrusivas no afecten la privacidad e inviolabilidad de las comunicaciones de sus usuarios más allá de lo estrictamente necesario. Otro cambio a destacar es la incorporación de un párrafo que señala que, en caso de solicitarse datos sensibles de sus clientes para fines de desarrollo de políticas públicas, estos solo podrán ser entregados de forma agregada y anonimizada. Finalmente, dentro de los requisitos que debe tener la solicitud para realizar una interceptación telefónica, se modificó el tercer punto, reemplazando el verbo "indicar" en la frase "Indicar claramente el afectado por la medida intrusiva", por el verbo "identificar". De esta manera se exige un mayor nivel de precisión respecto del individuo afectado por la medida. En virtud de lo anterior, concluimos que la empresa no aceptaría solicitudes de carácter colectivo, sin embargo, lo ideal sería que Entel señalara expresamente que las solicitudes de información que contengan datos personales sensibles, junto con la orden judicial previa, deban también referirse a individuos determinados.

Valoramos positivamente que Entel ahora señala expresamente la obligación legal de la autoridad de notificar a las usuarias afectados por medidas intrusivas en los términos contenidos en el art. 224 del Código Procesal Penal.

La empresa recibe ¾ de estrella.

53 Disponible en: https://www.entel.cl/legales/centro-privacidad/public/pdf/guia%20solicitud%20judiciales.pdf?v=10 [Fecha última consulta: 23 de agosto de 2022]

4.2.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

En su sitio web, Entel pone a disposición del público un documento llamado "Compromiso Entel con la protección de información de sus clientes", en donde se muestra el compromiso que tiene Entel con la privacidad de datos y cómo, a través de gremios, se han realizados acciones de defensa de la privacidad.

En dicho documento destacan su participación voluntaria en alianzas con distintos actores sectoriales, como Chile Telcos, ACTI, Cámara Nacional de Comercio, Fundación País Digital, entre otros, con el objetivo de aunar esfuerzos en estrategias y posturas gremiales en diversos temas relevantes para las usuarias e industria, entre ellos, la protección de los datos de clientes, por ejemplo, por medio de las acciones realizadas durante el año 2021 mediante la Asociación de Empresas de Telecomunicaciones de Chile (Chile Telcos), oponiéndose al requerimiento de entrega de los datos de contacto de gran parte de las bases de datos de clientes de la compañía, instancia en la que se logró acordar compartir solo una muestra proporcional de la base de datos, lo que se traduce en una acción concreta de Entel por la defensa de la privacidad de sus clientes. Otro ejemplo es la acción realizada por la Asociación Chilena de Empresas de Tecnologías de Información (ACTI), que focalizó los esfuerzos para empujar observaciones y ajustes a lo que fue la tramitación del Proyecto de ley de Delitos informáticos.

Adicionalmente, valoramos el que la compañía ponga a disposición de sus usuarios diversas guías e infografías para ayudarles a defenderse de distintos tipos de ataques que pueden amenazar su ciberseguridad, dejando incluso constancia de un caso de phishing del cual se percataron.[54]

En vista de esto, Entel obtiene ½ estrella.

54 Disponible en: **https://www.entel.cl/legales/public/pdf/Campana_activa_de_Mekotio_busca_captar_clientes_de_Chile_resumen.pdf** [Fecha última consulta: 14 de junio de 2022]

4.3. GTD Manquehue

4.3.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

Al igual que el año pasado, GTD Manquehue mantiene a disposición del público tres contratos generales que pueden ser encontrados rápidamente haciendo clic en la sección "Contratos de Servicios Gtd", ubicada al final de su página web inicial. El primero, es una copia de su contrato de servicios de telecomunicaciones con las condiciones generales de contratación;[55] el segundo, es sobre condiciones de solicitud y contrato de servicios,[56] 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.[57]

La cláusula de "Tratamiento y Resguardo de los Datos Personales" (numeral 10 de las Condiciones Generales de Contratación de Servicios de Telecomunicaciones GTD Manquehue S.A., CGCST), se mantiene prácticamente inalterada, estableciendo 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, con la diferencia, que ahora la cláusula señala expresamente que se dará cumplimiento a los principios de licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, confidencialidad, limitación y transparencia, faltando únicamente el principio de lealtad. Por su parte, el numeral 13 del tercer documento, denominado "Condiciones Generales de Contratación GTD Móvil",[58] ahora replica en forma íntegra el texto del numeral 10 recién referido.

Otra de las novedades que trae GTD este año es la renovación de su Política de Privacidad y Protección de Datos Personales,[59] a la nueva edición de abril de 2022. Entre los nuevos aspectos destacamos el que ahora se señalen los objetivos que busca cumplir la política, siendo estos i) Que GTD pueda optimizar la toma de sus decisiones asociadas a los datos que captura

55 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: 05 de junio de 2022]

56 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: 05 de junio de 2022]

57 Disponible en: **https://www.gtd.cl/condiciones-comerciales/contratos-de-servicios-gtd/condiciones-generales-de-contratacion-gtd-movil** [Fecha última consulta: 05 de junio de 2022]

58 Disponible en: **https://www.gtd.cl/condiciones-comerciales/contratos-de-servicios-gtd/condiciones-generales-de-contratacion-gtd-movil** [Fecha última consulta: 26 de mayo de 2022]

59 Disponible en: **https://www.gtd.cl/media/gtd/pdf/Politica_Proteccion_de_Datos_Abril_2022.pdf** [Fecha última consulta: 26 de mayo de 2022]

o genera tanto en calidad de Dueño/Responsable como aquellos que recibe en calidad de Encargado/Procesador, ii) Reducir los costos y aumentar la eficiencia a través de una estructura y coordinación de un eventual gobierno de datos, iii) Designar los roles en los procesos relacionados con el manejo de datos, determinando funciones y responsabilidades, y iv) Asegurar el cumplimiento del marco normativo en manejo de datos; y la incorporación de una nueva sección de definiciones dónde se precisan los conceptos de dato personal, datos comerciales, dueño o responsable del tratamiento.

Felicitamos particularmente la incorporación del principio de Privacidad por Diseño, con el que se incluye un enfoque preventivo a la política; y la incorporación de una sección llamada Elementos de Control de la Política, mediante la cual GTD Manquehue se compromete a la realización de capacitaciones y de auditorías internas periódicas, estas últimas con el objeto de obtener información suficiente para el desarrollo de indicadores de medición de la fortaleza de la Política, que les permita realizar un análisis comparativo del alcance y desarrollo de una progresiva cultura de protección de los Datos Personales y Datos Comerciales.

Tanto el principio de Privacidad por Diseño como los Elementos de Control de la Política representan una novedad, y esperamos marque una pauta para las demás compañías, de manera que en una próxima versión podamos ver también reflejado este principio en otras políticas de privacidad.

Felicitamos a GTD Manquehue por todos los avances mostrados desde la última versión de este informe, lo que significa un salto exponencial en relación con los primeros informes. Sin embargo, para cumplir de manera satisfactoria con este criterio, aún faltan ciertos parámetros por satisfacer, como son: incluir el principio de lealtad, obligarse a notificar aquellos cambios que introduzca a las condiciones de tratamiento de datos personales (y así no traspasar a los usuarias la carga de revisar constantemente los documentos en busca de eventuales modificaciones); informar si comunica datos personales a terceros, y de ser el caso, la base jurídica y finalidades de dicha comunicación; incluir en su política de privacidad información relativa a los plazos de almacenamiento de los datos que tratan y su forma de eliminación una vez vencidos los plazos respectivos, y asimismo mayor información sobre la existencia o no de flujo transfronterizo de datos personales (la mera definición del concepto no entrega información sobre las operaciones de tratamiento de datos de GTD).

Considerando que aún faltan varios criterios por cumplir, pero también valorando los esfuerzos realizados por GTD Manquehue para mejorar sus cláusulas en materia de protección de datos personales, ***en esta categoría le otorgamos 3/4 de estrella.***

4.3.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

GTD Manquehue mantiene a disposición del público en su página web los informes de transparencia correspondientes a los años 2019, 2020 y 2021.[60] El informe 2021[61] muestra la información referida a las solicitudes recibidas durante dicho año ordenada según el tipo de solicitud recibida. El año 2021 recibieron un total de:

* 17 solicitudes de interceptación telefónica (vs 0 en 2020)
* 26 solicitudes de información general (vs 16 en 2020)
* 28 solicitud de metadatos (vs 35 en 2020)

Del total de 71 solicitudes, 22 fueron rechazadas u objetadas, lo que equivale a un 31% (tasa similar al 33% del año anterior). Las causales de rechazo dicen relación con 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.

Como novedad, este año GTD también muestra la información según un criterio geográfico, conforme al cual es posible ver que 57 de las 71 solicitudes recibidas se refieren a la región metropolitana.
Felicitamos a GTD Manquehue por mejorar el nivel de detalle de su informe de transparencia. Con todo, la metodología actual es más exigente en este parámetro y este año esperábamos conocer algunos detalles sobre los requerimientos de autoridad, que no están presentes en el informe de GTD Manquehue, tales como los motivos específicos de rechazo; las autoridades de las cuales han emanado los requerimientos; las categorías de datos involucradas en los distintos tipos de requerimientos; las solicitudes recibidas para bloquear el acceso a sitios web, para bloquear o filtrar contenido; y la existencia —o no— de solicitudes de naturaleza colectiva.

Tomando en consideración los criterios de la metodología, así como el nivel de detalle alcanzado por otras compañías en sus respectivos informes, ***GTD Manquehue recibe 1/2 de estrella.***

60 Disponible en: **https://www.gtd.cl/normativa/privacidad-y-proteccion-de-datos-personales** [Fecha última consulta: 26 de mayo de 2022]

61 Disponible en: **https://www.gtd.cl/media/gtd/pdf/Informe_Transparencia_2021.pdf** [Fecha última consulta: 26 de mayo de 2022]

4.3.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

Al igual que otras compañías, 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", en su "Protocolo de requerimiento de información".[62] Pero tal como hemos señalado en ocasiones anteriores, esta reserva no se traduce en absoluto en acciones concretas. Además, no encontramos en la página web de GTD Manquehue ningún antecedente donde conste la adopción de alguna otra acción para lograr este objetivo.

GTD Manquehue obtiene 0 estrellas.

4.3.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

GTD Manquehue cuenta con una Política de Requerimientos de Información actualizada. En su última versión, de abril de 2022,[63] GTD incorpora varias innovaciones. La primera de ellas dice relación con el principio de finalidad, y consiste en el compromiso de tratar la información personal de sus clientes única y exclusivamente para otorgar un servicio de calidad de acuerdo con lo establecido en su política de privacidad,[64] analizada precedentemente. El mismo párrafo añade que el acceso a la información personal de sus clientes está limitado únicamente a aquellos colaboradores que tienen necesidad de conocerla y teniendo como antecedente una fuente de licitud para dicho tratamiento, estando siempre obligados a velar por la confidencialidad de ésta. Continúa, ligando lo anterior al código de ética del Grupo GTD, conforme al cual "Para todos efectos, la información de los clientes adquiere carácter de confidencialidad para el Grupo GTD y todos sus trabajadores y, por lo mismo, es obligación de los trabajadores mantener bajo estricta reserva dicha información y no divulgarla bajo ningún concepto".

62 Disponible en: https://www.gtd.cl/documents/20121/4380870/Requerimientos_de_Informacion_Abril_2022.pdf. [Fecha consulta: 23 de agosto de 2022]

63 Disponible en: https://www.gtd.cl/documents/20121/4380870/Requerimientos_de_Informacion_Abril_2022.pdf. [Fecha consulta: 23 de agosto de 2022]

64 Disponible en: https://www.gtd.cl/media/gtd/pdf/Politica_Proteccion_de_Datos_Abril_2022.pdf [Fecha última consulta: 14 de junio de 2022]

Destacamos especialmente el hecho que la guía actual haga explícito que cuando la información solicitada se refiera una persona identificada o identificable se requerirá la respectiva orden judicial previa; y el que ahora detallen los datos de individualización de la causa que deben contener las solicitudes de registro de tráfico telefónico (número de folio interno del Ministerio Público, RUC de la investigación, delito asociado, fiscal a cargo de la investigación, correo electrónico institucional del fiscal y del funcionario policial), así como los antecedentes que deben adjuntarse a las solicitudes de interceptación telefónica (todo antecedente relevante para la realización de la medida, tales como: número de folio interno del Ministerio Público, Número o números de teléfono a interceptar, RUC de la investigación, delito asociado, fiscal a cargo de la investigación, institución policial con la que se trabaja, correo electrónico institucional del fiscal y del funcionario policial, fecha de la autorización judicial, tribunal que concedió la autorización). También valoramos que la guía actual haga explícito que las solicitudes de metadatos u otros datos asociados al cliente deberán ir acompañadas de la resolución judicial correspondiente y demás antecedentes que permitan realizar correctamente la medida de entrega de información solicitada.

Celebramos las mejoras introducidas por GTD Manquehue a su protocolo de requerimiento de información. Esperamos que en el futuro también puedan indicar el plazo máximo de almacenamiento de los datos y metadatos, y su forma de eliminación. Asimismo, instamos a la compañía a señalar expresamente en sus futuros protocolos que la información relativa a la ubicación de usuarios para efectos de políticas públicas, solo se entregará en forma agregada y anonimizada; y que para toda solicitud que conlleve la entrega de datos sensibles (v.gr. geolocalización) se requerirá —además de los requisitos comunes—, que la solicitud se refiera a personas determinadas.

Adicionalmente, este año esperábamos que las compañías hicieran referencia explícita a la norma legal que obliga a notificar a las personas afectadas por una medida investigativa intrusiva (artículo 224 del Código Procesal Penal). Este último criterio era particularmente importante, por tratarse de una obligación legal que no está siendo cumplida en el presente.

Considerando que aún faltan criterios por cumplir, pero también valorando los esfuerzos realizados por GTD Manquehue para mejorar su protocolo, ***en esta categoría le otorgamos 3/4 de estrella.***

4.3.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

Durante la elaboración del preinforme no se tuvieron a la vista documentos u otros antecedentes disponibles en la página web de GTD que demuestren que ha defendido los derechos de sus usuarios en sede judicial o en sede administrativa. Tampoco encontramos declaraciones que den cuenta de un rol activo en el ámbito legislativo para colaborar en leyes que brinden mayor protección a sus usuarios.
Sin perjuicio de lo anterior, con posterioridad al envío del preinforme, GTD dio cuenta de las actuaciones realizadas por intermedio de Atelmo en defensa de la privacidad y datos de las usuarias, ante el Consejo de Transparencia.

Al respecto, GTD señaló que haber participado activamente en la elaboración de estrategias y presentaciones, entre las cuales mencionan las siguientes:

* **Acciones ante el Consejo para la Transparencia**:
En diciembre de 2020, ATELMO, en representación de todos sus asociados, hizo una presentación ante el Consejo solicitando su pronunciamiento respecto de una serie de observaciones sobre la forma en que SUBTEL ha ejercido sus atribuciones legales en materia de recolección y tratamiento de datos personales en el sector de las telecomunicaciones.

A través del Oficio 127 de 30 de abril de 2021, el Consejo se pronunció acogiendo parcialmente la solicitud.

Contra esta resolución Atelmo (hoy Chile Telcos) interpuso un recurso de reposición, ya que si bien el Consejo acogió parcialmente el requerimiento de ATELMO, en lo referido a la falta de legitimidad de la Subsecretaría de Telecomunicaciones ("SUBTEL") para acceder y tratar los datos personales recolectados con ocasión del Reglamento y Norma Técnica relativos a la Ley N°21.046, incurrió en una errada interpretación de los hechos y el derecho al pronunciarse sobre la falta de apego a las normas sobre protección de datos personales que SUBTEL ha mostrado al momento de solicitar enormes volúmenes de información personal a las empresas de telecomunicaciones, comunicándolos a una empresa externa para la realización de encuestas de satisfacción de las usuarias.

El Consejo se pronunció del Recurso en Reposición, mediante oficio N° 224 de 26 de agosto de 2021, y rechazó el recurso interpuesto por la Asociación Gremial.

* **Acciones ante SUBTEL**:
En marzo de 2022, Chile Telcos hizo una presentación al Subsecretario de Telecomunicaciones, a propósito de la solicitud que hizo la Subsecretaría a la industria, y en particular a nuestras empresas asociadas, de datos personales de sus clientes, para efectos de la realización de encuestas de satisfacción 2021.

Se planteó al Subsecretario que nuestra industria es la primera en comprender el valor de la competencia efectiva, lo que desde luego implica mantener altos grados de satisfacción de nuestros clientes. Por otro lado, y como lo hemos señalado anteriormente en otras sedes, entendemos que no habría una habilitación legal expresa que permita a Subtel solicitar datos personales fuera de aquellos procesos en los que existen reclamos de usuarios. En dichos casos, se subentiende que las usuarias autorizan a esta Subsecretaría a recabar el detalle de su propia información. Sin ir más lejos, no hay otros organismos del Estado que tengan la citada facultad que Subtel declara detentar, pues si se revisan ejemplos como el Servicio Nacional del Consumidor, o alguna Superintendencia, en cada uno de esos organismos fiscalizadores, la vigilancia sobre estándares de satisfacción que supuestamente los habilitarían a pedir información personal, está encomendada a las propias empresas concesionarias y secundariamente al organismo público.

Sin perjuicio de lo anterior, y como también se ha mencionado por esta industria en las respectivas sedes, nuestro ordenamiento jurídico establece una serie de requisitos y obligaciones para la recolección, procesamiento y almacenamiento de información personal, contenidas o derivadas de la Ley N°19.628, sobre Protección a la Vida Privada que como responsables de la información de nuestros clientes no podemos dejar de cumplir. Especialmente relevantes son el principio de proporcionalidad (el volumen y la naturaleza de los datos recolectados debe tener relación con el fin buscado, y no pueden ser excesivos en relación con dicho fin) y de seguridad (deben tomarse medidas de resguardo suficientemente eficaces para asegurar la protección de las bases de datos personales que se están tratando, asumiendo los riesgos derivados de ese tratamiento, y evitando que los datos caigan en terceros no autorizados).

Como lo indicó el propio Consejo Para la Transparencia a Subtel, en relación a la proporcionalidad, en las operaciones de tratamiento de datos personales por parte de los Órganos de la Administración del Estado, "se deberá dar aplicación estricta al principio de proporcionalidad y mínima recolección de datos o minimización. (...) muchas de las amenazas a la adecuada protección de los datos personales surgen debido a la excesiva recopilación de características personales o registros que no son esenciales para el cumplimiento de las competencias y funciones del responsable del tratamiento". Además, este organismo sugiere que "los organismos públicos sigan pautas de minimización de datos, limitando la recopilación de información personal a aquella que sea directamente pertinente y necesaria para lograr un propósito específico". El principio de proporcionalidad mandata también evaluar las realidades distintas de cada una de las compañías, en cuanto a su base de clientes, para los distintos tipos de servicios sobre los cuales Subtel ha ordenado informar.

Se hizo presente que las solicitudes de datos que se realicen para las encuestas de satisfacción 2021 de Subtel deben tener en consideración estas directrices sobre la proporcionalidad, para evitar las amenazas a la adecuada protección de datos que el propio Consejo indica. La excesiva recopilación de datos no tiene justificación estadística, y es un peligro para la privacidad de las usuarias de telecomunicaciones. La realización de las encuestas contempladas en el estudio adjudicado no requiere de una base de datos de la dimensión solicitada a las empresas, incluso con tasas de respuesta de 1%, la cual es altamente improbable. Más aún, no se justifica que las bases de datos en algunos casos sean cercanas al total de la cartera para algunos servicios.

En vista de lo expuesto ***la empresa recibe ¼ de estrella.***

4.4. Movistar Chile

4.4.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

En el sitio web de Movistar, a tan solo un clic de distancia desde la página principal, es posible encontrar los modelos de sus contratos en el apartado "Condiciones Comerciales y Contractuales", dividido en Servicios Móviles[65] y Servicios Hogar.[66] En ambos apartados es posible encontrar una cláusula referida a la privacidad, prácticamente idéntica a la de años anteriores, dónde se limitaban a señalar que el tratamiento de datos personales informados o que se deriven de la contratación y uso del Servicio podrán ser tratados y/o utilizados por Telefónica Móviles Chile S.A. (TMCH) y su relacionada Telefónica Chile S.A (TCH), de conformidad a lo establecido por la ley Nº 19.628. Sin embargo, tras el informe preliminar de QDTD 2022, dónde se identificaron ciertas inconsistencias entre las cláusulas de los distintos servicios, Movistar armonizó su texto y agregó que dichos datos serán tratados de acuerdo con lo establecido en la Política de Privacidad, cuyo link de acceso puede ser consultado desde la misma cláusula.

Valoramos positivamente estos cambios realizados por Movistar, así como el hecho que la nueva edición de las Condiciones contractuales haga explícito el derecho de revocación establecido en la ley Nº 19.628, señalando que el mismo podrá ser ejercido en **https://www.movistar.cl**, o llamando al nivel 103 o 600 600 3000. También considera los mismos canales para solicitar modificaciones a sus datos personales sumando además el canal. Lo anterior puede ser consultado tanto en el apartado de Condiciones Contractuales como en el Centro de Transparencia de Movistar.[67]

Por otra parte, en el informe preliminar de QDTD 2022 advertimos que el documento titulado "Términos y Condiciones del Servicio de Sugerencia de Descarga de Aplicaciones y Contenidos"[68] (ubicado en la sección "Servicios Digitales" de la página de condiciones contractuales y comerciales),[69] tenía una política de tratamiento de datos muy diferente al resto de

65 Disponible en: **https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/** [Fecha última consulta: 23 de mayo de 2022]

66 Disponible en: **https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-hogar/** [Fecha última consulta: 23 de mayo de 2022]

67 Disponible en: **https://ww2.movistar.cl/centro-de-transparencia/condiciones-movistar-productos.html** [Fecha última consulta: 23 de julio de 2022]

68 Disponible en: **https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/pdf/Terminos_y_Condiciones_Servicio_Sugerencia_de_Descarga_de_Aplicaciones_y_Contenidos.pdf** [Fecha última consulta: 23 de mayo de 2022]

69 Disponible en: **https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/** [Fecha última consulta: 23 de julio de 2022]

los documentos analizados, indicándose que “para cualquiera de las finalidades previstas en la Política de Privacidad, Movistar podrá ordenar su tratamiento a proveedores de confianza”, agregando que, Movistar garantiza la adopción de las medidas necesarias para asegurar el tratamiento confidencial de dichos datos. En la misma línea, el documento “Política de Privacidad de Descarga de Aplicaciones y Contenidos”[70] tiene un apartado donde se refieren explícitamente a “la transferencia de datos internacionales” con sus socios de confianza y proveedores de servicios que operan a nivel mundial. Si bien notamos una incoherencia entre lo señalado precedentemente y la información contenida en la política de privacidad general de la empresa,[71] donde se indica explícitamente que los datos personales no son compartidos a personas ajenas a la Compañía, Movistar señaló que ello se explica por tratarse de un servicio prestado por un tercero proveedor, Digital Turbine, Inc., y que ellos no tienen injerencia en la elaboración o modificación de sus términos y condiciones. Con todo, queda la duda sobre cómo entonces Movistar podría cumplir con su compromiso de adoptar las medidas necesarias para asegurar el tratamiento confidencial de dichos datos.

Este año Movistar actualizó su política de privacidad[72] y además hizo explícita su fecha de entrada en vigencia e incorporó un vínculo para acceder a la versión pasada del documento. Todos cambios sugeridos tanto en el informe preliminar de esta versión de QDTD como en informes anteriores. Valoramos los cambios introducidos por Movistar, al mismo tiempo que le sugerimos incorporar en el futuro algún método de notificación para informar a sus usuarios de los cambios que pueda sufrir la referida política.

Dentro de los cambios realizados, ahora Movistar hace explícito que tratará los datos personales solo en aquellos casos en que estén habilitados por ley o cuenten con el consentimiento previo del titular, como establece la Ley 19.628. lo que es una manifestación del principio de finalidad. Destacamos el nuevo compromiso asumido por Movistar en orden a responder legalmente si se constata el incumplimiento de los principios y deberes legales relacionados con la protección de los datos personales de sus usuarios y suscriptores, haciendo manifiesto el principio de responsabilidad. Finalmente, Movistar hace una precisión nueva en su sección de ¨Personas u organismos a los cuales los datos son transmitidos y cedidos¨, indicando que para cualquiera de las finalidades previstas en la Política de Privacidad,

70 Disponible en: **https://ww2.movistar.cl/terminos-regulaciones/condiciones-comerciales-y-contractuales-movil/pdf/Politica_de_Privacidad_descarga_de_Aplicaciones_y_Contenidos.pdf** [Fecha última consulta: 23 de julio de 2022]

71 Disponible en: **https://ww2.movistar.cl/centro-de-transparencia/politica.html** [Fecha última consulta: 23 de julio de 2022]

72 Disponible en: **https://ww2.movistar.cl/centro-de-transparencia/politica.html** [Fecha última consulta: 23 de julio de 2022]

Movistar podrá encomendar el tratamiento de datos personales a Proveedores de confianza, quienes se han obligado contractualmente a garantizar el cumplimiento de los estándares de seguridad y de protección de la privacidad de Grupo Telefónica, con pleno respeto a la normativa vigente de protección de datos personales. Por último, en la versión actual de su política de privacidad Movistar informa sobre la entrega a la autoridad, para la adopción de políticas públicas, de información relativa a la ubicación y movilidad de sus usuarios, haciendo presente que en todos esos casos se han cautelado la privacidad de las personas, entregando la información en forma agregada, anonimizando los datos de las usuarias contemplados en la muestra. Este último punto es evaluado en la sección pertinente.

Sin perjuicio de los cambios realizados, nos sigue preocupando la amplitud y ambigüedad de aquella parte donde informan que tratarán "todos los datos personales que se originan a consecuencia de la prestación de los servicios de telecomunicaciones contratados". En nuestra opinión esto sería contrario a los principios de minimización, transparencia y lealtad. Además, tampoco señala por cuánto tiempo almacena los datos que recolecta ni cuál es su forma de eliminación una vez transcurridos los plazos que correspondan.

En cuanto a los principios mencionados en la metodología, dados los cambios realizados por Movistar a su política de privacidad, podemos decir que en la actualidad la compañía recoge de una manera u otra el principio de seguridad, el principio de responsabilidad, el principio de licitud, el principio de finalidad, y el principio de confidencialidad.

A diferencia de años anteriores, en esta oportunidad queremos felicitar a Movistar por los avances realizados en reacción al preinforme de esta edición de QDTD oportunidad en la que obtuvieron ½ estrella. Sin embargo, todavía vemos con preocupación las disonancias existentes entre los "Términos y Condiciones del Servicio de Sugerencia de Descarga de Aplicaciones y Contenidos" y los demás documentos analizados. Invitamos a la compañía a trabajar en la mejora de sus contratos y políticas. Para ello creemos que podrían servir de guía los criterios de evaluación contenidos en la metodología de este informe.

Si bien consideramos que aún faltan cambios por hacer, especialmente en relación a la información que entregan sobre las categorías de datos personales que recogen y tratan, reconocemos los esfuerzos realizados por Movistar en esta oportunidad, ***otorgándole en esta categoría ¾ de estrella.***

4.4.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

Movistar cuenta con un informe de transparencia actualizado, publicado tanto en el sitio web de su matriz internacional, como en la sección "Centro de Transparencia"[73] de su sitio web local.

Al igual que en su versión 2020, 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 restringir contenido y para suspender temporalmente el servicio. De conformidad con este informe, en 2021 Movistar Chile recibió 11.503 solicitudes de interceptación de comunicaciones, de las cuales 309 fueron rechazadas; 35.983 solicitudes de acceso a metadatos, de las cuales 2.543 fueron rechazadas, y ninguna solicitud para bloqueo y filtrado de determinados contenidos ni para suspender temporalmente el servicio.

El informe actualizado de Movistar no presenta diferencias con los informes anteriores en cuanto a las categorías de información que entregan. Esperamos que en el futuro Movistar pueda señalar por cuanto tiempo almacenan los datos y su forma de eliminación una vez transcurridos los plazos que correspondan; entregar información más detallada sobre los requerimientos recibidos, conforme lo establecido en la metodología de este informe (v.gr. incorporar criterio geográfico, señalar cuántas de las solicitudes recibidas se refieren a un individuo en particular o a una colectividad; informar qué autoridades solicitan datos y qué categorías de datos se incluyen en cada diferente tipo de solicitud; etc.), y qué categorías de datos se comunican a terceros y bajo qué resguardos. Esto último resulta especialmente relevante en el caso de Movistar, al tratarse de una empresa internacional.

Dado que Movistar no ha realizado cambios en cuanto al tipo de información que entrega en su informe, mostrando menos detalles que otras compañías, ***recibe en esta categoría ¾ de estrella.***

73 Disponible en: **https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf** [Fecha última consulta:23 de julio de 2022]

4.4.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

En el informe QDTD 2021 Movistar obtuvo ¼ de estrella en esta categoría. Dado que no se registran avances ni cambios en esta materia, en circunstancias que la metodología de este año resulta más exigente, ***la compañía recibe 0 estrellas.***

4.4.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

Movistar cuenta con un "Protocolo de entrega de datos a autoridades competentes",[74] disponible en su sitio "Centro para la Transparencia". Aquí Movistar Chile da a conocer su política en relación con 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.

En cuanto al "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.

74 Disponible en: **https://ww2.movistar.cl/centro-de-transparencia/protocolo.html** [Fecha última consulta: 5 de junio de 2022]

Bajo el título “Política de entrega de tráficos de llamadas”, Movistar diferencia entre llamadas entrantes y salientes de una línea, indicando que entrega las herramientas para que sus usuarios puedan tener acceso de manera eficaz y segura al tráfico de llamadas salientes de sus respectivas líneas, como extensión de su derecho de acceso a la información personal, ya que consideran que dicha comunicación es información personal del cliente o usuario que las origina. Esta misma consideración aplica a las llamadas entrantes, por lo que, el contenido de ellas no está a disposición del usuario receptor de las llamadas, excepto en el caso que exista una orden judicial que permita acceder a ese registro de llamadas.

Movistar informa que cuenta con un área especializada para requerimientos judiciales indicando inmediatamente el procedimiento de gestión de requerimientos. En el preinforme hicimos presente que la exigencia de resolución judicial para solicitudes de información no se contemplaba en esta sección (aunque reconociendo que si se mencionaba en su política de privacidad).[75] Movistar recogió esta observación incorporando una modificación en su Protocolo. De igual manera, Movistar recogió nuestra sugerencia de expresar que la información relativa a la ubicación de usuarios para efectos de políticas públicas solo se entregará en forma agregada y anonimizada, mediante la incorporación de un nuevo párrafo en su Política de Privacidad.

Invitamos a la compañía a actualizar su Protocolo de entrega de datos a autoridades competentes, y a incorporar, entre otros, información sobre el tiempo máximo de almacenamiento de los datos y metadatos; y su forma de eliminación.

Adicionalmente, este año esperábamos que las compañías hicieran referencia explícita a la norma legal que obliga a notificar a las personas afectadas por una medida investigativa intrusiva (artículo 224 del Código Procesal Penal).

La empresa recibe ¾ de estrella.

75 Disponible en: **https://ww2.movistar.cl/centro-de-transparencia/politica.html** [Fecha última consulta: 17 de mayo de 2022]

4.4.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

Valoramos la participación de Movistar en la declaración pública que a principios de 2022 realizaron Derechos Digitales, ACTI y el Centro de Estudios en Derecho Informático de la Universidad de Chile, entre otros, para mostrar el rechazo transversal generado por la norma introducida al proyecto de ley de delitos informáticos que buscaba autorizar el acceso a metadatos sin autorización judicial. Esta declaración fue clave para lograr la eliminación de dicha norma del proyecto. Asimismo, valoramos la participación de Movistar en Atelmo (hoy Chile Telcos), por las gestiones ya comentadas en el presente informe.

Con excepción de lo anterior, no encontramos otros antecedentes que den cuenta de una posición o rol de defensa activo por parte de Movistar en relación a la defensa de los derechos de sus usuarios, por lo que instamos a Movistar a involucrarse de manera más activa en la defensa de los derechos de sus usuarios.

La empresa recibe ½ de estrella.

4.5. VTR

4.5.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

En la parte inferior de la página principal de VTR, encontramos la sección "Condiciones y servicios".[76] Dentro de esta se nos presentan 3 contratos de suministro.

Los primeros dos contratos corresponden al de suministro de internet fijo[77] y al de suministro de internet móvil[78] y el tercero es un contrato de suministro de internet fijo para empresas.[79] Estos contienen una cláusula idéntica encontrada en la sección 13 de ambos documentos para internet fijo y la 11 para servicios móviles, la cual se integra mediante las Condiciones Generales de Contratación (CGC).

Esta parte por agregar contenido no contemplado a la fecha de envío de la versión preliminar de este informe, al indicar los tipos de datos que recolecta, procesa y almacena con el objeto de proveer el servicio de telecomunicaciones. Estos son:

1. Los datos que el suscriptor voluntariamente entregue al momento de suscribir el contrato, y en particular, aquellos datos incluidos en el formulario de solicitud de servicios que forma parte del presente contrato.

2. La información personal que se produzca con ocasión de la provisión de servicios de telecomunicaciones y que sea necesario almacenar y procesar para la entrega de dicho servicio o por mandato legal o de la autoridad competente.

La sección 13.2 del documento para internet fijo (11.2 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 suscriptores 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.

76 Documento disponible en: https://vtr.com/moviles_contratos [Fecha última consulta: 29 de mayo de 2022].

77 Documento disponible en: https://lla-cms-prod.directus.app/assets/76df6949-898d-4258-ba3c-e012388debc7..pdf [Fecha última consulta: 29 de mayo de 2022].

78 Documento disponible en: https://lla-cms-prod.directus.app/assets/e8266035-6878-404b-b0c5-2dbd6d6d2b3f..pdf [Fecha última consulta: 29 de mayo de 2022].

79 Documento disponible en: https://lla-cms-prod.directus.app/assets/4b513b90-b5cc-4f4d-987c-0af7b8d38d0f..pdf [Fecha última consulta: 29 de mayo de 2022].

La sección 13.3 del documento para internet fijo (11.3 para servicios móviles) alude al registro y análisis de información nominativa de cada suscriptor relativa al uso de los servicios y su interacción con VTR; por ejemplo, la fecha y duración de sus llamadas telefónicas, el volumen de tráfico de su conexión, 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, el tratamiento de esta información tiene por finalidad entregar adecuadamente los Servicios contratados o mejorar la forma en que se entregan sus servicios. Dicha información será procesada directamente por VTR o por sus proveedores de esta, velando por que se apliquen adecuados estándares de confidencialidad. Esta sección tiene la novedad de expresar que sucederá en los casos que dicha información sea procesada por medio de algún proveedor autorizado de VTR. Aquí se explica que, en dicho caso, el proveedor realizará el procesamiento en calidad de mandatario de VTR, con la finalidad exclusiva de entregar los servicios contratados y sujeto a condiciones de estricta reserva, 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.

Continuando con el análisis, La sección 13.4 (11.4 para servicios móviles) establece que, al momento de contratar, el cliente al marcar la casilla correspondiente en el formulario de solicitud de servicios que forme parte del contrato podrá autorizar a VTR o terceros autorizados para que en traten sus datos personales relativos a sus antecedentes de contacto, servicios contratados y/o comportamiento de pago. Asimismo, consciente para que VTR o terceros autorizados por ésta puedan enviarle comunicaciones publicitarias o comerciales. La novedad que trae consigo esta versión de la cláusula de protección de datos es que ahora exige una acción del usuario —marcar la casilla— para prestar consentimiento.

La sección 13.5 es completamente nueva y hace referencia a que VTR podrá compartir “esta información” —sin ser claros a si se refieren exclusivamente a la nombrada en la sección anterior—, con empresas del grupo Liberty Global, filiales, u otras empresas bajo control común; empresas relacionadas de VTR (según indica el art. 100 de la ley de mercado de valores) y con terceros con quienes la empresa mantiene relaciones comerciales.

En la sección 13.6 (11.4 para servicios móviles) En caso de ser terceros quienes envíen las comunicaciones publicitarias en virtud de la autorización de publicidad, estos deberán informar a los clientes la naturaleza de la asociación comercial con VTR. El cliente puede ejercer su facultad de revocar dicha autorización en cualquier momento. Siendo que en la versión anterior se necesitaba que una compañía remita información publicitaria para poder revocar la autorización.

Finalizando con la sección 13.7, se informa a los clientes que podrán hacer uso en cualquier momento los derechos de acceso, rectificación, cancelación u oposición de sus datos, sin alusión al procedimiento para estos fines.

De la misma manera que se indicó en la última versión de este informe, al tratarse de un contrato de adhesión, resulta en extremo preocupante que la cláusula 13.3 establezca que al momento de contratar el cliente autoriza tácitamente 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, 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 lo que, además, puede prestarse para robo de identidad o phishing, ya que el contacto se hace directamente con terceros y no a través de canales oficiales de la compañía. Esta modalidad contrasta, cada vez más, con la de otras compañías, que siguen un mucho más estricto estándar de finalidad, permitiendo únicamente 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.

Por su parte, VTR también tiene publicado un apartado destinado exclusivamente a comunicar su política de privacidad.[80] Este sitio contiene una introducción a la que le siguen distintas pestañas desplegables.

En dicha introducción destaca la primera modificación sustancial hecha a la política de privacidad: los cambios sustanciales de que sea objeto serán comunicados a los clientes y quedará registro de la versión y fecha de publicación de cada modificación a la Política. Felicitamos esta mejora, a la vez que invitamos a la compañía a señalar en el futuro cuál será el medio de notificación que utilizarán para dicho efecto.

La primera pestaña desplegable es también una adición nueva a la política y se refiere a los principios del tratamiento de datos. En este título se indica que el tratamiento de datos de VTR se verá sujeto a los 10 principios evaluados en esta versión del informe: licitud, finalidad, proporcionalidad, minimización de datos, calidad, responsabilidad, seguridad, transparencia, confidencialidad y lealtad. Los que proceden a desarrollarse.

80 Disponible en: **https://vtr.com/politica-privacidad** [Fecha última consulta: 26 de julio de 2022]

En el segundo apartado VTR define qué entiende por información personal, utilizando la definición de la ley 19.628 y mencionando explícitamente los datos de tráfico, direcciones IP, uso de internet (registro de navegación) e información personal como por ejemplo nombre y apellidos, direcciones, fecha de nacimiento, e información de facturación.

La tercera sección del sitio lleva el nombre de "¿Qué información personal recolectamos?" En primer lugar, se señala la información de contacto del usuario (nombres, dirección, números de teléfono, correo electrónico, nombres de usuario, edad, género, preferencias de lenguaje y detalles de envío de la boleta o factura). En segundo lugar, la información de la cuenta del usuario, como son los datos bancarios e información de facturación junto con la información entregada por ingresar a concursos además de que recolectan información de quienes los contactan para conocer sobre sus productos o servicios. En tercer lugar, información para entregar el servicio como el modelo y número de serie de tu D-Box, versión del software utilizada, smartcard ID, IP/dirección de Mac, y planes comerciales contratados. En cuarto lugar, información de uso general respecto a cómo las usuarias están usando los servicios sin necesidad de identificar al usuario, ejemplos de esto es la información recogida cuando el usuario hace llamadas telefónicas, navega por internet, visita el sitio web de VTR, ve programas de televisión, utiliza el Video on Demand (VOD) o los "App Store" de la empresa, o también cuando navega en los menús de televisión como la "Guía" o el catálogo de "VOD". En quinto y último lugar, se recolecta otra información personal, se refiere a aquella información obtenida tanto de fuentes públicas como enviada por otros operadores de telecomunicaciones.

Asimismo, se recolectará la información de otros individuos cuando sea entregada por el mismo usuario, por ejemplo, cuando compra un regalo para otra persona.

La cuarta pestaña informa con qué propósitos VTR utiliza la información recolectada dividiéndola en grupos, abordando así directamente el principio de finalidad.

* El primer grupo, dice servir para proveer productos y servicios. VTR recolecta, procesa y almacena información personal para instalar, mantener y proveer sus servicios, para procesos administrativos y para administrar concursos y sorteos. Estas actividades incluyen aprovisionamiento, soporte técnico, actualización de software y hardware, facturación, emisión de boletas, pagos y revisión de créditos.

* El segundo grupo se refiere a gestión de desempeño. VTR indica que podría usar tu inf ormación personal para indagar sobre la calidad de sus servicios y productos, la atención al cliente y su operación. Además, VTR expresa que en el grado que la ley lo permita, podría usar datos sobre el uso y acceso a nuestros servicios con el propósito de administrar el tráfico, facturas, consultas de clientes y la prevención o detección de fraudes. Asimismo, VTR podría monitorear y grabar sus comunicaciones con las usuarias, incluyendo correos electrónicos y conversaciones telefónicas, para fines de entrenamiento, aseguramiento de calidad, y para guardar detalles de productos y servicios solicitados por los mismos. Siempre informando previamente antes de grabar las comunicaciones.

* El tercer grupo tiene como finalidad que VTR mejore sus productos y servicios. En este grupo se utilizaría la información de uso general como, por ejemplo, información acerca del tráfico de subida para evitar afectar la calidad del servicio o realizar estudios de mercado.

* El cuarto grupo tiene como objetivo presentarle al usuario productos o servicios mediante comunicaciones directas con el usuario. Es necesario recordar que se puede solicitar en cualquier momento dejar de recibir estas comunicaciones.

* El quinto grupo tiene la finalidad de permitir la compra de bienes y servicios de los socios estratégicos de VTR. Si el usuario decidiese aprovechar alguna de estas ofertas o realizar una transacción, VTR recolectaría y comunicaría su información personal relevante al socio estratégico correspondiente, el que podría usar los datos personales para enviarle información adicional que podría ser de su interés. Es menester indicar que este tercero no se regirá por las políticas de privacidad de VTR sin embargo los socios de la empresa se comprometen a guardar la confidencialidad de los datos y respetar la ley.

* El sexto subgrupo se refiere a información necesaria para que VTR pueda cumplir con sus obligaciones legales. VTR para cumplir con los términos de un proceso legal válido o por requerimiento de otros organismos similares, podrá divulgar la información personal del cliente con o sin consentimiento y conocimiento, y con o sin aviso, de acuerdo con la legislación aplicable al caso. Sin embargo, VTR se reserva el derecho a cuestionar el acceso a información personal a las autoridades. VTR se compromete a verificar y exigir a la autoridad el cumplimiento de todos los requisitos y garantías establecidas en la legislación según se estudiará en la sección correspondiente.

Se hace la mención a que VTR podría usar información anónima y agregada para desarrollar informes y análisis estadísticos sobre los tipos de contenidos y/o publicidad (como un todo o en subgrupos) que son vistos u omitidos por sus usuarios, para estudios y otros propósitos legítimos del negocio.

La quinta pestaña está destinada a informar con quienes podría VTR divulgar los datos personales de sus usuarios. El primer caso, es con empresas dentro del grupo Liberty Global, las cuales deben suscribir y respetar la política de privacidad de VTR. El segundo son los empleados de la compañía los cuales deben mantener un deber de confidencialidad. En tercer lugar, están los socios estratégicos de VTR en caso de que el usuario acepte participar de una oferta o transacción especial presentada por ellos mismos, estos deben mantener la confidencialidad y respetar la ley como ya se dijo anteriormente. El cuarto caso ocurre si VTR es adquirido o se fusiona con otra empresa, en este caso la empresa deberá asumir los derechos y obligaciones que establece la política de privacidad para tratar datos. En quinto lugar, si se divulgan datos personales con terceros de confianza, se les requerirá mantener la información confidencial y segura y que sea solo utilizada con el fin de proveer los servicios específicos para VTR. Asimismo, se podrá divulgar información con empresas de validación de antecedentes comerciales. Para finalizar, se reitera que se podrá revelar información en los casos que la ley lo exija.

La sexta pestaña está 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, cifrado de información, firewalls, antivirus, sistema de detección de intrusos, detección de anomalías y control de accesos para sus colaboradores. Indican además que únicamente mantendrán la información por el tiempo necesario para los que fue recolectada, lo cual tiene únicamente como limitación que la ley especifique algo diferente.

La séptima pestaña detalla el procedimiento para evitar recibir comunicaciones promocionales o publicitarias, lo que se puede hacer mediante cualquier canal de atención de la empresa.

La octava pestaña explica qué son las cookies indicando que además de usar las cookies propias usan las de terceros.

En la novena pestaña VTR expresa que no es responsable por ninguna aplicación a la que puedas tener acceso a través del servicio “Sucursal Virtual”. Así como en la undécima pestaña se eximen de la responsabilidad por los sitios web a los que se pueda acceder mediante vínculos en el propio sitio web de VTR.

La décima pestaña recoge el principio de calidad, esta se denomina "¿Cuáles son tus derechos?". En ella VTR entrega un correo de contacto específico (**privacidad@vtr.cl**) para que sus usuarios puedan hacer efectivos sus derechos de acceso, rectificación, cancelación u oposición. Así como también dejan constancia de que se puede llamar al número de atención para solicitar no recibir más información de marketing o llamadas.

Finalmente, se agrega una fecha de entrada en vigor de la política actual y se pone a disposición su versión pasada en la página web.

Hacemos presente que gran parte de la información descrita precedentemente fue incorporada por VTR con posterioridad al envío de la versión preliminar de este informe. Felicitamos a VTR por su pronta reacción a las recomendaciones realizadas, y los esfuerzos realizados por mejorar el contenido de sus cláusulas contractuales y las disposiciones de su política de privacidad, las que ahora reflejan un mayor compromiso de la empresa con el respeto y la protección de los derechos de las usuarias. Sin perjuicio de lo anterior, instamos a la compañía a incorporar un método de notificación para los cambios que realice a sus cláusulas contractuales, hacer referencia expresa a la existencia o no de flujo transfronterizo de datos, y al proceso contemplado para la eliminación de los datos una vez transcurrido el plazo establecido para su almacenamiento. Este último debiera tener al menos un límite máximo y no limitarse a señalar que los mantendrán por tanto tiempo como sea necesario para cumplir con los propósitos para los cuales fueron recolectados.

La empresa obtiene ¾ estrellas.

4.5.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

El informe de transparencia de 2022[81] comprende el periodo de julio de 2021 a junio de 2022. Este hace un desglose entre solicitudes de interceptaciones telefónicas, solicitudes de información y solicitudes para bloquear o filtrar contenido, bloquear accesos a sitios web o suspender temporalmente el servicio de sus clientes.

Durante este periodo hubo 134 solicitudes de interceptación telefónica, todas correspondientes a telefonía móvil.

81 Disponible en: **https://lla-cms-prod.directus.app/assets/4a545aab-89ce-4026-b785-c4948298a43d.pdf** [Fecha última consulta: 26 de julio de 2022]

Durante el mismo periodo hubo 5.570 solicitudes de información las que se dividen en dos categorías: solicitudes de acceso a tráfico telefónico y solicitudes de otros datos.

Las 2.745 solicitudes de acceso a tráfico telefónico se desglosan en 4 categorías:

* Tráfico de llamadas Fono Fijo (26)
* Tráfico de llamadas Fono Móvil (67)
* Tráfico de antenas e información relativa a IP, MAC (116)
* Tráfico de IMEI (2.536)

Las 3.005 solicitudes de otros datos se desglosan a su vez en 4 categorías:

* Solicitudes de información de IMEI de equipos telefónicos móvil (1821)
* Solicitudes de información de clientes (1179)
* Solicitudes de copias de contrato de servicios (0)
* Solicitudes de copia de grabación de cámaras de seguridad (5)

Finalmente, se muestra que en 2022 ninguna de las solicitudes fue rechazada ya que todas cumplieron con los requisitos legales o bien, fueron enmendadas luego de haberse presentado observaciones ante errores formales.

VTR no recibió solicitudes para bloquear o filtrar contenido, bloquear accesos a sitios web o suspender temporalmente el servicio de sus clientes.

VTR no recibió solicitudes que hicieran referencia a una colectividad de individuos no identificados.

A pesar de no informar específicamente acerca de las solicitudes recibidas de metadatos, VTR sí indica que mantendrá el registro de los metadatos de comunicaciones de sus clientes por un plazo no inferior a un año, y serán eliminados tras 2 años.

Debido a que aún carece de información necesaria para cumplir con los criterios de este informe, ***la compañía obtiene ¾ de estrella en esta categoría.***

4.5.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

El protocolo de 2022[82] al igual que el analizado en la edición pasada, hace referencia explícita a la posibilidad de notificar a sus clientes respecto de una medida intrusiva que le haya afectado, solo se reservaba el derecho de hacer la notificación, sin comprometerse a ello, ni señalar en qué casos notificaría a sus clientes y en cuáles no. Por otro lado, la empresa tampoco muestra señales de encontrarse en algún proceso de discusión con la autoridad o de haber participado en el congreso para establecer un mecanismo de notificación para sus usuarios que han sido objeto de una medida intrusiva.

Vemos con preocupación la falta de actualización e iniciativa en la materia.

Dado lo anterior, ***en esta categoría VTR vuelve a recibir 0 estrellas.***

4.5.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

VTR cuenta con un protocolo de entrega de información a la autoridad, publicado en su página web, que data de 2022.[83] 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 el método de eliminación.

Este documento establece de forma bastante detallada el procedimiento que la autoridad deberá cumplir para requerir información personal de las usuarias 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 datos; 3) solicitudes de información que dicen relación con otros datos.

82 Disponible en: https://lla-cms-prod.directus.app/assets/683541ba-08f6-485f-8ae7-7fb0bdfa81e7.pdf [Fecha última consulta: 26 de julio de 2022]

83 Disponible en: https://lla-cms-prod.directus.app/assets/683541ba-08f6-485f-8ae7-7fb0bdfa81e7.pdf [Fecha última consulta: 26 de julio de 2022]

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). Agregando en la edición 2022 que para las solicitudes de interceptación comunes y urgentes, así como también las solicitudes de información las resoluciones judiciales deberán ser debidamente firmadas e individualizadas, excluyendo así la posibilidad de aplicar este tipo de medidas a una colectividad.

Por último, VTR ahora hace explícito que, conforme el artículo 224 del Código Procesal Penal, el Ministerio Público tiene el deber de notificar a la persona afectada por una medida intrusiva de investigación con posterioridad a su realización. Valoramos las mejoras introducidas por VTR en su protocolo de entrega de información a la autoridad. Esperamos que en el futuro puedan también informar la forma de eliminación de los datos y metadatos una vez transcurridos los plazos legales y explicitar que la información relativa a la ubicación de las usuarias solo puede ser entregada a la autoridad competente y de forma anonimizada y agregada.

En esta categoría VTR recibe ¾ de estrella.

4.5.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

Durante la elaboración del presente informe no se tuvieron a la vista documentos u otros antecedentes que demuestren que la empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente en sede judicial, administrativa o legislativa, durante el último año.

Sin perjuicio de lo anterior, con posterioridad al envío del preinforme, VTR dio cuenta de las actuaciones realizadas por intermedio de Atelmo en defensa de la privacidad y datos de las usuarias, ante el Consejo de Transparencia.

Dado lo anterior, ***VTR recibe ¼ de estrella en esta categoría.***

4.6. WOM

4.6.1. ¿Reflejan sus cláusulas contractuales y las disposiciones de su política de privacidad un compromiso de la empresa con el respeto y la protección de los derechos de las usuarias?

Tanto la política de privacidad como los modelos de contrato de servicios de WOM se encuentran a tan solo un par de clics de distancia desde la portada de su sitio web, específicamente desde la sección "términos comerciales, contractuales y transparencia"[84] ubicada en la parte inferior del sitio, que lleva a un menú desplegable dónde la información puede ser encontrada en una serie de títulos expandibles, resultando muy claro y fácil de manejar para el usuario.

Desde el primer título desplegable ("Política de Privacidad y Seguridad, Política de Contactabilidad y Estudios") es posible descargar tanto la actual política de privacidad (que data de febrero 2022),[85] como las de años anteriores (que datan de 2018 y 2019).[86]

La nueva política de privacidad de WOM trae varias novedades que evaluamos en forma positiva: suma dos nuevos principios a los ya contemplados (el de lealtad y el de transparencia e información); especifica de mejor manera las finalidades con las que podría tratar los datos que recolecta; señala las diversas fuentes desde las cuales recolecta los datos; declara que en los contratos que suscribe WOM y sus empresas relacionadas con terceros y que por su naturaleza tenga que entregar ciertos datos de sus clientes, se incluye una cláusula de confidencialidad, además de los NDA respectivos cuando los servicios son licitados ("Acuerdo de no divulgación o Contrato de Confidencialidad y No revelación" [en inglés, Non-Disclosure Agreement]); hace referencia a la existencia de flujo transfronterizo de datos (señalando que se encuentran resguardados por el principio de finalidad y la normativa internacional en la materia); y toma una conducta activa en el ámbito de la eliminación de datos, al declarar que los metadatos que almacena en cumplimiento de una obligación legal, son eliminados luego de 2 años de acuerdo a parámetros técnicos para asegurar su eliminación segura y la reserva de la misma (en cumplimiento del protocolo interno de eliminación de tráfico). Con todo, si bien suponemos que el plazo de 2 años se cuenta a partir del momento en que dicha información es recolectada, el texto no es del todo claro en ello. Otra cuestión que no queda clara es el plazo de almacenamiento de los datos personales que recolecta, toda vez que la sección sobre la eliminación de la información se refiere exclusivamente a los metadatos de comunicaciones de sus clientes, por lo que esperamos encontrar dicha información en futuras versiones

84 Disponible en: https://www.WOM.cl/terminos-condiciones/ [Fecha última consulta: 17 de mayo de 2022]

85 Disponible en: https://www.wom.cl/bases/bases/documents/wom-politica-de-privacidad-y-seguridad.pdf [Fecha última consulta: 28 de abril de 2022]

86 Disponible en: https://www.wom.cl/bases/bases/documents/politica-de-privacidad-versiones-anteriores.pdf [Fecha última consulta: 28 de abril de 2022]

de su política de privacidad. Asimismo, sería ideal que en una futura versión se volviera a hacer referencia expresa a la comercialización de los datos, de manera de tener certeza que su eliminación se traduce en un compromiso de la empresa en vender los datos de sus clientes.

Especial mención merece el compromiso adoptado por WOM en su política de privacidad, en orden a notificar a sus usuarios cualquier modificación a la misma, mediante un email, un SMS y/u otro medio que asegure su distribución oportuna. Finalmente, suman una sección sobre entrega de información a entidades, lo que será analizado en la sección 4.1.4.

Por otra parte, también es posible encontrar a la protección de los datos personales de clientes, en la cláusula octava de su contrato tipo para la contratación de servicios, cuya copia puede ser descargada desde la sección "Nuestro Contrato de Servicios".[87] El nuevo contrato es muy similar al que analizamos para la versión pasada de QDTD, con la ventaja de incluir expresamente el principio de seguridad y el principio de lealtad, y facilitar el ejercicio de los derechos Acceso, Rectificación, Cancelación y Oposición, que ahora podrán ser ejercidos también en sucursales y por medio del Call Center, además del mecanismo ya previsto, consistente en el envío de una comunicación escrita al correo **datospersonales@wom.cl**, canales por medio de los cuales también es posible solicitar el no envío de información publicitaria, promocional y/o de entretenimiento en **www.wom.cl/nomasinformacion**.

La empresa obtiene 1 estrella *al cumplir con todos los parámetros contemplados en esta sección.*

4.6.2. ¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?

Al igual que en años anteriores, WOM cuenta con un informe de transparencia actualizado, siendo posible descargar todas sus versiones (a contar de 2018) desde la sección "Informe de Transparencia y Defensa Privacidad Usuarios" de su menú desplegable.[88]

En el último informe publicado reconocemos varios avances. Este año WOM comenzó a dividir las solicitudes recibidas, según su emisor, en dos nuevas categorías: "Solicitud emitidas por el Ministerio Público y otras Instituciones afines del Estado de Chile" y "Solicitud emitidas por el Ministerio de Transportes y Telecomunicaciones a través de la Subsecretaría de Telecomunicaciones".

87 Disponible en: **https://www.wom.cl/bases/bases/documents/2022/contrato-de-servicios.pdf** [Fecha última consulta: 28 de abril de 2022]

88 Disponible en: **https://www.WOM.cl/bases/bases/documents/2022/Informe_Transparencia_2022.pdf** [Fecha última consulta: 26 de mayo de 2022]

Dentro de la categoría “Solicitud emitidas por el Ministerio Público y otras Instituciones afines del Estado de Chile”, la información sobre el total de solicitudes recibidas se divide en tres grupos distintos: 1) interceptaciones, 2) solicitudes de información, y 3) solicitudes de otros datos.

Durante el año 2021 se reportaron un total de 8.804 Solicitudes de Interceptaciones (lo que muestra un alza en comparación a las 8.700 de 2019 y 8.332 de 2020) de las cuales 197 fueron rechazadas, lo que significa un aumento importante en comparación con los 30 rechazos de 2020.

En cuanto al total de Solicitudes de Información, WOM declara haber recibido un total de 28.113 solicitudes durante el año 2021, doblando las 12.563 recibidas durante 2020. Estas solicitudes se encuentran desglosadas según el tipo de información solicitada, dando a conocer que 1.951 de ellas se relacionan a tráfico y 26.162 a “Otras Solicitudes de Información”. Esta última categoría se subdivide en: 1. Datos asociados a números telefónicos y simcards de WOM; 2. Datos asociados a RUT de personas o empresas clientes de WOM; y, 3. Número telefónicos asociados a IMEIs. Lamentablemente, dada la amplitud del término “datos asociados”, no es posible conocer con exactitud qué tipo de información es entregada por la compañía ante esta clase de solicitudes, ni qué porcentaje del universo “otras solicitudes de información” corresponde a cada una de estas subcategorías. Del total de Solicitudes de Información, 4.175 fueron rechazadas y/u observadas en 2021, número muy superior al de años anteriores (95 en 2019 y 1021 en 2020), y que se traduce en una tasa de rechazo u observaciones cercana al 16%.

WOM informa los rechazos de interceptaciones y/o de solicitudes de información se produjeron debido a la falta de antecedentes suficientes para sustentar los requerimientos conforme su política de requisitos para el envío de información a la autoridad en respuesta a requerimientos judiciales (“Protocolo de Entrega de Información a la Autoridad”) y de acuerdo con la normativa vigente. Sin embargo, esta información no permite conocer los motivos específicos en base a los cuales se han rechazado u observado estas solicitudes y, por tanto, las irregularidades que podrían estar ocurriendo en materia de solicitudes por parte de la autoridad. Por otra parte, en su informe 2020 WOM informó haber encontrado casos con diferencias entre la Resolución Judicial y la ficha del Sistema RESIT, no siendo claro si la omisión de este año al respecto se explica por la inexistencia de casos similares o solo en un menor detalle de la información entregada.

Por su parte, las “Solicitudes de Otros Datos” corresponden a una tercera categoría de requerimientos, distintos de los señalados en el artículo 222

inciso 5° del CPP, la cual comenzó a ser reportada en el Informe de Transparencia 2020.Durante el año 2021 se recibieron un total de 543 de estas solicitudes lo que muestra un aumento significativo respecto de las 14 solicitudes informadas en 2019 y las 218 de 2020. En cuanto a los datos solicitados, la compañía informa los siguientes 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. Lamentablemente, en esta categoría no se informa el número de solicitudes rechazadas, y la enunciación de las categorías de información solicitada a modo meramente ejemplar hace imposible conocer con exactitud los datos que podrían ser solicitados.

Valoramos que esta sección venga acompañada de distintos gráficos que facilitan la lectura de la información: tres tablas comparativas que permiten ver la evolución de las Solicitudes de Interceptaciones y de Información, a partir del año 2017, así como las de Otros Datos desde el año 2019, observándose un aumento significativo y sostenido en el tiempo para las tres categorías; una tabla de solicitudes de interceptaciones 2021 desagregada geográficamente; y otros dos que muestran el total de interceptaciones rechazadas por incumplimiento de requisitos legales desde el año 2019 en adelante, así como el total de solicitudes de información rechazadas y observadas.

Por último, valoramos la mención expresa que hace WOM en su informe 2021 respecto a solicitudes para bloquear el acceso a sitios web, para bloquear o filtrar contenido o para suspensiones temporales del servicio, declarando no haber recibido solicitudes de este tipo durante el 2021; así como el compromiso adoptado por WOM en esta sección, en orden a informar sobre aquellas solicitudes de información que digan relación con una colectividad (v.gr.: conectados a una antena determinada durante un periodo determinado) a partir del año 2021, respecto del cual informaron haber recibido 429 solicitudes.

Por su parte, las Solicitudes emitidas por el Ministerio de Transportes y Telecomunicaciones a través de la Subsecretaría de Telecomunicaciones se dividen en:

1. Solicitudes de fiscalización que incluían datos personales y
2. Solicitudes para encuestas de satisfacción de las usuarias de servicios de telecomunicaciones.

Durante el año 2021, las Solicitudes de fiscalización que incluían datos personales provinieron de 7 oficios ordinarios y/o circulares, mediante los cuales Subtel pidió a WOM determinada información, por ejemplo, boletas o números que han dado de baja el servicio, grabaciones de contratación, etc.

En cuanto a la categoría de Solicitudes para encuestas de satisfacción de las usuarias de servicios de telecomunicaciones, WOM informa haber recibido 2 oficios circulares (Oficio Circular N° 206[89] y Oficio Ordinario N° 11.645,[90] ambos de la División Análisis y Planificación de la Subtel), los cuales fueron respondidos por WOM requiriendo mayores antecedentes sobre el cumplimiento de la Resolución Exenta N° 304, de 30 de noviembre de 2020, en particular, sobre cómo se cumplen los principios de veracidad, finalidad, proporcionalidad, de seguridad, confidencialidad o secreto, deber de información, y por último deber de protección especial de los datos personales. Conforme lo publicado por WOM, aún no han sido notificados de la solicitud de información correspondiente a la "Etapa 2" del oficio circular, esto es, la muestra necesaria y suficiente de información requerida.

Valoramos positivamente los cambios realizados por WOM a su informe de transparencia, en orden a entregar mayor información sobre las solicitudes que reciben, especialmente en lo referido a las solicitudes de información que dicen relación con una colectividad y aquellas para bloquear el acceso a sitios web, para bloquear o filtrar contenido o para suspender temporalmente el servicio. Asimismo, reconocemos un mayor compromiso de la compañía con la protección de los derechos de sus usuarios en el número de solicitudes rechazadas, asumiendo que esto se explica en un análisis más profundo de las solicitudes que reciben. Con todo, esperamos que los informes futuros entreguen el detalle completo de las categorías de datos que les han sido requeridos, y especifique qué ha de entenderse por "datos asociados"; así como mayores detalles sobre el número de solicitudes que provienen de órdenes judiciales, y sobre los motivos específicos en base a los cuales se han rechazado u observado solicitudes, tal como requería la metodología de este año.

La empresa recibe 1 estrella.

4.6.3. ¿La empresa notifica a sus usuarios sobre las solicitudes de acceso a su información personal por parte de la autoridad o, al menos, ha realizado esfuerzos concretos para ello?

Dentro de la sub-sección "Informe de Transparencia y Defensa Privacidad Usuarios", bajo el título "Conoce nuestra declaración acerca de la notificación a usuarios respecto de solicitudes de autoridad", es posible encontrar una declaración de enero 2022 sobre las notificaciones a las usuarias por requerimientos judiciales.

89 WOM Oficio Circular N° 206.Disponible en: **https://www.WOM.cl/bases/bases/documents/neutralidad_condiciones/2022/2021Q3_oficios_y_respuestas_publico.pdf** [Fecha última consulta: 30 de mayo de 2022]

90 WOM Oficio Ordinario N° 11.645. Quinta página del documento disponible en: **https://www.WOM.cl/bases/bases/documents/neutralidad_condiciones/2022/2021Q3_oficios_y_respuestas_publico.pdf** [Fecha última consulta: 14 de junio de 2022]

En lo relativo al ámbito penal, el texto de este documento es prácticamente idéntico al de años anteriores, dónde informan haberse contactado con autoridades del Ministerio Público para explorar la vía por la cual se pueda notificar a las usuarias acerca de las solicitudes de acceso a su información personal o interceptaciones. Con todo, tal como se señala en el propio documento, dichos esfuerzos fueron realizados durante los años 2019 y 2020, con lo que no es posible acreditar la realización de acciones determinadas por parte de WOM para velar por el respeto del derecho a ser informado que tiene todo afectado por una medida intrusiva de investigación, conforme dispone el artículo 224 del Código Procesal Penal.

Como novedad, el documento contiene la siguiente declaración: "respecto de las causas civiles, laborales y de familia, WOM —a contar del 1° de enero de 2022— notificará a sus clientes por solicitudes de requerimiento de información, siempre que esta notificación no ponga en riesgo a los procedimientos y/o a terceros."[91] Esta declaración representa un avance por parte de WOM en materia de protección de los derechos de sus usuarios, aunque no explicita la forma en que estas notificaciones podrían ser realizadas, ni entrega otros antecedentes que permitan corroborar la eficacia de la medida. Instamos a la compañía a dar cuenta de su sistema de notificación en futuras declaraciones.

La empresa recibe ¾ de estrella *por incluir información relativa a requerimientos recibidos en el ámbito civil, y hacer públicas sus acciones en la materia analizada.*

4.6.4. ¿La empresa cuenta con una guía pública para el manejo de datos de las usuarias, destinada específicamente a orientar los requerimientos por parte de la autoridad, en relación con el procedimiento, requisitos y obligaciones legales que se deben cumplir para requerir información de las usuarias?

WOM cuenta con una de las guías más completas para el manejo de datos de las usuarias.[92] En su versión más reciente, publicada este año, destacamos que WOM haga explícito que la información relativa a la ubicación de sus usuarios para efectos de políticas públicas que les sea requerida solo podrá entregarse a la autoridad de forma anonimizada y agregada. Asimismo, consideramos como un avance las nuevas referencias

91 WOM. Declaración Enero 2022 en cuanto a las notificaciones a las usuarias por requerimientos judiciales. Disponible en: **https://www.wom.cl/bases/bases/documents/2022/declaracion-notificaciones-a-los-usuarios-2022.pdf** [Fecha última consulta:26 de mayo de 2022]

92 Disponible en: **https://www.wom.cl/bases/bases/documents/2022/protocolo-entrega-informacion-autoridad-2022.pdf** [Fecha última consulta: 29 de mayo de 2022]

al Decreto Ley N° 1.762 que crea la Subsecretaría de Telecomunicaciones y a la Ley N° 18.168 General de Telecomunicaciones, pues dan cuenta de una continua mejora en la calidad de la información que entrega. Otra de las novedades es la distinción que ahora hace —al igual como hizo en su Informe de Transparencia— entre solicitudes emitidas por el Ministerio Público y otras Instituciones afines del Estado de Chile, y aquellas emitidas por el Ministerio de Transportes y Telecomunicaciones y/o la Subsecretaría de Telecomunicaciones.

Las solicitudes emitidas por el Ministerio Público y otras Instituciones afines se dividen en Interceptaciones y Solicitudes de Información. En relación con las primeras, la información que se entrega se divide según se trate de a) solicitudes de interceptación comunes; b) solicitudes de interceptación urgente; c) casos de prórroga; d) modificación de canales de derivación; o, e) desconexiones anticipadas. En esta sección no encontramos diferencias sustanciales con el contenido del protocolo analizado para la versión anterior de nuestro estudio.

En cambio, en la sección "Solicitudes de Información" si encontramos algunas diferencias sustantivas, específicamente en la subsección sobre solicitudes relativas a tráficos y geolocalización, dónde se agrega como requisito para toda solicitud de información que contenga datos personales sensibles como la geolocalización, el que la orden deba referirse a personas determinadas, excluyendo la posibilidad de entregar este tipo de información respecto de una colectividad de usuarios indeterminados.

Por su parte, la sección relativa a las solicitudes emitidas por el Ministerio de Transportes y Telecomunicaciones y/o la Subsecretaría de Telecomunicaciones, es totalmente nueva. Felicitamos a WOM por incluir esta sección, la que contiene tanto los fundamentos normativos que facultan a estas entidades para hacer solicitudes a las empresas de telecomunicaciones, como los requisitos que estas deben cumplir. Así, el protocolo establece que los requerimientos en los que Subtel solicite información para vigilar, controlar y fiscalizar las telecomunicaciones en el país, deberán ser por escrito, mediante oficio correctamente foliado y firmado y especificar claramente el propósito y finalidad de la solicitud, así como también el cuerpo normativo que desea fiscalizar. Adicionalmente, WOM da otro paso significativo en la materia al manifestar que para el caso particular de encuestas de satisfacción de las usuarias de servicios de telecomunicaciones, se espera que Subtel especifique cómo cumple con lo estipulado por el Consejo para la Transparencia, mediante Resolución Exenta N° 304, de 30 de noviembre de 2020, la cual aprobó el texto actualizado y refundido de las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de

la Administración del Estado; y, por último, al comprometerse con que, cualquiera sea el caso, tomará los resguardos necesarios a fin de velar por la privacidad de los datos personales de nuestros usuarios y clientes. Como contrapartida, hacemos presente que la empresa no informa sobre el tiempo máximo durante el cual almacena la información que le puede ser requerida (no solo metadatos), ni sobre su forma de eliminación, como contempla la metodología.

Por último, valoramos que WOM haga explícita la obligación legal de la autoridad de notificar a las personas afectadas por una medida investigativa intrusiva, en los términos señalados en el artículo 224 del Código Procesal Penal. Dada la importancia de la notificación al afectado de las medidas intrusivas de las que ha sido objeto, y la constatación de tratarse de una obligación legal que no está siendo cumplida en la actualidad por la autoridad respectiva, este parámetro es un punto central de nuestra metodología.

En esta categoría WOM recibe 1 estrella.

4.6.5. ¿La empresa proveedora ha defendido la privacidad y protegido los datos de las usuarias activamente, ya sea públicamente, en sede judicial o administrativa o en el marco de una discusión legislativa en el Congreso?

En cuanto a la defensa activa de la privacidad y protección los datos de sus usuarios en sede administrativa, destacamos algunas de las acciones desplegadas por la compañía frente a solicitudes de Subtel, de que dan cuenta los documentos ubicados en la sección "Informe de Transparencia y Defensa Privacidad Usuarios",[93] misma en la que se encuentra la "declaración acerca de la notificación a usuarios respecto de solicitudes de autoridad 2022"[94] ya analizada.

En específico, en el ámbito de las solicitudes de fiscalización de Subtel, felicitamos la actitud tomada por WOM frente al Oficio Circular N° 293[95] de octubre 2021 de la División Análisis y Planificación, Subtel, en virtud del cual se le exigió entregar los números telefónicos de aquellos clientes que utilizaron el servicio de roaming en Argentina a partir de marzo de 2021.

93 Disponible en: **https://www.wom.cl/terminos-condiciones/** [Fecha última consulta: 22 de mayo de 2021]

94 Disponible en: **https://www.wom.cl/bases/bases/documents/2022/declaracion-notificaciones-a-los-usuarios-2022.pdf** [Fecha última consulta: 22 de mayo de 2021]

95 Disponible en: **https://www.wom.cl/bases/bases/documents/neutralidad_condiciones/2021/2021Q4_Oficios_y_Respuestas_Publico.pdf** [Fecha última consulta: 22 de mayo de 2021]

Dado el carácter colectivo de esta solicitud, WOM respondió censurando los datos personales contenidos en la documentación enviada en respuesta al oficio, con el fin de proteger la privacidad e información de sus clientes, y solicitando, además, “las acciones para que ésta sea tratada con el mayor resguardo y confidencialidad posible, dado que se trata de información comercial altamente sensible para la compañía y también para nuestros clientes”. Asimismo, valoramos positivamente que, en el ámbito de las solicitudes para encuestas de satisfacción de las usuarias de servicios de telecomunicaciones,

Asimismo, felicitamos a WOM por hacer presente la Resolución Exenta N°304, de 30 de noviembre de 2020 del Consejo para la Transparencia, para dar cuenta de las falencias de la solicitud recibida, con respecto a las obligaciones y principios que se deben respetar en materia de datos personales, y para exigir mayores antecedentes sobre la forma en que se daría cumplimiento a las indicaciones del Consejo de la Transparencia, y sobre las acciones qué se tomarían para asegurar que los datos personales de sus clientes fueran tratados de acuerdo a la normativa vigente.

En relación con la defensa de la privacidad y protección activa de los datos de sus usuarios en sede judicial y legislativa, WOM no tiene publicados documentos que den cuenta de cumplir con estos criterios.

La empresa recibe ½ estrella *al cumplir con la mitad de los parámetros contemplados para esta categoría.*

5. Tabla de resultados

¿QUIÉN DEFIENDE TUS DATOS?

DERECHOS DIGITALES América Latina

ELECTRONIC FRONTIER FOUNDATION EFF

2022

	Claro	Entel	GTD	Movistar	VTR	WOM
¿Refleja la política de privacidad y las cláusulas contractuales un compromiso de la empresa con la protección de los derechos de las usuarias?	★	★	★	★	★	★
¿Cuenta la empresa proveedora con un informe de transparencia actualizado que entrega información de calidad?	★	★	★	★	★	★
¿La empresa notifica a sus usuarias sobre las solicitudes de acceso a su información personal por parte de las autoridades?	★	☆	☆	☆	☆	★
¿La empresa cuenta con una guía pública para orientar a la autoridad a realizar requerimientos de información sobre sus usuarias?	★	★	★	★	★	★
¿La empresa ha protegido y defendido activamente la privacidad de sus usuarias y sus datos personales?	★	★	☆	★	☆	★
De un máximo de ***5 estrellas****, obtiene:*	5 ★★★★★	2,75 ★★½☆☆	2,25 ★★☆☆☆	2,75 ★★½☆☆	2,75 ★★½☆☆	4,25 ★★★★½

La escala de medición indica que:

★ cumple todos los parámetros

★ cumple con la mayor parte

☆ cumple parcialmente

☆ cumple con una mínima parte

☆ no cumple con ningún parámetro


DERECHOS
DIGITALES
América Latina