Universidad de Chile
Facultad de Derecho
Departamento de Derecho Comercial

REGULACIÓN DE LOS ÓRGANOS DEL ESTADO EN MATERIA DE DATOS PERSONALES: ANÁLISIS DESDE EL CASO ENTEL CON SUBSECRETARÍA DE TELECOMUNICACIONES

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

Isabel Alejandra Cantillana Cerón

Profesor guía: Claudio Magliona Markovitcth

Santiago de Chile
2020

Tabla de contenido

Resumen

El presente trabajo tiene como objetivo analizar la regulación de protección de datos personales que actualmente es aplicable a los órganos de la Administración del Estado, revisando los puntos que pueden ser mejorados. Para hacerlo, se tomará como punto de partida la controversia que inició por un requerimiento de información de la Subsecretaría de Telecomunicaciones a la empresa Entel.

En una primera parte, se analizarán conceptos generales de protección de datos personales, para tener un marco teórico sobre el cual analizar el caso. A continuación, se explicará la controversia en sus diversas etapas procesales, adoptando una perspectiva crítica de las decisiones administrativas y judiciales. En un tercer capítulo se desarrollará el caso dando aplicación a la legislación chilena vigente sobre protección de datos. Después, se procederá a detallar los elementos normativos que podrían ser modificados para evitar que casos como este vuelvan a ocurrir. Finalmente, se desarrollará una conclusión general resumiendo los distintos puntos revisados a lo largo del trabajo.

Introducción

La tecnología avanza cada día más rápido, lo que representa, innegablemente, grandes beneficios para las personas; pero no se puede ser indiferente a los riesgos que dichos avances pueden configurar para el completo goce de los derechos y libertades fundamentales. En ese sentido, el Derecho y los distintos operadores jurídicos deben tener herramientas suficientes para defender los intereses de las personas.

En materia de protección de datos personales, los riesgos se vuelven cada vez más patentes. El manejo de datos por grandes corporaciones y por los Estados, constituye una de las amenazas modernas más importantes a la privacidad y, sin la regulación adecuada, el tratamiento de datos, facilitado por la tecnología, puede terminar atentando contra la dignidad misma de las personas. Es en este contexto, relativo a la protección de datos personales y la forma en que esta protección debe ser regulada, que el presente trabajo se circunscribe.

El año 2018, la Subsecretaría de Telecomunicaciones requirió a las empresas que fiscaliza una serie de datos para proceder a realizar un estudio de satisfacción de los usuarios con los servicios de telecomunicaciones en el país. Esta solicitud inició un litigio en el que, una de las empresas, Entel, defendió su negativa a hacer entrega de la información, argumentando que esta calificaba como dato personal. En esta memoria se tomará como punto de partida el caso descrito para estudiar la regulación de datos personales que aplica a los órganos de la Administración del Estado.

En el primer capítulo, se definirán algunos de los conceptos claves para poder entender el caso que en este trabajo se presenta. Para ello, se expondrá, en lo relevante, la normativa vigente sobre protección de datos personales en Chile; las definiciones doctrinales y jurisprudenciales en la materia y el proyecto de ley que viene a modificar la normativa vigente. Finalmente se abordarán algunas recomendaciones de organizaciones internacionales y otras regulaciones de derecho comparado que serán útiles para el análisis del caso.

Después, en el segundo capítulo, se procederá a narrar el caso, para tener una base para su posterior análisis. Por eso, se enunciarán las alegaciones de la empresa Entel y de la Subtel en las distintas etapas de conocimiento de la controversia. Se reseñarán también las resoluciones que fueron dictadas por la Ministra de Transportes y Comunicaciones, la Corte

de Apelaciones de Santiago y la Corte Suprema. Finalmente, se procederá a comentar las sentencias.

A continuación, en el capítulo tercero, se procederá a reconstruir el caso desde la perspectiva de datos personales, analizando la calidad jurídica de la información requerida y las consecuencias que aquello acarrea tanto para los privados en juego, como para la Subsecretaría de Telecomunicaciones. Para ello se revisará la normativa vigente aplicable al caso y, brevemente, algunos elementos de la ciencia estadística para comprender si el tratamiento de datos en la realización de la encuesta de satisfacción fue correcto.

En el cuarto capítulo se hace referencia a la necesidad de modificar la normativa vigente en materia del derecho a la protección de datos personales para asegurar la eficacia de esa garantía fundamental. Así se contextualiza, mencionando la importancia de la información en la sociedad actual y el uso que hacen los Estados a su respecto. A continuación, se proponen algunos cambios normativos.

Finalmente, se hace una conclusión general del trabajo, resumiendo los hallazgos a los que se llegó al analizar el caso de Entel con la Subsecretaría de Telecomunicaciones y la normativa vigente en materia de protección de datos personales por parte de órganos de la Administración del Estado, planteando, por último, algunas consideraciones finales de cara al cambio normativo.

Capítulo I: Consideraciones generales

I. Marco jurídico de la protección de datos personales en Chile

El marco regulatorio vigente en materia de protección y tratamiento de datos personales está compuesto, en lo medular, por la disposición constitucional que incluye dicha protección en el listado de garantías fundamentales, los distintos tratados de derechos humanos que incluyen disposiciones relativas a la protección de la privacidad y la Ley N° 19.628 sobre Protección de la Vida Privada.

Sin perjuicio de que en este apartado se hará referencia exclusivamente a las normas antes señaladas, es necesario tener en cuenta que, en nuestro ordenamiento jurídico, podemos encontrar otras leyes que hacen alusión al tratamiento y protección de datos personales; lo que ocurre, por ejemplo, en materia laboral y de seguridad social, en la regulación de prestaciones de salud, en la reglamentación de las limitaciones al principio de transparencia y en la normativa tributaria.

1. Datos personales en la Constitución

Hasta antes de la reforma constitucional del año 2018, no existía disposición alguna que hiciera referencia expresa a la protección de datos personales como derecho fundamental. Por ello, el resguardo de este tipo de información se entendía como parte integrante del conjunto formado por los derechos de protección de la privacidad [1] y de inviolabilidad de las comunicaciones[2] sin reparar en la especificidad de la materia.

Recién con la modificación hecha el año 2018 a través de la ley N° 21.096 se incluye de forma expresa la protección de datos personales como derecho fundamental en el listado de garantías de la Constitución, respondiendo en parte a los cuestionamientos sobre “la ausencia de una institucionalidad específica e independiente que sirva para cautelar efectivamente los derechos asociados al tratamiento de datos”[3].

[1] Según la redacción antigua del artículo 19 N° 4 el respeto y protección a la vida privada y a la honra de la persona y su familia.
[2] La Constitución Política de la República, en su artículo 19 N° 5 establece “La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.”.
[3] Boletín N° 9.384-07, Proyecto de reforma constitucional, iniciado en moción de los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que consagra el derecho a la protección de los datos personales. Ingreso de Proyecto, p. 1.

La redacción vigente del artículo 19 señala que “la Constitución asegura a todas las personas: 4° El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley”[4].

Así, si bien se sigue relacionando la protección de datos con la protección a la vida privada, actualmente nuestra regulación considera que son derechos diferenciables, que cuentan con características propias. En la misma línea que las comprensiones contemporáneas del derecho a la privacidad y protección de datos.

En su redacción actual, la regulación constitucional establece principalmente dos cuestiones. En primer lugar, dispone que la protección de los datos personales es un derecho fundamental, lo que consagra a dicho resguardo como un límite a la actividad del Estado, ya que, como se señala en doctrina, “el sistema jurídico y muy especialmente sus derechos fundamentales, actuarán sobre el mismo poder limitando su libertad, sujetándole a restricciones en su voluntad y en su capacidad de acción”[5].

En segundo lugar, la redacción vigente del artículo 19 en su numeral cuarto tiene consecuencias sobre el sistema jurídico, porque, por un lado, establece que la regulación del tratamiento y protección de los datos quedará entregado a la ley y, por otro, permite el ejercicio del recurso de protección como medida para reparar acciones ilegales o arbitrarias que priven, perturben o amenacen el legítimo ejercicio del derecho antes mencionado.

2. Tratados internacionales de derechos humanos

El derecho internacional de derechos humanos ha consagrado en sus diversos instrumentos y, desde temprano, los derechos a la privacidad e inviolabilidad de las comunicaciones. Así, encontramos que la Declaración Universal de Derechos Humanos del año 1948 dispone que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales ataques”[6]. Por su parte, la Declaración Americana de Derechos y Deberes del Hombre, del mismo año, establece que “toda persona tiene derecho

[4] Como lo establece la Constitución Política de la República, en su artículo 19 N° 4, según su redacción vigente.
[5] PECES-BARBA, Gregorio, Curso de Derechos Fundamentales Teoría General, Imprenta de la Universidad Carlos III de Madrid, p. 348.
[6] Artículo 12 de la Declaración Universal de Derechos Humanos.

a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar"[7].

A su vez, dentro de los instrumentos vinculantes ratificados por Chile, el Pacto Internacional de Derechos Civiles y Políticos, establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"[8]. Una disposición similar existe en la Convención Americana sobre Derechos Humanos[9].

Considerando que el artículo 5° inciso 2° de la Constitución señala que "el ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana"[10] y, fundamentalmente, en su segunda parte, que "es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes"[11] y, que la doctrina del bloque de constitucionalidad ha sido reconocida por el Tribunal Constitucional, las disposiciones antes mencionadas deben ser vistas como ley, en el caso de los tratados y, como elementos interpretativos, en el caso de las declaraciones, en la resolución de controversias relativas a privacidad y, por extensión, protección de datos personales.

3. Datos personales en la legislación chilena

La regulación nacional de la protección de datos personales está contenida principalmente en la ley N° 19.628 sobre Protección de la Vida Privada. Este cuerpo regulatorio "constituye una normativa marco, de carácter general, que es aplicable a distintas circunstancias relativas al tratamiento de datos personales"[12].

La Ley sobre Protección de la Vida Privada regula el tratamiento de datos de carácter personal en registros o bancos de datos, sea que dicha operación se lleve a cabo por organismos públicos o por particulares. Excepciona de este tratamiento a aquel que se efectúe en ejercicio

[7] Artículo V de la Declaración Americana de los Derechos y Deberes del Hombre.
[8] Artículo 17.1. del Pacto Internacional de Derechos Civiles y Políticos.
[9] La Convención Americana de Derechos Humanos, establece en su artículo 11: "Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.".
[10] Artículo 5° inciso 2° de la Constitución Política de la República.
[11] Artículo 5° inciso 2° de la Constitución Política de la República.
[12] VIOLLIER, Pablo, 2017, El Estado de la Protección de Datos Personales en Chile. [En línea] <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [consulta: 6 de abril 2020] p. 16.

de las libertades de emitir opinión e informar. Así, se puede distinguir un ámbito objetivo y uno subjetivo de aplicación de la norma.

Para los casos en que la ley es aplicable, la entidad que realiza el tratamiento de datos deberá observar ciertos principios básicos, que garantizan en alguna medida la legitimidad de la utilización de los datos. Establece también, acciones que los titulares podrán ejercer si ven vulnerados sus derechos.

3.1. Ámbito de aplicación objetivo de la Ley N° 19.628

La Ley sobre Protección de la Vida Privada define una serie de términos que permiten especificar el alcance que tiene como cuerpo normativo. Recordando que, la ley será aplicable al tratamiento de datos personales realizado en registros o bancos de datos.

Así, respecto de las condiciones objetivas de aplicabilidad, señala que tratamiento de datos es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma"[13].

Además, se define al dato de carácter personal o dato personal como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables"[14]. La norma no especifica a qué se refiere con personas identificadas o identificables, lo que tendrá repercusiones al analizar el caso objeto del presente trabajo.

Por otro lado, la ley distingue al dato de carácter personal del dato sensible, estableciendo una relación de género especie entre ambos. Así, los datos sensibles son definidos como "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual"[15]. Esta distinción tendrá impacto sobre la forma en que se puede tratar, o no, la información.

Se define finalmente, a los registros o bancos de datos como "el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su

[13] Artículo 2 letra o) de la Ley N° 19.628 sobre Protección de la Vida Privada.
[14] Artículo 2 letra f) de la Ley N° 19.628 sobre Protección de la Vida Privada.
[15] Artículo 2 letra g) de la Ley N° 19.628 sobre Protección de la Vida Privada.

creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos"[16].

3.2. Ámbito de aplicación subjetivo de la Ley N° 19.628

En este nivel, primero, la ley señala que será titular de datos "la persona natural a la que se refieren los datos de carácter personal"[17]. Es a este individuo a quien la ley dota de determinados derechos.

Por otro lado, la ley de protección de la vida privada, en general, no hace diferencia respecto de la entidad que hace el tratamiento de datos. De este modo, se siguen prácticamente las mismas reglas en caso de que sea un privado o un órgano de la administración quien realiza operaciones con datos personales.

Sin perjuicio de lo anterior, en su Título IV, la Ley N° 19.628 establece algunas normas especiales para el tratamiento de datos por los organismos públicos. Así, señala que "el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia"[18] y ajustándose a las normas de la Ley, caso en el cual no se necesitará del consentimiento del titular de los datos. Se establece también que el "Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos"[19].

3.3. Aspectos generales de la Ley sobre Protección de la Vida Privada

Para los casos en que la normativa es aplicable, corresponderá a quien haga tratamiento de datos, observar los principios de finalidad e información, respetando el consentimiento de los titulares de los datos.

En lo fundamental, el principio de finalidad está contenido en el artículo noveno de la ley, que establece que "los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público"[20].

Expresiones del principio de información se aprecian en el artículo tercero que se refiere a en la recolección de datos a través de encuestas, estudios de mercado u otros equivalentes y

[16] Artículo 2 letra m) de la Ley N° 19.628 sobre Protección de la Vida Privada.
[17] Artículo 2 letra ñ) de la Ley N° 19.628 sobre Protección de la Vida Privada.
[18] Artículo 20 de la Ley N° 19.628 sobre Protección de la Vida Privada.
[19] Artículo 22 inciso 1° de la Ley N° 19.628 sobre Protección de la Vida Privada.
[20] Artículo 9 inciso 1° de la Ley N° 19.628 sobre Protección de la Vida Privada.

señala que “se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información”[21], y, en lo dispuesto en el artículo cuatro, el cual indica que “la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público”[22].

La legalidad y el consentimiento, por su parte, aparecen en el artículo cuarto, que establece que “el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello” [23]. Esta disposición señala también las condiciones de validez de la autorización hecha por el titular de datos personales.

Por otra parte, la regulación establece que el titular de los datos tendrá derecho de información y acceso; rectificación, cancelación o bloqueo; y, derecho a obtener copia sobre los datos que fueron tratados.

II. La protección de datos personales en la doctrina y jurisprudencia chilenas

1. Doctrina

La doctrina nacional ha desarrollado los principios que subyacen a la regulación antes mencionada. Otros, han insertado la protección de datos personales en un sistema normativo de protección de la vida privada. En esta sección se resumirán dichas perspectivas por cuanto constituyen criterios interpretativos que servirán para analizar las controversias en la materia; además, se revisarán algunas de las críticas más importantes que se hacen a la regulación vigente.

1.1. La normativa y sus principios

La doctrina en su trabajo hermenéutico se ha encargado de reconstruir la normativa de protección de datos personales. Así, algunas autoras y autores han enmarcado dicha regulación en un sistema constitucional de respeto a la privacidad, que estaría integrado por los derechos a la vida privada y a la inviolabilidad del hogar, las comunicaciones y los documentos privados; otros especialistas han contribuido estableciendo los principios que subyacen a las reglas.

[21] Artículo 3 inciso 1° de la Ley N° 19.628 sobre Protección de la Vida Privada.
[22] Artículo 4 inciso 2° de la Ley N° 19.628 sobre Protección de la Vida Privada.
[23] Artículo 4 de la Ley N° 19.628 sobre Protección de la Vida Privada.

Se señala en la literatura nacional que los derechos consagrados en la constitución, junto a las normas relevantes de tratados internacionales, configuran un "sistema constitucional de protección de la privacidad, que debiera servir a varios propósitos. Por una parte, servir de mandato constitucional para el legislador al momento de desarrollar, en el nivel legal, la protección efectiva de estos derechos; mandato para el juez al momento de interpretar y aplicar los derechos protegidos constitucionalmente; mandato para las autoridades públicas en el desempeño de sus funciones; entre otros"[24].

Sobre la Ley, la doctrina reconoce que el "legislador ha optado por lo que se denomina una ley ómnibus, esto es, una normativa general aplicable en diversos contextos en los cuales se verifica tratamiento de datos personales, a juzgar por la circunstancia de que ella misma no prevea tratamiento de datos que hayan de ceñirse a otras disposiciones legales y, más aún, legislación posterior se remite a ella para reglar el tratamiento de datos que se produce con motivo de un contrato de trabajo, del seguro de desempleo, de las prestaciones asociadas al virus de inmunodeficiencia humana y enfermedades catastróficas, así como las obligaciones de los prestadores de servicio de certificación de firma electrónica, o limitaciones al principio de transparencia pública activa"[25].

Quienes han escrito en esta materia, también hacen referencia a una serie de principios relativos al tratamiento de información, sobre los que estaría construida la normativa vigente. El primero de estos principios, es la llamada libertad en el tratamiento de datos personales. Al respecto se dice que "la ley dista de prohibir el tratamiento de datos personales, antes bien procura someterlo a un régimen jurídico que conjugue de un lado el interés de quienes requieren el procesamiento de ellos con una garantía a los derechos de aquellos a quienes se refieren"[26].

También se hace referencia al principio de información y consentimiento del titular pues, "siendo el propósito legislativo conferir facultades al titular de los datos personales para poder controlar la información que le concierne, indudablemente ha debido condicionar la legitimidad del tratamiento de sus datos al consentimiento previo, libre e informado prestado por él mismo"[27].

[24] ÁLVAREZ, Daniel, 2020, El sistema constitucional de protección de la privacidad en el derecho chileno. Revista del Departamento de Ciencias de la Computación de la Universidad de Chile, Edición N° 19. p. 43.
[25] CERDA, Alberto, 2012, Legislación sobre Protección de las Personas frente al tratamiento de Datos Personales. Apuntes de clases, Centro de Estudios de Derecho Informático. Universidad de Chile. p. 15
[26] CERDA, Alberto. Op. Cit. p. 20
[27] CERDA, Alberto. Ibid. p. 20.

Otro de los principios reconocidos en la normativa es el de finalidad, porque “si los datos son proporcionados por su titular, autorizando el tratamiento de los mismos con determinados objetivos, hemos de aceptar que su uso para fines diversos de aquellos que justificaron su recogida no puede quedar bajo el amparo de la ley”[28].

La ley también habría recogido el principio de calidad de los datos en el sentido de exigir “que ellos se correspondan con la situación real del titular a quién conciernen”[29].

Además, la normativa consideraría el principio de protección especial de datos sensibles, aquellos que demandan “un régimen jurídico especial, pues su tratamiento constituye un serio peligro de lesión para los derechos fundamentales”[30].

Sobre el deber de secreto, se señala al respecto que “la ley 19.628 ha acogido tal exigencia y ha previsto que quienes trabajan en el tratamiento de datos personales están obligados a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público”[31].

Finalmente, se habla de las garantías ante la transmisión de datos. Se dice que “nuestra ley 19.628 establece ciertas garantías frente a la transmisión de datos en general; sin embargo, no prevé disposición alguna sobre la transferencia transfronteriza de datos personales”[32].

1.2. Críticas a la legislación

Por otro lado, la doctrina no ha guardado silencio sobre los problemas de la normativa vigente. Fue, en parte, la crítica doctrinaria, la que motivó al legislador a incluir la protección de datos personales en el listado de garantías constitucionales y a proponer modificaciones a la ley 19.628.

Una de las críticas que se plantea tiene que ver con el hecho de que la Ley N° 19.628 sea una ley marco que, en su amplitud, no se hace cargo, en su especificidad, de todos los problemas que surgen a propósito del tratamiento de datos. Al respecto, hay quienes, consideran

[28] CERDA, Alberto. Ibid. p. 23.
[29] CERDA, Alberto. Ibid. p. 24.
[30] CERDA, Alberto. Ibid. p. 24.
[31] CERDA, Alberto. Ibid. p. 26.
[32] CERDA, Alberto. Ibid. p. 26.

conveniente “inclinarse por una legislación mixta, que conjugue la necesidad de disponer de un marco normativo general y satisfacer los requerimientos particulares”[33].

También se ha dicho que “se puede sostener que la Ley N° 19.628 se limita a regular el mercado de los datos personales eliminando o disminuyendo en lo posible los obstáculos para la actividad, pero no ha puesto su foco en la protección de los derechos de los titulares de esos datos, lo que acarrea la carencia de una adecuada protección de los datos personales que esté en sintonía con lo que los socios comerciales de países más avanzados exigen a Chile”[34].

Entre los cuestionamientos más fuertes se encuentran aquellos referidos al hecho de que no exista un órgano con facultades para fiscalizar el cumplimiento de la normativa de protección de datos. En ese sentido, “constituye hoy una opinión generalizada y mayoritaria, la necesidad de contar con una autoridad de control en materia de protección de datos personales en Chile. El disenso se produce al momento de determinar qué órgano debiera ejercer dicha función”[35].

En definitiva, la doctrina entiende que, en la Ley “solamente se ha regulado el tratamiento de datos y no un derecho efectivo de los titulares a tener control sobre los mismos. Esto es así, entre otras razones, por la inexistencia de un ente fiscalizador, de un procedimiento administrativo efectivo de reclamo y la falta de sanciones eficaces y disuasivas. Lo único que existe a este respecto es una acción judicial especial que se interpone ante los tribunales ordinarios, la acción de *habeas data* de escasa aplicación práctica”[36]

2. Jurisprudencia

En este punto se revisará de forma general y breve aquello que han señalado, por una parte, la Contraloría General de la República y el Consejo para la Transparencia, que se han pronunciado respecto del tratamiento de datos por parte de Órganos del Estado; y por otra, los tribunales ordinarios, que conocen controversias de datos personales contra entidades públicas y privadas, a través de las acciones de *habeas data* y del recurso de protección.

[33] CERDA, Alberto. Op. Cit. p. 15
[34] CAMACHO, Gladys. 2014. La protección de datos como frontera del derecho de acceso a la información en la legislación chilena. *Revista de Gestión Pública*. Vol. 3, n. 1. p. 81.
[35] ÁLVAREZ, Daniel. Acceso a la información pública y Protección de Datos Personales. 2016. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *RDUCN*. Vol. 23. n. 1. p. 60. [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-97532016000100003&lng=es&nrm=iso>.
[36] ÁLVAREZ, Daniel. Acceso a la información pública… Op. cit. pp. 62 y 63.

2.1. Jurisprudencia administrativa

La Contraloría General de la República ha dado aplicación a la normativa de la ley 19.628 en múltiples ocasiones[37]. Al respecto, ha dictaminado la legalidad del tratamiento de datos personales por parte de diversos órganos de la administración, señalando que, en dicha operación, los datos deben "ser utilizados estrictamente dentro del marco de las funciones del servicio"[38].

Por su parte, el Consejo para la Transparencia, es una entidad que ha asumido la responsabilidad de velar por la protección de datos personales en la administración pública, al no existir un organismo que se dedique a velar por el cumplimiento de la normativa en esta materia. Algunos autores han señalado que es problemático que sea esta institución la que garantice la protección de datos, porque la principal función del Consejo es velar por la correcta aplicación de la Ley de Transparencia, de modo que "le ha correspondido realizar una labor de armonización y ponderación de estos valores jurídicos"[39].

Sin perjuicio de lo anterior, el Consejo ha realizado un trabajo importante al dictar Recomendaciones que "tienen por objeto orientar la aplicación concreta del nuevo derecho fundamental a la protección de datos personales, además de entregar criterios jurídicos a los órganos de la Administración del Estado en el tratamiento de datos personales que realicen dentro del ámbito de sus competencias, a fin de dar cumplimiento a las obligaciones legales que éstos tienen como responsables de tratamiento, conforme a lo dispuesto en la ley N°19.628 y en las demás normas pertinentes."[40]

2.2. Jurisprudencia judicial

Por su parte, la justicia ordinaria puede conocer de causas relativas a datos personales, en general, por dos vías. Primero, a través de la acción de *habeas data,* establecida en la ley 19.628, que permite a los titulares de datos que se han visto perturbados en sus derechos y, segundo, por el recurso de protección, desde la reciente incorporación del derecho al amparo de los datos personales en el listado de garantías constitucionales.

---

[37] Ver, por ejemplo, Dictámenes N° 37456 de 2010, N° 38604 de 2010, N° 25682 de 2019 y N° 11171 de 2020, de la Contraloría General de la República.
[38] Dictamen N° 25682 de la Contraloría General de la República, del 27 de septiembre de 2019
[39] CAMACHO, Gladys. Op. Cit. p. 86
[40] Resolución exenta N° 304 del Consejo para la Transparencia, de 2020, que aprueba 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 Sustituye texto que indica.

Hay tribunales que se han pronunciado respecto de la compatibilidad del recurso de protección con la acción de *habeas data,* en ese sentido se ha señalado que "corresponde desestimar la alegación de la recurrida respecto a la improcedencia de la acción constitucional materia de autos por el hecho que la recurrente pueda ejercer otras acciones, como las del procedimiento especial denominado 'Habeas Data' previsto en el artículo 16 de la Ley 19.628. Ello debido a que la interposición de la acción de protección, como se dijo, no es incompatible con las demás acciones que la recurrente pudiese ejercer en otras instancias, administrativas y/o judiciales"[41].

Quien también ha tenido algo que decir sobre la protección de datos personales es el Tribunal Constitucional, se ha señalado que, si bien el reconocimiento ha sido tardío y poco sistemático, se han establecido ciertos estándares, que son: el principio de legalidad en la protección de datos personales; fundamento en la primacía axiológica del ser humano de la protección de datos personales y el libre desarrollo de la personalidad; el principio del consentimiento para la injerencia en la esfera amparada; el efecto horizontal de esta garantía; que la protección de la vida privada no es un derecho absoluto y sus restricciones deben tener por fundamento un objetivo legítimo; el principio de no afectación a un bien jurídico superior; la protección constitucional de datos personales (datos sensibles) y su anclaje constitucional en la protección de la vida privada; la irrelevancia de la cualidad del ámbito especial de desarrollo de la actividad libre amparada por el derecho; el principio de protección con garantías adecuadas y suficientes; principio de no lesión de intereses sociales o derechos fundamentales; y, la interdicción de seguimientos o monitoreos sistemáticos, constantes y focalizados[42].

Con todo, es difícil hablar de que exista una jurisprudencia robusta en materia de protección y tratamiento de datos personales. Es más, puede decirse que hay un desconocimiento de la materia por parte de los tribunales, lo que es patente en el caso que se analizará en los capítulos siguientes.

III. Proyectos de ley relativos a protección de datos personales

Actualmente y, producto de las fallas en la regulación denunciadas por la doctrina y la sociedad civil en general, hay más de 60 iniciativas legales en tramitación relativas a la protección y tratamiento de datos personales, algunas apuntan a modernizar la totalidad de la ley 19.628,

[41] Sentencia de la Corte de Apelaciones de Valdivia, del día 21 de marzo de 2019, en autos rol N° 379-2019 caratulados Soto/Yoliquido S.A. p. 5.
[42] Al respecto, ver: QUEZADA RODRÍGUEZ, Flavio, 2012, La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile, Revista Chilena de Derecho y Tecnología, Universidad de Chile, Vol. 1 N°1. pp. 144 y 145.

acercándola a los nuevos estándares internacionales y otras, apuntan a resolver algunos problemas particulares[43].

El año 2017, se presentaron dos iniciativas de reforma total a la norma vigente sobre protección de datos personales, el primero proyecto de ley, de moción parlamentaria, ingresó el 17 de enero al Senado[44]. El segundo proyecto, iniciado por mensaje del ejecutivo[45], se puso en conocimiento de la Cámara Alta el 15 de marzo del mismo año. Actualmente, ambos proyectos han sido refundidos y se encuentran en primer trámite constitucional.

El proyecto reconoce que la Ley sobre Protección de la Vida Privada constituye, en la actualidad, una regulación insuficiente para dar efectiva protección a los datos personales y sus titulares y, en este sentido, se señala que "la obsolescencia de algunos de sus criterios u orientaciones y la ausencia de una autoridad de control que den eficacia a la ley, son parte de un diagnóstico en el que existe un amplio consenso entre los actores políticos e institucionales, agentes económicos, medios de comunicación social y ciudadanía en general"[46].

Se establece, entonces, como objetivo particular la modernización de estándares para el tratamiento de datos personales por organismos públicos[47]. Al respecto se señala que "el tratamiento de los datos personales que efectúan los órganos públicos será lícito cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de conformidad a las normas legales correspondientes"[48], de forma similar a la regulación

[43] Por ejemplo, el año 2020, ingresó un proyecto de ley que modifica la ley N°20.575, que establece el principio de finalidad en el tratamiento de datos personales, para prohibir la exigencia de la información a que ella se refiere, en los procesos de otorgamiento de créditos, con ocasión de la pandemia de Covid-19. Podemos incluir, también, el proyecto de ley que modifica la ley n°19.496, que establece normas sobre protección de los derechos de los consumidores, en el sentido de imponer a los proveedores que indica, la obligación de dar a conocer las vulneraciones a las bases de datos que contengan información sobre sus clientes y usuarios.
[44] Proyecto de Ley sobre Protección de Datos Personales, Boletín N° 11092-07.
[45] Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.
[46] Mensaje del Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07. p. 3.
[47] El proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07, contiene disposiciones relacionadas con las siguientes temáticas: 1. Determinación precisa del ámbito regulatorio, 2. Principios rectores y actualización de definiciones legales, 3. Reforzamiento y ampliación de los derechos de los titulares de datos, 4. Consentimiento del titular como la principal fuente de legitimidad del tratamiento de datos, 5. Régimen de responsabilidades de los responsables de datos, 6. Nuevos estándares para el tratamiento de datos sensibles y categorías especiales de datos personales, 7. Tratamiento de datos personales de niños, niñas y adolescentes, 8. Regulación del flujo transfronterizo de datos personales, 9. Modernización de estándares para el tratamiento de datos personales por organismos públicos, 10. Creación de una autoridad de control, 11. Modelo general de cumplimiento de la ley, 12. Disposiciones transitorias.
[48] Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07

actual, se dice que, en cumplimiento de dicha condición de legalidad, el tratamiento no requiere consentimiento del titular.

Se incorpora la "facultad de los órganos públicos para comunicar o ceder datos personales a otros órganos públicos, siempre que la comunicación o cesión de los datos sea necesaria para el cumplimiento de funciones legales y ambos actúen dentro del ámbito de sus competencias"[49], para favorecer la eficiencia en la gestión pública. Agrega que "también pueden comunicar o ceder datos personales cuando se requieran para un tratamiento que tenga por finalidad otorgar beneficios al titular, evitar duplicidad de trámites o reiteración de requerimientos de información o documentos para los titulares"[50].

Se señala que "también se regula la comunicación y cesión de datos a personas o entidades privadas"[51]. Esto, constituye una completa innovación respecto de la regulación vigente y se consagra en el proyecto de ley, al señalar, en un primer lugar, que "para los efectos de poder comunicar o ceder datos personales a personas o entidades privadas, los organismos públicos deberán contar con el consentimiento inequívoco del titular, obtenido al momento de la recolección de los datos o con posterioridad a ella"[52] y, a continuación, que "las cesiones de todo o parte de sus bases de datos personales realizadas por un órgano público deberán constar por escrito a través de un convenio suscrito por el cedente y el órgano o persona cesionaria de la información"[53].

Finalmente, en el proyecto "se consagran y regulan los principios que rigen el tratamiento de los datos personales por parte de los órganos públicos, los derechos que se reconocen a los titulares, la forma de ejercer estos derechos y se define un procedimiento de reclamación administrativa y de tutela judicial efectiva para el ejercicio y protección de estos derechos"[54].

---

[49] Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07

[50] Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07

[51] Mensaje del proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07. p. 9.

[52] Artículo 22 inciso 4, primera parte, proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07, según el archivo en que ingresó el 15 de marzo de 2017. Desde esa fecha, se han presentado indicaciones a estos artículos por parte del ejecutivo y parlamentarios.

[53] Artículo 22 inciso 5, primera parte, proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07, según el archivo en que ingresó el 15 de marzo de 2017. Desde esa fecha, se han presentado indicaciones a estos artículos por parte del ejecutivo y parlamentarios.

[54] Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, boletín N° 11144-07

IV. Aproximaciones internacionales a los datos personales

La regulación de la protección y el tratamiento de datos personales se ha abordado también por organizaciones internacionales. Por ello, en esta sección se revisarán las recomendaciones en la materia hechas por la Organización de Estados Americanos y la Organización para la Cooperación y Desarrollo Económico a sus Estados Miembros.

Por otro lado, se resumirán los principios esenciales del reglamento europeo de datos personales, el cuerpo normativo más reciente, evolucionado y adaptado a la era digital en la materia, porque, si bien sus disposiciones no pueden ser consideradas ley a la hora de resolver controversias en nuestro país, si pueden constituir criterio interpretativo.

1. Organización de Estados Americanos

La Organización de Estados Americanos (OEA) ha recomendado a sus Estados Miembros tomar medidas para mejorar las regulaciones de datos personales en la región. En ese sentido, la Asamblea General resolvió "reafirmar la importancia de proteger los datos personales y de respetar el derecho a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como el derecho de toda persona a la protección de la ley contra esas injerencias, de acuerdo con lo establecido en la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Declaración Americana de los Derechos y Deberes del Hombre y la Convención Americana sobre Derechos Humanos"[55].

Por otro lado, el Departamento de Derecho Internacional de la OEA, se encuentra actualmente elaborando una Ley Modelo Interamericana sobre Protección de Datos Personales, que sirva para la modernización de las normativas de la región.

Para su construcción se considerarían doce principios, los de propósitos legítimos y justos, claridad y consentimiento, pertinencia y necesidad, uso limitado y retención, deber de confidencialidad, protección y seguridad, fidelidad de la información, acceso y corrección, información sensible, responsabilidad, flujo transfronterizo de información y responsabilidad y publicidad de las excepciones[56].

---

[55] Organización de Estados Americanos, AG/RES. 2842 (XLIV-O/14) Acceso a la Información Pública y Protección de Datos Personales. [En línea] <http://www.oas.org/es/sla/ddi/docs/AG-RES_2842_XLIV-O-14.pdf> [Consulta: 13 de septiembre, 2020]

[56] Organización de Estados Americanos, Ley Modelo Interamericana sobre protección de Datos Personales (en elaboración). [En línea] <http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp> [Consulta: 13 de septiembre, 2020]

2. Organización para la Cooperación y el Desarrollo Económicos

El año 2010 Chile ingresó a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), tras esto, el país adquirió el compromiso de seguir realizando modificaciones a las estructuras democráticas y económicas para cumplir con los estándares de la organización. Dentro de aquellos desafíos de modernización, se encuentra la adaptación de la normativa sobre protección de la privacidad para la era digital.

En particular, la OCDE dictó Directrices de sobre Protección de la Privacidad y Flujos Transfronterizos de Datos, que fueron adoptadas inicialmente en 1980 y actualizadas en el 2013. "Su objetivo, si bien recoge los principios que informan la protección de datos personales, consiste en adoptar estándares mínimos para garantizar la privacidad, ello a pesar de que carece de un carácter vinculante"[57].

En lo medular, la Directriz consagra entre sus principios básicos de aplicación nacional los de limitación de recogida, calidad de los datos, especificación del propósito, limitación de uso, salvaguardia de la seguridad, transparencia, participación individual y responsabilidad[58].

3. Normativa europea de protección de datos personales

En Derecho comparado, el cuerpo normativo más importante en esta materia es el Reglamento General de Protección de Datos de la Unión Europea[59] (o GDPR por sus siglas en inglés). Esta norma viene a reforzar la consagración de la protección de datos personales como derecho fundamental en la Carta de Derechos Fundamentales de la UE[60] y el Tratado de la Unión Europea[61]. El Reglamento entró en vigor el año 2016 y comenzó su aplicación en mayo

[57] MAQUEO RAMIREZ, María Solange; MORENO GONZALEZ, Jimena y RECIO GAYO, Miguel. 2017, Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Rev. derecho (Valdivia)*, vol.30, n.1, [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004> [Consulta 9 de septiembre, 2020]

[58] Organisation for Economic Co-operation and Development, 2013, The OECD Privacy Framework p. 14, 15. [En línea] <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [Consulta: 09 septiembre 2020]

[59] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Disponible en línea en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?d1e3109-1-1=&uri=CELEX%3A32016R0679>

[60] El artículo 8 de dicha Carta consagra la protección de datos personales en los siguientes términos: "Artículo 8. Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente". Carta de los Derechos Fundamentales de la Unión Europea. Disponible en línea en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A12012P%2FTXT>

[61] "Artículo 16 (antiguo artículo 286 TCE) 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de

de 2018, a dos años del inicio de su utilización, la Comisión Europea evaluó la norma positivamente y destacó su impacto a nivel internacional[62].

En general, los principios que subyacen al GDPR son los de licitud, lealtad y transparencia, que refieren a que los datos deben tratarse "de forma lícita y transparente, garantizando la lealtad hacia las personas cuyos datos personales se están tratando"[63]; la limitación de la finalidad, según el cual, por un lado, "deben tenerse fines específicos para el tratamiento de los datos e indicarse dichos fines a las personas al recopilar sus datos"[64] y, por el otro, "no se pueden seguir utilizando los datos personales para otros fines que no sean compatibles con la finalidad original de la recopilación"[65]; y, la minimización de datos, que implica que "solo deben recopilarse y tratarse los datos personales que sean necesarios para cumplir esa finalidad"[66].

La normativa incluye también, al principio de exactitud, que implica que "debe garantizarse que los datos personales sean exactos y estén actualizados, en relación con los fines para los que son tratados, y corregirlos en caso contrario"[67]; la limitación en el plazo de conservación, por la que "debe garantizarse que los datos personales no se conserven más tiempo del necesario

carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea." Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea disponibles en línea en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012E&from=EN>

[62] En un Comunicado de la Comisión europea al Parlamento y Consejo europeos, tras dos años de aplicación del Reglamento, se señala que "[t]he adoption of the GDPR has spurred other countries in many regions of the world to consider following suit. This is a truly global trend running from Chile to South Korea, from Brazil to Japan, from Kenya to India, and from California to Indonesia. The EU's leadership on data protection shows it can act as a global standard-setter for the regulation of the digital economy and has been welcomed by important voices of the international community such as UN Secretary General Antonio Guterres who has noted how the GDPR has 'set an example (…) inspiring similar measures elsewhere' and 'urge[d] the EU and its Member States to continue to lead to shape the digital age and to be at the forefront of technological innovation and regulation'". Traducción libre del texto: "la adopción del RGPD ha estimulado a otros países en diversas regiones del mundo a considerar hacer lo mismo. Esta es una verdadera tendencia mundial que va desde Chile a Corea del Sut, de Brasil a Japón, de Kenia a la India y de California a Indonesia. El liderazgo de la UE en protección de datos muestra que puede actuar como un creador de estándares globales para la regulación de la economía digital y ha sido bienvenido por voces importantes en la comunidad internacional, tales como el Secretario General de la ONU, Antonio Guterres, quien ha señalado como el RGDP ha 'establecido un ejemplo (…) inspirando medidas similares en otros lugares' e 'instó a la UE y a sus Estados Miembros a continuar liderando la configuración de la era digital y a estar a la vanguardia de la innovación tecnológica y de la regulación'". El comunicado "Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" está disponible en línea en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264>

[63] Comisión europea, ¿Qué datos podemos tratar y en qué condiciones? [En línea] <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_es> [Consulta: 18 de septiembre, 2020].

[64] Comisión europea, Ibid.

[65] Comisión europea. Op. Cit

[66] Comisión europea. Ibid.

[67] Comisión europea. Ibid.

para los fines para los que fueron recopilados" [68] ; y los principios de integridad y confidencialidad según los cuales "deben establecerse garantías técnicas y organizativas apropiadas que garanticen la seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de la tecnología apropiada"[69].

V. Conclusiones

Se puede concluir de lo revisado anteriormente, que en Chile la protección de datos personales es un derecho fundamental que se relaciona con el sistema de garantía a la privacidad, de modo tal que, a la hora de resolver controversias, no sólo se debe considerar la normativa constitucional y legal nacional, sino también tener en cuenta aquello que está regulado por tratados de derechos humanos y otras normas internacionales que sean vinculantes para los tribunales del país.

Además, si bien existe una ley que regula la protección y tratamiento de los datos personales, esta es criticada, y con razón, por la mayoría de la doctrina y la sociedad civil, porque no constituye garantía eficaz para el resguardo de la información y no cuenta con las herramientas suficientes para enfrentar los desafíos que impone la era digital y el tratamiento masivo de datos personales.

La jurisprudencia nacional, particularmente de los tribunales ordinarios, no es precisamente robusta en el tema y no siempre ha dado respuesta satisfactoria a las controversias relativas a datos personales. Aquello se debe, entre otras razones, a la falta de especialización de los tribunales y las deficiencias en la regulación.

Por eso es importante que la normativa chilena pase por un proceso de actualización, para ello, la modificación de la ley no debe ignorar la experiencia regulatoria de otras latitudes. En ese sentido, el Reglamento europeo ha marcado, sin duda, un camino que debe ser tomado en cuenta, en sus aciertos y errores.

Si bien es importante que haya una modificación legal sustancial que mejore, entre otros aspectos, la regulación del tratamiento de datos por parte de Órganos del Estado sigue siendo fundamental que la normativa actual sea aplicada correctamente, tomando en cuenta las

[68] Comisión europea. Ibid.
[69] Comisión europea. Ibid.

interpretaciones que logren resguardar de mejor forma el derecho fundamental a la protección de los datos personales.

Finalmente, la breve revisión de las diversas normas, doctrina y jurisprudencia hecha en este capítulo funciona como la base teórica desde la cual se analizará el caso de la empresa Entel con la Subsecretaría de Telecomunicaciones en los próximos capítulos del presente trabajo.

Capítulo II: Entel con Subsecretaría de Telecomunicaciones

I. Presentación del caso Entel/Subtel

Esta controversia surge a propósito de dos solicitudes de información que realizó la Subsecretaría de Telecomunicaciones ("Subtel") a las entidades que fiscaliza el año 2018. En la oportunidad, se indicó que la información recopilada sería utilizada para llevar a cabo una encuesta de satisfacción respecto de los servicios ofrecidos por dichas empresas.

Una de las empresas de telecomunicaciones que fue requerida por la Subsecretaría, Entel, se negó a hacer entrega de la información, alegando desde un comienzo que se trataría de datos personales y, por ello, no se encontraría habilitada a hacer entrega de ellos a la autoridad.

Ante la negativa a entregar la información de Entel, la Subsecretaría inició dos procedimientos sancionatorios en su contra, que finalizaron con multas a la empresa. La controversia se judicializó, siendo finalmente conocida por los tribunales superiores.

1. Solicitudes de información

La Subtel realizó dos solicitudes de información el día 16 de mayo de 2018, en ambas se pidió entregar una base de datos que incluyera a la totalidad de los clientes persona natural de las empresas a abril de 2018. Se justificó el requerimiento en el "contexto del análisis de información de mercado que realiza permanentemente, respecto de la satisfacción de los usuarios de los servicios de telecomunicaciones"[70].

La primera solicitud, se efectuó a través del Oficio Circular N°108/DAP N°47.180/F-67, en el que se señala que:

> *"La Subsecretaría de Telecomunicaciones en el contexto del análisis de información de mercado que realiza permanentemente, respecto de la satisfacción de los usuarios de los servicios de telecomunicaciones, requiere contar con datos de contacto de los clientes de servicios móviles al cierre del mes de abril 2018."*[71]

[70] La misma justificación se da tanto en el oficio circular N° 106/DAP N°47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 de mayo de 2018, que solicita base de números telefónicos de clientes de televisión de pago para estudio de satisfacción de usuarios de telecomunicaciones y fija plazo, como en el oficio circular N° 108/DAP N° 47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 mayo 2018, de igual objeto.

[71] Oficio circular N° 108/DAP N° 47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 mayo 2018, que solicita base de números telefónicos de clientes de telefonía móvil para estudio de satisfacción de usuarios de telecomunicaciones y fija plazo.

En este se demandó a las concesionarias del servicio de telefonía móvil[72] que entregaran la siguiente información respecto de la totalidad de sus clientes:

(i) Número telefónico;
(ii) Tipo de plan contratado (pre o post pago);
(iii) Región y comuna del cliente;
(iv) Si registra o no tráfico de datos y/o voz durante los últimos 30 días; y
(v) Si el cliente cuenta con multiservicios.

La segunda solicitud, se realizó por el Oficio Circular N°106/DAP N°47.182/F-67. El documento indica que:

> *"La Subsecretaría de Telecomunicaciones en el contexto del análisis de información de mercado que realiza permanentemente, respecto de la satisfacción de los usuarios de los servicios de telecomunicaciones, requiere contar con los datos de contacto de los clientes de televisión de pago al cierre del mes de abril 2018."*[73]

En este se pidió a las concesionarias del servicio de televisión de pago[74] la remisión de un archivo que contuviera la siguiente información, respecto de la totalidad de sus clientes:

(i) Números telefónicos móviles y/o fijos;
(ii) Región y comuna del suscriptor;
(iii) Tipo de tecnología (satelital o cable); y
(iv) Si el cliente cuenta con multiservicios.

Entel se negó a entregar la información respecto de ambas solicitudes, fue multado por los dos incumplimientos y finalmente esto desembocó en dos procedimientos judiciales diferentes que fueron conocidos en paralelo[75].

[72] Entel PCS Telecomunicaciones S.A., Telefónica Móviles Chile S.A., Claro Chile S.A., Virgin Mobile Chile Spa, Wom S.A.
[73] Oficio circular N° 106/DAP N°47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 de mayo de 2018, que solicita base de números telefónicos de clientes de televisión de pago para estudio de satisfacción de usuarios de telecomunicaciones y fija plazo.
[74] Telefónica Chile S.A., Claro Comunicaciones S.A., VTR Comunicaciones SpA, Entel Telefonía local S.A., DIRECTV Chile Televisión Ltda.
[75] Uno de los procesos corresponde a la solicitud de datos a las empresas sobre el servicio de televisión de pago. Este se conoció en primera instancia por la Ministra de Transportes y Telecomunicaciones con el rol N°10.629-2018, en segunda, ante la Corte de Apelaciones rol N°2095-2019 y fue conocido por la Corte Suprema a través del recurso de queja causa rol n°14.607-2019. El otro procedimiento se conoció en primera instancia con el rol

A continuación, se analizará que pasó después de haberse presentado dichas solicitudes por parte de la autoridad. Para ello, se hará referencia particularmente a la solicitud de información respecto del servicio de televisión de pago, sin perjuicio de que, al ser las solicitudes y las sentencias que arribaron posteriormente prácticamente iguales, las conclusiones pueden ser extendidas a ambas.

2. Sede administrativa

2.1. Procedimiento administrativo sancionador

Tras ser oficiada, la empresa Entel respondió a la Subsecretaría en dos oportunidades. En un primer momento[76], se negaron a entregar los datos, argumentando que la información solicitada por la Subtel correspondía a datos personales, de forma que, su simple entrega violaría la exigencia de consentimiento en el tratamiento de datos de sus clientes.

Posterior a esto[77], Entel hizo entrega parcial de los datos solicitados, enviando a la entidad fiscalizadora únicamente los datos de contacto de sus clientes, de modo que fuera la Subsecretaría la encargada de obtener el consentimiento de los clientes para usar los demás datos en la realización de la encuesta.

A través de dos Ordinarios[78] la Superintendencia acusa el incumplimiento de Entel, por no entregar los datos solicitados. Se formuló el cargo único de

> *"Haber infringido las disposiciones contenidas en la letra K del artículo 6° del Decreto Ley N°1.762 de 1977 y el inciso 2° del artículo 37° de la Ley N°18.168, General de telecomunicaciones, al no cumplir con la obligación de proporcionar en forma íntegra la información requerida mediante oficio"*[79].

N°10.628-2018, en segunda, con rol n°2811-2019 y en la Corte Suprema con el rol N°14609-2019, este versó sobre la solicitud de información por concepto de telefonía móvil.

[76] Presentación de Entel Telefonía Local S.A., de fecha 11 de junio de 2018, Ingreso Subtel N°88674, de fecha 14 de junio de 2018; y su paralela, la Presentación de Entel PCS Telecomunicaciones S.A., de fecha 11 de junio de 2018 Ingreso Subtel N° 88673, de 14 de junio de 2018.

[77] Presentación de Entel Telefonía Local S.A., de fecha 15 de junio de 2018, Ingreso Subtel N°89884, de 15 de junio de 2018; y su paralela, la Presentación de Entel PCS Telecomunicaciones S.A., de fecha 15 de junio de 2018, Ingreso Subtel N° 89883, de 18 de junio de 2018.

[78] El Ordinario N° 10629/DJ-3 N° 244, de la Subsecretaría de Telecomunicaciones, de 25 de junio de 2018, que formula cargo e imparte instrucciones bajo apercibimiento legal, respecto del incumplimiento a lo requerido para telefonía móvil y el ordinario N° 10628/DJ-3 N° 244, para la solicitud de televisión.

[79] Ord. N° 10629/DJ-3 N°245 de la Subsecretaría de Telecomunicaciones, de 25 de junio de 2018, que formula cargo e imparte instrucciones bajo apercibimiento legal.

Además, en dos Informes Técnicos [80] se fundamentaron las facultades del organismo fiscalizador para realizar la solicitud de datos en los artículos 6 y 7 Decreto Ley 1.762 de 1982. Estos artículos establecen, específicamente:

> *Artículo 6°. - El Ministerio de Transportes y Telecomunicaciones tendrá las siguientes funciones y atribuciones en materia de telecomunicaciones, las que ejercerá a través de la correspondiente Subsecretaría:*
>
> *a) Proponer las políticas de telecomunicaciones;*
>
> *b) Participar en la planificación nacional y regional de desarrollo de las telecomunicaciones;*
>
> *c) Velar por el cumplimiento de las leyes, reglamentos, normas técnicas y demás disposiciones internas, como, igualmente, de los tratados, convenios y acuerdos internacionales sobre telecomunicaciones vigentes en Chile y de las políticas nacionales de telecomunicaciones aprobadas por el Supremo Gobierno;*
>
> *d) Elaborar y mantener actualizados los planes fundamentales de telecomunicaciones;*
>
> *e) Aplicar el presente decreto ley, sus reglamentos y normas complementarias;*
>
> *f) Administrar y controlar el espectro radioeléctrico;*
>
> *g) Dictar las normas técnicas sobre telecomunicaciones y controlar su cumplimiento;*
>
> *h) Representar al país, como Administración Chilena de Telecomunicaciones, ante la Unión Internacional de Telecomunicaciones y en la suscripción de los acuerdos sobre telecomunicaciones con otros Estados, sin perjuicio de las facultades del Ministerio de Relaciones Exteriores;*

[80] Informe Técnico N° 26655/F-67, de fecha 18 de junio de 2018, emanado de la División de Fiscalización de la Subsecretaría de Telecomunicaciones, respecto de la solicitud por telefonía móvil e Informe Técnico N° 26658/F-67, de fecha 18 de junio de 2018, emanado de la División de Fiscalización de la Subsecretaría de Telecomunicaciones.

i) Informar y pronunciarse, según corresponda, acerca de las solicitudes de concesión y permisos de telecomunicaciones, su otorgamiento, denegación, suspensión, caducidad y término con arreglo a la ley;

j) Coordinar con el Ministerio de Defensa Nacional y demás organismos y entidades competentes la dictación de las normas destinadas a controlar el ingreso al país de material y equipo de telecomunicaciones, como asimismo las relativas a su fabricación y uso;

k) Requerir de las entidades que operen en el ámbito de las telecomunicaciones y de cualquier organismo público los antecedentes e informaciones necesarios para el desempeño de su cometido, los que estarán obligados a proporcionarlos, y

l) Aplicar las sanciones administrativas que establece la Ley General de Telecomunicaciones.

Artículo 7°- El Subsecretario de Telecomunicaciones es la autoridad competente para conocer y resolver acerca de las materias de carácter técnico relativas a las telecomunicaciones.

En el ejercicio de estas facultades el Subsecretario podrá adoptar todas las medidas que sean necesarias y aplicar las sanciones, administrativas que se establezcan en la legislación respectiva.[81]

Como se puede ver, las disposiciones citadas son las que facultan, de forma general, a la Subsecretaría y establecen que es la autoridad competente para conocer y resolver las materias de carácter técnico relativas a telecomunicaciones, pudiendo adoptar las medidas necesarias a su efecto y sancionar si aquello corresponde, pero en ningún punto hacen referencia a sus facultades para realizar estudios de satisfacción o hacer tratamiento de datos.

2.2. Impugnación ante el Ministerio de Transportes

Entel formuló sus descargos al Ministerio de Transportes y Telecomunicaciones, impugnando el cargo que se le imputó. En esta instancia la empresa insistió en que los datos solicitados

[81] Artículos 6 y 7 del DL 1762, de 1977, que crea la Subsecretaría de Telecomunicaciones dependiente del Ministerio de Transportes y organiza la dirección superior de las telecomunicaciones del país.

por la Subsecretaría eran aquellos de carácter personal, por lo que se encontraba impedida de entregarlos, dadas las restricciones impuestas por la ley N° 19.628.

Resolviendo la impugnación, la Ministra de Transportes y Telecomunicaciones dictó una Resolución[82] en la que se hace cargo de la alegación de Entel, en el sentido de que el fiscalizador habría solicitado datos personales. Al respecto, se señala que "en relación a las a las alegaciones planteadas por Entel, debe tenerse presente que la Subsecretaría de Telecomunicaciones, sólo ha requerido información sobre una base de número telefónicos -con el objeto de generar estadísticas-, en tal sentido, la autoridad no ha solicitado nombres, apellidos y otros datos que identifiquen o permitan identificar al usuario"[83].

La sentencia procede a explicar la diferenciación que se hace en la ley entre los datos personales y los datos sensibles, señalando que, los últimos "comprenden un tratamiento más riguroso y estricto"[84], agregando que el número de teléfono no constituye dato sensible.

Se señala también que "en el formato que han sido requeridos estos datos tampoco permitirán identificar a los usuarios, ni será información entregada a terceros, pues sólo se trata de información necesaria para el cumplimiento de las funciones propias de la autoridad sectorial, con el objeto de efectuar estadísticas que permitan comparar la calidad de los servicios de telecomunicaciones entregada a los usuarios y medir la satisfacción de éstos respecto al servicio recibido, favoreciendo la toma de decisiones que promuevan la competencia, y que asimismo, resguarden los derechos de los consumidores"[85].

Además, se dice que "corresponde especialmente destacar que conforme lo establece el artículo 20° de la Ley 19.628, los órganos del Estado, como la Subsecretaría de Telecomunicaciones, se encuentran facultados para requerir información sobre datos personales cuando se trate de aquellas materias que se encuentran contenidas dentro de sus competencias, no siendo necesario el consentimiento del titular para ello"[86]. En el mismo sentido se declara que "cuando un órgano de la administración del Estado exige información a una entidad, en el ejercicio de sus facultades legales conforme a lo dispuesto en los artículos 6° y 7° de la Constitución Política de la República, no es posible que el requerido pueda

[82] Resolución de la Ministra de Transportes y Telecomunicaciones, de 24 de septiembre de 2018, en autos Rol N° 10.629-2018.
[83] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 4
[84] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 4
[85] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 4
[86] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 5

negarse a tal solicitud, salvo que la Ley contemple norma expresa al respecto, situación que en la especie no ha ocurrido"[87].

También se pronuncian respecto la reserva de la información recibida, señalando que "aún frente a la improbable hipótesis planteada por Entel, en cuanto a que estaríamos frente a datos de carácter personal, (…) es del caso señalar que no es posible divulgar la información en razón del cumplimiento al deber de reserva"[88].

En definitiva, la Ministra consideró que, la información solicitada no constituye dato personal por no ser relativa a un titular identificable y que, aún si lo fuera, la Subsecretaría de Telecomunicaciones tenía facultades para solicitarla. Por ello, se resolvió:

> *"1.- Sancionar a ENTEL TELEFONÍA LOCAL S.A., ya individualizada, en su calidad de reincidente, con el pago de una multa a beneficio fiscal ascendente a la cantidad de 900 (novecientas) Unidades Tributarias Mensuales, en su equivalente en moneda de curso legal, por haber infringido las disposiciones contenidas en la letra K del artículo 6° del Decreto Ley N°1.762 de 1977 y el inciso 2° del artículo 37° de la Ley, al no cumplir con la obligación de proporcionar en forma exacta, íntegra y oportuna la información que le fuera requerida por la Subsecretaría, mediante el oficio Circular N° 106/DAP N° 47.182/F-67, de fecha 16 de mayo de 2018.*
>
> *2.- Sancionar, además, a la afectada, de conformidad con lo dispuesto en el artículo 38° de la Ley, bajo cuyo apercibimiento fuera expresamente conminada en el oficio de cargo de fojas 12 y siguiente, con el pago de una multa a beneficio fiscal ascendente a 0,25 (cero como veinticinco) Unidad Tributaria Mensual, en su equivalente en moneda de curso legal, por cada día que la afectada haya dejado transcurrir sin dar cumplimiento a la orden que le fuere impuesta en el aludido oficio."*[89]

[87] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 5
[88] Resolución de la Ministra de Transportes y Telecomunicaciones. Op. Cit. p. 6
[89] Resolución de la Ministra de Transportes y Telecomunicaciones. Ibid. p. 10

3. Corte de Apelaciones

3.1. Recurso de Entel

La sentencia anteriormente descrita fue objeto de recurso de una reclamación de ilegalidad, que fue conocido por la Octava Sala de la Corte de Apelaciones de Santiago, con el rol N°2059-2019.

En su recurso, la empresa Entel vuelve a alegar que la información requerida constituiría dato de carácter personal. Se señala que, el negarse a entregar la información fue una conducta justificada, por lo que no se trataría de una conducta típica, no correspondiendo imponer la multa. En ese sentido, agregan que, la Subtel no tiene atribuciones para requerir información de toda la base de datos de suscriptores para hacer una encuesta, siendo improcedente la aplicación del artículo 20 de la Ley sobre Protección de la Vida Privada.

En subsidio, la concesionaria solicita la rebaja de la multa impuesta. Funda aquello en que la multa excede el límite legal, que se vulneró el principio de proporcionalidad, y que la reincidencia imputada no era efectiva. Además, alegan la improcedencia de la multa diaria, señalando que, esta infringiría el principio *non bis in ídem.*

3.2. Sentencia de la Corte de Apelaciones

En esta instancia, la sentencia estableció:

> *"Que la imposición de la multa a que se refiere la norma anterior viola el principio non bis in ídem, aplicable también a las sanciones de tipo administrativo, pues si lo que motivó la sanción impuesta a Entel Telefonía Local S.A. fue un hecho determinado -no entregar a la autoridad la información requerida por la Subsecretaría de Telecomunicaciones-, parece evidente que atenta contra el referido principio considerar como una infracción distinta cada día que el infractor dejó transcurrir sin entregar dicha información. Obviamente, dicho incumplimiento motiva la sanción pecuniaria principal y multar, además, por la cantidad de días que ello sucede, es aplicar dos veces una sanción por el mismo hecho.*
>
> *Que, en cuanto al quantum de la multa principal, entendiendo que los datos solicitados obedecen a la necesidad de la autoridad de hacer una suerte de encuesta a través de un tercero, una empresa privada -Cadem-, lo que no dice relación al menos directamente con ninguna de las atribuciones del ente*

fiscalizador que el artículo 6° D.L. 1.762 le entrega, la sanción pecuniaria debe ser reducida sustancialmente. En efecto, sólo muy indirectamente podría sustentarse que la función de proposición de políticas públicas en materia de telecomunicaciones que la letra a) de la señalada norma entrega a la Administración, requiere que se recaben datos de los clientes de la empresa sancionada para que una empresa privada, un tercero, haga una 'encuesta de satisfacción'"[90].

De esta forma, la Corte revoca la sentencia dictada por la Ministra de Transportes y Telecomunicaciones, en cuanto impone una multa de 0,25 UTM por cada día de incumplimiento. En lo demás, se confirma la sentencia, declarando que reduce la multa impuesta a solo 5 UTM.

La sentencia de apelación se acordó en la confirmatoria con un voto en contra. En la argumentación de su voto, el Ministro, que estuvo por absolver de todo cargo a la empresa, sostiene que el artículo 6° del D.L. 1.762 no incluye norma alguna en que "se señale que es función de la autoridad la de escudriñar la 'satisfacción de los usuarios de servicios de telecomunicaciones'"[91], en el mismo sentido afirma que "no parece que una 'encuesta de satisfacción' sea menester para proponer tales políticas públicas, que se deben basar en antecedentes técnicos del área en cuestión"[92].

Resulta evidente que la Corte de Apelaciones, en su sentencia, jamás se pronunció sobre la problemática de datos personales planteada por Entel en su recurso; problemática que fue discutida en la primera instancia y respecto de la cual el tribunal formado por la Ministra de Transportes resolvió. No es claro porqué el tribunal no se pronunció a este respecto.

Lo anterior es problemático, sobre todo considerando que parte de la argumentación de la sentencia era útil para leer la controversia desde la perspectiva de la protección de los datos personales. En ese sentido, es fundamental tener presente, para el análisis con el que se continuará en el presente trabajo, que la Corte de Apelaciones de Santiago reconoce, por un lado, que los datos serían entregados a un tercero, la empresa privada Cadem y, por el otro, que la solicitud no tiene relación directa con las atribuciones que tiene la Subsecretaría.

[90] Sentencia de Corte de Apelaciones, de 27 de mayo de 2019, en Causa Rol N°2095-2019, p. 1.
[91] Sentencia de Corte de Apelaciones. Ibid. p. 2.
[92] Sentencia de Corte de Apelaciones. Ibid. p. 2.

4. Corte Suprema

4.1. Recurso de Subtel

La Subsecretaría interpuso un recurso de queja contra los Ministros que dictaron la sentencia anteriormente revisada, aquello porque los jueces habrían incurrido en graves faltas y abusos en la dictación de su fallo. Dicho recurso fue conocido por la Corte Suprema con el rol N°14.607-2019.

Se argumentó que el razonamiento de los jueces es errado, tanto en la parte en que señalan que la multa diaria transgrede el principio *non bis in ídem* administrativo, como en aquella en que determinan que la Subtel no tendría, al menos directamente, las facultades para solicitar la información que requirió a Entel para realizar una encuesta de satisfacción.

Respecto de la supuesta transgresión al principio de *non bis in ídem* administrativo al imponer la multa diaria, la Subsecretaría señala que los jueces recurridos fallaron uno de los asuntos en contravención formal a la ley. Sobre la disminución de la multa, dicen que esta no tuvo relación con la gravedad del incumplimiento y que aquello, da cuenta de un grave cercenamiento a las potestades sancionatorias de la autoridad.

4.2. Sentencia de la Corte Suprema

La Corte Suprema desechó el recurso de queja interpuesto por la Subsecretaría de Telecomunicaciones. Al respecto, señalaron:

> *"Que los abusos denunciados por la vía del recurso de queja se reconducen, en su mayoría a una cuestión de interpretación acerca de la sanción especial contemplada en el artículo 38 de la Ley N°18.168 y de la facultad de los jueces de determinar la multa en su rango legal.*
>
> *En consecuencia, en el presente caso, el mérito de los antecedentes no permite concluir que los jueces recurridos, al decidir como lo hicieron, hayan realizado alguna de las conductas que la ley reprueba y que sería necesario reprimir y enmendar mediante el ejercicio de las atribuciones disciplinarias de esta Corte, toda vez que resolvieron en el sentido expresado en lo dispositivo, haciendo uso de su facultad de interpretar las disposiciones legales atinentes al caso"*[93].

[93] Sentencia de Corte Suprema, de fecha doce de noviembre de 2019, en Causa Rol N°14607-2019. p. 8.

Sin perjuicio de lo anterior, la Corte actuó de oficio y así, sobre la sanción cuyo quantum fue reducido, el máximo tribunal señaló que la sentencia impugnada "no cuestionó la existencia de la infracción normativa que motivó la sanción pecuniaria, ni la procedencia de ésta"[94], que, legalmente, la multa impuesta por la Subtel estaba dentro del rango legal, que "los sentenciadores no tuvieron por configurada ilegalidad alguna sobre la infracción, ni sobre la procedencia de la multa ni sobre el monto de la multa impuesta, sino que más bien, orientaron sus motivaciones en restarle gravedad e importancia a la conducta infraccional"[95]. Estiman, en definitiva, que "al tribunal sólo le cabe examinar la eventual concurrencia de las infracciones, sin que le esté permitido efectuar consideraciones mérito en torno a los extremos de la sanción aplicada por la autoridad administrativa, salvo que se infrinja el principio de proporcionalidad"[96].

Sobre la multa diaria, la Corte argumenta que, mientras el fundamento de su interposición está cuestionado, su cobro atentaría contra las garantías del debido proceso. Por ello establecen que "la única forma de evitar tal efecto pernicioso, que trae como consecuencia la administración de una sanción pecuniaria con efecto retroactivo, es considerar que su cálculo se encuentra suspendido por el tiempo que dura la tramitación ante la Corte de Apelaciones"[97].

Por las consideraciones anteriores, la Corte Suprema determina que:

> *"[D]eja sin efecto de oficio la sentencia dictada por la Corte de Apelaciones de Santiago el 27 de mayo recién pasado, dictada en los autos tenidos a la vista, ingreso de esa Corte N° 2095-2019 y, en su lugar, se dispone que ambas sanciones contenidas en la decisión de 24 de septiembre de 2018, emitida por la Ministra de Transportes y Telecomunicaciones se confirman con declaración que el cómputo de la multa diaria de 0,25 Unidades Tributarias Mensuales impuesta por cada día que la empresa Entel Telefonía Local S.A. haya dejado transcurrir sin dar cumplimiento a la orden impuesta por la Subsecretaría de Telecomunicaciones, sólo podrá iniciarse una vez que el fallo que la establece, de manera definitiva, se encuentre notificado."*[98- 99].

[94] Sentencia de Corte Suprema. Ibid. p. 9.
[95] Sentencia de Corte Suprema. Op. Cit. p. 10.
[96] Sentencia de Corte Suprema. Ibid. p. 11
[97] Sentencia de Corte Suprema. Ibid. p. 15.
[98] Sentencia Corte Suprema. Ibid.
[99] Cabe notar que la decisión de actuar de oficio respecto de la reducción de la multa principal se acordó con el voto en contra del Ministro Sr. Fuentes, quien fue del parecer de no ejercer la facultad. Por su parte, la decisión de

II. Comentario a las sentencias

Es posible notar que, el abordar esta controversia a partir de las sentencias que fueron dictadas no será útil para transparentar el conflicto de protección de datos personales que existe en el caso. Aquello porque, de las sentencias dictadas, únicamente la de la Ministra de Transportes y Comunicaciones se hace cargo de las argumentaciones de Entel, que se defiende señalando que entregar los antecedentes requeridos por la Subsecretaría implicaría violar la normativa contenida en la Ley N°19.628.

El reconocer que la primera instancia fue la única que abordó el conflicto desde la perspectiva de la protección de datos personales, no implica que estemos de acuerdo con los criterios utilizados por el tribunal. Esto porque, según se abordará en el próximo capítulo, hay buenos argumentos para sostener, por un lado, que la información solicitada si corresponde a datos personales de los clientes de la empresa de telecomunicaciones, datos que no se pueden compartir sin el consentimiento de sus titulares y, por el otro, que la Subsecretaría no tiene facultades para requerir a las entidades reguladas tal cantidad de información, menos considerando que los datos serían finalmente tratados por un tercero privado.

Por otro lado, entre las sentencias de la Corte de Apelaciones de Santiago y la Corte Suprema encontramos un común denominador. Ninguna de estas decisiones hace referencia a la protección de datos personales ni su influencia en el caso, aun cuando esta cuestión fue planteada tanto por Entel, como por la Subtel en sus diversas presentaciones y recogida en la sentencia de primera instancia.

La sentencia de la Corte de Apelaciones recoge algunos de los argumentos planteados por Entel, al dictaminar que la realización de una encuesta de satisfacción por parte de la Subsecretaría no puede relacionarse directamente con las facultades que la ley le otorga. Sin embargo, los sentenciadores en ningún momento hacen referencia a cómo dicha falta de facultades por parte del organismo impacta en la aptitud que éste tendría para requerir datos, en los términos de la Ley sobre Protección de la Vida Privada.

Por su parte, la sentencia de la Corte Suprema tampoco se pronuncia sobre la controversia desde el punto de vista de la protección de datos personales. Esto, probablemente, se explica debido al tipo de recurso por el que conoció el caso, en el entendido que el recurso de queja se interpone contra los jueces que dictaron sentencia y se pronuncia exclusivamente respecto

computar la multa diaria desde la notificación de la sentencia definitiva que la establece se acordó contra la opinión del Ministro Suplente Sr. Muñoz Pardo.

de la existencia de graves faltas y abusos en la dictación de un fallo, en los términos que señala el Código Orgánico de Tribunales.

En general, los fallos de los tribunales superiores representan una oportunidad perdida por parte de la judicatura ordinaria de construir una jurisprudencia sólida sobre el derecho fundamental a la protección de datos personales y sobre la manera en que tanto particulares como organismos públicos deben tratar la información que poseen respetando siempre a sus titulares de los datos.

Las referidas decisiones parecen indicar una falta de conocimiento o de interés de parte de los juzgadores para referirse a la aplicación de la regulación de protección de datos personales. Esto es especialmente preocupante si se considera que, a la fecha de la dictación de las sentencias, el derecho a la protección de datos personales ya había sido consagrado como garantía fundamental.

III. Conclusiones

En conclusión, la controversia suscitada entre Entel y Subtel permite hablar de al menos dos cuestiones. En primer lugar, posibilita comentar cómo se comporta la justicia cuando se ve enfrentada a una problemática de datos personales. Como se vio en este capítulo, la actuación de los tribunales superiores del país fue especialmente deficiente, porque no aplicaron la regulación de datos personales vigente, ignorando que en el caso había derechos fundamentales comprometidos, lo que constituye, a lo menos, la pérdida de una oportunidad para generar jurisprudencia en la materia.

En segundo lugar, este litigio nos permite comentar de manera más general cómo aplicar las normas de protección de datos personales en un caso complejo como el presentado. A la vez la controversia, abre la puerta para comentar cómo debiera actuar un órgano de la administración del Estado al solicitar y tratar este tipo de información. Por ser esto de suma importancia para el desarrollo del presente trabajo, es que se abordará de forma pormenorizada en los capítulos siguientes.

Capítulo III: El caso como una controversia de datos personales

I. Sobre la información requerida por Subtel

El primer aspecto que se revisará para determinar cómo aplicar la normativa de datos personales a la controversia entre Entel y Subtel es la información que fue requerida por el fiscalizador, analizando tanto si esos datos pueden ser considerados datos de carácter personal, como si la cantidad de información solicitada se corresponde con la finalidad enunciada por la Subsecretaría.

1. La información requerida constituye dato personal

En el caso, es fundamental determinar si la información requerida por la Subtel puede ser calificada como datos personales, esto es, como relativa a una persona identificada o identificable.

Como se señaló previamente, la Subsecretaría requirió el envío de una base de datos que incluyera, respecto de la totalidad de los clientes persona natural de las empresas de telecomunicaciones, los números telefónicos, la región y comuna de los suscriptores y datos sobre el tipo de servicio contratado. Es posible afirmar que con los datos requeridos se puede construir un perfil socioeconómico de los clientes de la empresa pues, se conoce donde viven y el tipo de servicio que contratan, lo que hace especialmente delicado el tratamiento de la información.

Por otro lado, se debe subrayar que, como no se pidió el nombre de los clientes, se descarta que los datos refieran a personas identificadas, por lo que, para determinar si se debe hacer aplicación de la Ley sobre Protección de la Vida Privada, corresponde verificar si la información se refiere a personas identificables.

La ley N° 19.628 no entrega una definición que permita determinar criterios de identificabilidad de los titulares, cuestión que sí ocurre, por ejemplo, en el Reglamento europeo. Dicho cuerpo normativo señala que “se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización,

un identificador en línea o varios elementos propios de la identidad física fisiológica genética, psíquica, económica, cultural o social de dicha persona"[100].

Agrega dicho Reglamento que "para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física"[101]. De este modo, la norma modera el alcance de aquellos medios útiles para identificar a las personas, al introducir un criterio de razonabilidad. Al respecto señala que "para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos"[102].

Por su parte, la Corte Suprema[103] estableció como estándar para determinar si un titular de datos es identificable el "mínimo esfuerzo de búsqueda"[104], con ese criterio determinó, por ejemplo, que una placa patente es un dato personal. Es posible señalar, que según este estándar un número telefónico también lo es.

El Consejo para la Transparencia, estableció un estándar de proporcionalidad, al señalar que "se entiende para estos efectos por identificable, toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante uno o más elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social, siempre y cuando el esfuerzo de determinación no resulte excesivo o desproporcionado." [105-106]

[100] Artículo 4.1. del Reglamento General de Protección de Datos de la Unión Europea.
[101] Razón 26) del Reglamento General de Protección de Datos de la Unión Europea.
[102] Razón 26), Reglamento General de Protección de Datos de la Unión Europea.
[103] Sentencia Corte Suprema, de 19 de julio de 2018. Causa Rol N° 2479-2018.
[104] Señala la corte que "en el que incluyó la imagen de un vehículo Audi, Placa Patente Única BH LP-99, sin borrar ni distorsionar la parte del cuadro que mostraba dicha placa y permitía, por ende, a cualquier persona que viera el programa identificar con un mínimo esfuerzo de búsqueda quién es el propietario del vehículo y, eventualmente, relacionarlo con el contenido del reportaje".
[105] Resolución exenta N° 304 del Consejo para la Transparencia, de 30 de noviembre de 2020, que aprueba 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 Sustituye texto que indica.
[106] Cabe notar que, en las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado de 31 de agosto de 2011, en el punto sobre la identificabilidad del titular, se enumeraban los siguientes ejemplos: "RUT o RUN, número de cuenta corriente bancaria, domicilio, número telefónico, etc."

Asimismo, el Consejo ha determinado que los números de teléfono son un dato personal. Por ejemplo, ha señalado que "desde el punto de vista de la protección de datos personales, en tanto el número telefónico se encuentre asociado o sea susceptible de asociarse al nombre de una persona natural, dicha información constituye un dato personal, por lo que quienes trabajen en su tratamiento están obligados a guardar secreto sobre los mismos, cuando estos provengan o hayan sido recolectados de fuente no accesibles al público"[107].

De lo anterior se colige que, pese a no haber una definición legal de persona identificable, si hay criterios adoptados en el ámbito nacional que permiten delimitar dicho concepto. Por ello, es complejo aceptar que, en su resolución, la Ministra de Transportes y Telecomunicaciones señale que "debe tenerse presente que la Subsecretaría de Telecomunicaciones, sólo ha requerido información sobre una base de número telefónicos -con el objeto de generar estadísticas-, en tal sentido, la autoridad no ha solicitado nombres, apellidos y otros datos que identifiquen o permitan identificar al usuario"[108].

Esto porque, por un lado, "cabe recordar que la definición de dato personal abarca mucho más que el nombre o el apellido de una persona -como parece defender la autoridad en los cargos que formula a la empresa-, y se extienden a cualquier información concerniente a personas identificadas o identificables"[109] y, por otro, "la base de datos solicitada por la autoridad permitiría a ésta -o al tercero al que se le encomendará la realización de la encuesta de satisfacción- la identidad de quienes son titulares de los números informados a través de un simple llamado, además de poder perfilarlos por nivel socioeconómico, mediante análisis de sus gastos y comuna de residencia, así como obtener información de sus hábitos a través de la utilización de servicios, todo lo cual califica como dato personal conforme a la definición de la ley"[110].

En definitiva, es posible afirmar, contra lo señalado en la resolución de la Ministra de Transportes y Telecomunicaciones, que la información solicitada correspondía a datos personales porque los titulares de esos datos eran identificables, pues era posible relacionar a cada titular con su información a través de los números telefónicos, a través de un simple llamado, que funciona, razonablemente como medio para identificar a una persona física.

---

[107] Sentencia del Consejo para la Transparencia de fecha 26 de octubre de 2010, en la causa Rol N° C-611-2010.
[108] Resolución de la Ministra de Transporte. Op. Cit. p. 4.
[109] CANALES, María Paz, en Derechos Digitales. 2019. ¿Quién defiende tus datos? La problemática acción de Subtel. [En línea] <https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/> [Consulta: 6 de octubre 2020]
[110] CANALES, María Paz, en Derechos digitales. Ibid.

Por lo anterior, se puede señalar que el requerimiento de la Subsecretaría de Telecomunicaciones recaía en parte en datos personales, por lo que debía tenerse en consideración la regulación de la protección de dicha información para proceder a su tratamiento.

2. Deberes de Entel respecto de la información

Al determinar que los números de teléfono son un dato personal y que, por lo tanto, parte de la información que requería la Subtel está sujeta a protección legal especial, debemos determinar cuáles son los deberes específicos de la empresa respecto de dichos datos.

2.1. Principio de finalidad y consentimiento del titular de datos

Lo primero es señalar que Entel debe regirse por el principio de finalidad en el tratamiento de la información de sus usuarios, esto quiere decir que el tratamiento de los datos sólo podrá ocurrir respecto de los objetivos para los cuales hubieren sido recolectados.

Las finalidades que reconoce la empresa para el tratamiento de los datos están contenidas en su política de privacidad de clientes. En ella declara que utilizarán datos personales "en aquellos casos que su tratamiento sea necesario para la ejecución del contrato, para el cumplimiento de los fines para los cuáles hemos solicitado tu consentimiento o para el cumplimiento de obligaciones legales"[111]. Agregan que, usan los datos para la celebración del contrato y el cumplimiento de sus obligaciones, para la mejora y monitoreo de sus servicios y para el envío de comunicaciones comerciales[112].

En definitiva, de acuerdo con la normativa chilena, el respeto al principio de finalidad implica que Entel no podría entregar simplemente los datos en cuestión a terceros y se requiere, en cambio, que medie el consentimiento de los titulares de la información, o bien, que exista alguna autorización legal.

Como lo señala la ley, en caso de existir alguna otra autorización legal, la empresa podría proceder a la entrega de los datos. Así lo reconoce la concesionaria de telecomunicaciones en su política de privacidad actualizada, en la cual explicitan que "en cumplimiento de obligaciones legales, nos podremos ver obligados a comunicar tus datos ante requerimientos

[111] Entel. 2019. Política de Privacidad Clientes Entel. [En línea] <https://www.entel.cl/legales/pdf/Pol%C3%ADtica-de-Privacidad-Clientes-Entel.pdf> [Consulta: 10 de octubre de 2020] p.1.
[112] Entel. Ibid. p.2.

judiciales y de la administración del Estado, sin que sea necesario para ello contar con consentimiento expreso"[113].

Una de las situaciones en las que la comunicación de datos sería procedente corresponde a las solicitudes de información por parte de órganos del Estado, en cumplimiento de sus funciones. Se analizará en los apartados siguientes si el requerimiento de la Subsecretaría cumplía con los estándares legales para configurarse como causal para el envío de los datos sin el consentimiento de sus titulares.

2.2. Sanciones por incumplimiento

Si aceptamos que los datos requeridos a Entel son datos personales, la empresa estaba obligada a usar los datos únicamente para los fines que los recolectó, a menos que mediara algún otro tipo de autorización legal que le permitiera comunicarlos. En el caso, la empresa consideró que la solicitud de la Subsecretaría no constituía razón suficiente para el envío de los datos, por las razones que ya fueron revisadas.

Considerando lo anterior, si Entel hubiese tomado la decisión de enviar los datos a la Subsecretaría, dicha acción constituiría un incumplimiento a la normativa de la ley N° 19.628. Tal incumplimiento exponía a la empresa de telecomunicaciones, a las multas contenidas a propósito de la acción de *habeas data,* en el caso, una sanción de, a lo sumo, cincuenta unidades tributarias mensuales[114].

Por otro lado, las sanciones a las que se exponía la empresa por no atender un requerimiento de este tipo por parte de su entidad fiscalizadora ascienden hasta mil unidades tributarias mensuales, a las que se pueden añadir multas especiales. Como se revisó antes, en este caso ocurrió que se impuso una multa por 900 UTM más una multa diaria especial por cada día de incumplimiento.

En general, es claro que los incentivos para respetar la normativa referida a protección de datos personales son bajos. En un caso complejo como este, la situación es aún más patente. Las empresas reguladas están en una posición, en que, por estrategia económica, es más razonable hacer entrega de la información que requiera la administración, para no arriesgar

[113] Entel. Ibid. p.1.
[114] De acuerdo con la norma de los incisos finales del artículo 16 de la Ley N° 19.628 sobre Protección de la Vida Privada.

ser objeto de las altas multas sectoriales, aún si aquello implica desconocer los derechos de sus clientes.

Por lo anterior, se entiende por qué "varias de las empresas concesionarias si bien cuestionaron la solicitud, atendieron al requerimiento de la autoridad bajo el temor de resultar multadas de no hacerlo"[115].

II. Tratamiento de datos por la Subsecretaría

Establecer que la Subsecretaría de Telecomunicaciones a través de sus oficios requirió el envío de datos personales de los clientes de las empresas sometidas a su control no basta para definir que la actuación de la administración fue ilegal y, por lo tanto, que la negativa de Entel a entregar la información se justificaba.

1. Facultades de Subtel

Como está definido en la Ley sobre Protección de la Vida Privada, los órganos de la administración pueden requerir datos personales sin el consentimiento del titular, sólo en la medida que sea respecto de las materias de su competencia y sujetándose a la normativa de la Ley 19.628.

Por ello, es fundamental determinar si las facultades que la ley confiere a la Subsecretaría de Telecomunicaciones tienen alguna relación con la finalidad perseguida a través del requerimiento de información, esto es, la confección de una encuesta de satisfacción con el servicio ofrecido por las empresas de telecomunicaciones que regula.

La Subtel tiene "como principales funciones proponer las políticas nacionales en materias de telecomunicaciones, de acuerdo a las directrices del Gobierno, ejercer la dirección y control de su puesta en práctica, supervisar a las empresas públicas y privadas del sector en el país, controlando el cumplimiento de las leyes, reglamentos y normas pertinentes"[116].

La Subsecretaría fundamenta sus facultades para realizar la encuesta de satisfacción en las disposiciones legales que indican que el organismo debe "proponer las políticas de telecomunicaciones" [117] y que "además le corresponderá controlar y supervigilar el funcionamiento de los servicios públicos de telecomunicaciones y la protección de los

[115] CANALES, María Paz, en Derechos digitales. Op. Cit.
[116] Subtel. Quienes Somos. [En línea] <https://www.subtel.gob.cl/quienes-somos/> [Consulta: 11 de octubre de 2020].
[117] Artículo 6° a), del Derecho Ley N° 1762 de 1977, que crea la Subsecretaría de Telecomunicaciones dependientes del Ministerio de Transportes y organiza la dirección superior de las telecomunicaciones del país.

derechos del usuario"[118]. De este modo, entienden que la información recolectada en la encuesta permitiría orientar nuevas políticas sectoriales y comunicar a los consumidores la calidad de los servicios que puedan contratar.

Sin negar en caso alguno que la Subtel tiene facultades para proponer políticas de telecomunicaciones, es a lo menos dudoso que dicha norma alcance a cubrir la realización de encuestas a los usuarios sobre la calidad del servicio que reciben. Esto porque, por ejemplo, otros órganos de la administración que realizan estudios y encuestas en este sentido tienen dichas potestades expresamente consagradas en sus respectivas leyes

Caso paradigmático es el del Servicio Nacional del Consumidor ("Sernac"), organismo que tiene facultades para realizar y promover estudios e investigaciones en el área del consumo[119]. Este órgano de la administración mantiene el monitoreo de los diversos mercados, incluido el de telecomunicaciones y, de hecho, trabaja junto a la Subsecretaría en el procesamiento de reclamos de los consumidores y la promoción de sus derechos en la materia. Por lo anterior, es razonable esperar la realización de una encuesta de satisfacción con el servicio por parte de Sernac y no por la Subtel.

Así, es posible determinar que, una relación, a lo sumo indirecta, entre la facultad de proponer políticas públicas en telecomunicaciones y la realización de una encuesta de satisfacción no es suficiente para alcanzar el estándar establecido en el artículo 20 de la Ley 19.628. En una lectura de dicho artículo considerando la normativa constitucional y de la ley de bases de la administración del Estado sobre el principio de legalidad, se vuelve más claro que una atribución que le permita a la Subsecretaría realizar encuestas y estudios debería estar delimitada de mejor manera.

Por otro lado, la constatación de que la Subsecretaría no efectuó el tratamiento de datos dentro de las materias de su competencia no implica que la encuesta no podía llevarse a cabo, por cuanto la ley establece que el cumplimiento de dicha condición permite un tratamiento sin el consentimiento del titular, dejando a salvo la posibilidad de que el órgano público obtenga la autorización de los titulares de datos para poder alcanzar sus objetivos.

[118] Artículo 7 inciso final de la Ley N° 18.168 General de Telecomunicaciones.
[119] Artículo 58 letras d) y k) de la Ley N° 19.496 que establece normas sobre protección de los derechos de los consumidores.

2. Aplicación de la normativa de datos personales

Aun si se considerara que la Subsecretaría tenía las facultades para realizar tratamiento de los datos solicitados a las empresas de telecomunicaciones, el organismo debe cumplir con la normativa de la Ley sobre Protección de la Vida Privada.

2.1. La cantidad de información solicitada fue desproporcionada.

Los órganos de la administración deben atender, en primer lugar, al principio de proporcionalidad que "implica que sólo pueden recabarse aquellos datos que sean necesarios para conseguir los fines que justifican su recolección"[120] y debe optarse, por tanto, por las vías que menos afecten la garantía a la protección de los datos personales.

La solicitud de información hecha por la Subsecretaría infringe al principio de proporcionalidad de dos formas. Primero, porque se requiere la totalidad de las bases de datos de las empresas de telecomunicaciones, siendo que, "la encuesta de satisfacción no se realizará a la totalidad de la base sino sólo a una muestra"[121]. Solicitar sólo una parte de las bases de datos hubiese sido optar por un tratamiento que garantice de mejor manera los derechos de los titulares.

En segundo lugar, la proporcionalidad en el tratamiento de los datos también se ve afectada por la entidad de la información requerida, porque, como se dijo, esta permite construir un perfil socioeconómico de los clientes de las empresas de telecomunicaciones. Aquello no es necesario para la realización de la encuesta de satisfacción, lo que representa, por tanto, un riesgo excesivo el derecho a la protección de los datos personales.

2.2. Seguridad de los datos

Sumado a lo anterior, la Subsecretaría tampoco respeta el principio de seguridad en el tratamiento de la información, que ha sido reconocido en diversos cuerpos normativos internacionales. El oficio por el cual requiere los datos no provee "certeza de ningún tipo de las medidas técnico-administrativas que se adoptarán para la seguridad de tales datos"[122].

Esto es especialmente gravoso considerando que los datos solicitados a las concesionarias de telecomunicaciones podrían verse expuestos a amenazas de ciberseguridad externas[123],

---

[120] Consejo para la Transparencia, Unidad Normativa, 2011. Protección de Datos Personales: Jurisprudencia relevante del Consejo para la Transparencia en relación a la Protección de Datos Personales. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/proteccion_de_datos_web.pdf> [Consulta: 10 de octubre 2020] p. 50.

[121] CANALES, María Paz, en Derechos digitales. Op. Cit.

[122] CANALES, María Paz, en Derechos digitales. Ibid.

[123] Como se ha visto el último tiempo, la ciberseguridad de las instituciones chilenas se ha visto amenazada. Para poner el asunto en perspectiva, sólo durante el año 2020, se ha conocido de dos ciberataques, el primero, contra

pero también podrían ser indebidamente comunicados por una mala aplicación de la ley de transparencia.

En definitiva, la entrega de la información requerida a la Subsecretaría implicaba exponerla a una serie de riesgos sin que se explicitara cómo serían mitigados. En ese sentido, se debe recordar que "no compete a las empresas concesionarias asumir frente a sus clientes que les han confiado sus datos personales en el marco de una relación contractual el riesgo sobre una eventual falta de reserva de la autoridad en la custodia de los datos, es la autoridad la que debe acreditar que satisface los requisitos legales para acceder a los datos personales de los usuarios y adoptará las medidas adecuadas para su protección"[124].

III. Entrega de los datos a un tercero

La información solicitada a Entel y las otras empresas del sector, fue requerida para hacer una encuesta que no sería realizada por la Subsecretaría, sino que, por un tercero, en este caso y, al igual que en versiones anteriores, por la empresa CADEM, que se dedica a realizar una diversidad de estudios "incluyendo las encuestas de tendencias políticas y categorización socioeconómica de la población"[125].

La entrega de esta información para que sea tratada por una empresa diferente es altamente problemática. Primero, porque los titulares de los datos no han consentido en su comunicación y, de hecho, este traspaso de información no se les ha comunicado, situación que por sí sola ya constituye a una violación a la garantía de protección de datos personales. Además, porque es posible afirmar que los riesgos de pérdida o robo de datos se ven incrementados al realizarse esta segunda transferencia.

1. Proceso de licitación

A través de un proceso de licitación pública[126] se determinó que sería CADEM la entidad encargada de realizar el sondeo en cuestión, al ser la que resultó mejor evaluada en el ítem

BancoEstado y, posteriormente, contra Gobierno Digital. Este acceso no autorizado al organismo dependiente del Ministerio Secretaría General de la Presidencia afectó "sistemas que operan en ese ministerio que están expuestos hoy día: plataformas completas, sistemas que tratan datos personales, algunas de las partes del Sistema Comisaría Virtual" según indicó Daniel Álvarez, académico de la Universidad de Chile, en entrevista con Chilevisión Noticias. CHV Noticias. Experto dice que el hackeo a página de claves únicas es peor de lo que se sabe públicamente [En línea] <https://www.chvnoticias.cl/nacional/experto-hackeo-pagina-claves-unicas_20201015/> [Consulta: 17 de octubre de 2020]

[124] CANALES, María Paz, en Derechos digitales. Op. Cit.

[125] CANALES, María Paz, en Derechos digitales. Ibid.

[126] Licitación ID: 606-15-LE18

experiencia demostrable del oferente, frente a la unión temporal de proveedores compuesta por Brújula, Investigación y Estrategia y C&M Investigación y Estudios de Mercado Ltda.[127].

En lo relevante, las bases de licitación[128] determinaron las características específicas que debía tener la encuesta de satisfacción a realizarse durante el año 2018. Así, se determinó como objetivo general, primero, "medir cuantitativamente el grado de satisfacción de los usuarios con los servicios de telefonía móvil, Internet móvil, televisión de pago y del servicio de Internet residencial, para cada una de las compañía proveedoras y cuya muestra calculada sea estadísticamente confiable y representativa a nivel nacional y regional, de manera que los datos recolectados permitan obtener conclusiones válidas y generar un proceso de comparación o benchmarking entre las mismas empresas"[129] y, segundo, "disponer de información relativa al grado de conocimiento que tienen los usuarios de servicios de telecomunicaciones respecto de la entrada en operación de la televisión digital en Chile".

Adicionalmente, en las bases técnicas se determinó que el oferente debía "definir y proponer el grupo objetivo de la encuesta, el diseño muestral y la muestra a considerar para la medición, con el margen de error igual o menor al 3,7% y el nivel de confianza de un 95%, (…) a nivel nacional, por empresa y para los servicios de telefonía móvil, televisión de pago, Internet móvil e Internet residencial"[130].

Lo anterior quiere decir que, la Subsecretaría conoció, antes de adjudicar el contrato, la cantidad de encuestas telefónicas que iban a realizar las oferentes. Por eso, la Subtel debió tener en cuenta el tamaño de la muestra propuesta al momento de entregar los datos de contacto de los usuarios de los diversos servicios de telecomunicaciones.

---

[127] Según consta en el Acta de evaluación de las propuestas presentadas a la licitación pública denominada: "Encuesta de satisfacción de usuarios y medición del nivel de calidad de servicios de telecomunicaciones", ID 606-15-LEP18, de 12 de julio de 2018, las oferentes tuvieron idénticos puntajes en los ítems: 1. Oferta Económica, 3. Grado de conocimiento y experiencia comprobable de los integrantes del equipo de trabajo que participarán en la ejecución del servicio requerido (Consultores y Jefe de Proyecto), en el desarrollo de consultorías, proyectos y/o estudios relacionados con el desarrollo de estudios de opinión , se satisfacción y calidad de servicio en materia de telecomunicaciones, en particular en: técnicas de diseño y aplicación de encuestas, determinación de tamaño de muestras, trabajo de campo análisis estadístico de resultados, difusión de resultados, etc. y 4. Descripción del trabajo a realizar, su metodología y plan de trabajo, de acuerdo a lo solicitado en el capítulo I, números 3) y 4) de las Bases Técnicas. Los oferentes sólo se diferenciaron en el punto 2. Experiencia demostrable del oferente en la prestación de servicios de consultoría y/o estudios en proyectos relacionados con la presente licitación.
[128] Resolución Exenta N° 1.079: llamado a licitación pública, aprobación de bases y sus correspondientes anexos, de la Subsecretaría de Telecomunicaciones, del 01 de junio de 2018
[129] Resolución Exenta N° 1.079: llamado a licitación pública, aprobación de bases y sus correspondientes anexos, de la Subsecretaría de Telecomunicaciones, del 01 de junio de 2018. p. 3.
[130] Resolución Exenta N° 1.079: llamado a licitación pública, aprobación de bases y sus correspondientes anexos, de la Subsecretaría de Telecomunicaciones, del 01 de junio de 2018. p. 22.

2. Contrato con CADEM

Según se ha señalado, la regulación chilena vigente no comprende disposiciones que se refieran a la comunicación de datos personales por parte de órganos de la administración, sin perjuicio de ello, dicha comunicación ocurre, porque el Estado externaliza variadas funciones. Es por eso que el contrato que regula la relación entre la Subsecretaría de Telecomunicaciones y CADEM[131] es el principal instrumento que condiciona el traspaso de datos.

A este respecto, el documento establece la manera en que la encuesta debe llevarse a cabo y señala, en general, que "el contratista deberá garantizar la confidencialidad en el manejo de la información relacionada con la asesoría"[132]. Incluye además que "a efectos de dar el debido cumplimiento a lo antes señalado y garantizar los derechos de terceros, el contratista deberá informar a las personas encuestadas del carácter facultativo de las respuestas y el propósito para el cual se está solicitando la información", agregan que "la comunicación de sus resultados debe omitir las señas o datos que puedan permitir la identificación de las personas consultadas (…) de conformidad con las normas contenidas en la Ley N° 19.628"[133]. Así, el contrato establece la forma en que se debe tratar la información obtenida como resultado de la realización del estudio.

El mismo instrumento se refiere a los datos que fueron entregados por la Subsecretaría para hacer el sondeo de forma menos detallada. En este sentido, se indica que "para efectos de la encuesta de estos dos servicios [telefonía e Internet móvil], la Subsecretaría proporcionará la base de datos de numeración telefónica móvil por empresas, sujetas a medición, en medios magnéticos (CD) y de cuya información, el contratista deberá mantener las reservas del caso"[134].

Esta situación no ha mejorado con los años, dado que, para los sucesivos estudios, la Subtel ha seguido contratando con terceros para la realización del estudio. Además, en los contratos suscritos con CADEM, para la realización de la encuesta de satisfacción del año 2019 y con IPSOS, quien realizará la encuesta del año 2020, no hay un avance hacia una mejor protección de la información de los usuarios del servicio de telecomunicaciones.

[131] El contrato fue aprobado por la Resolución Exenta N° 1742, de 22 de agosto de 2018, de la Subsecretaría de Telecomunicaciones, que aprueba contrato con Consultores Asociados de marketing CADEM S.A.
[132] Cláusula 15.a. Contrato entre Subtel y CADEM, suscrito el 10 de agosto de 2018.
[133] Contrato entre Subtel y CADEM, suscrito el 10 de agosto de 2018. Cláusula 15.h.
[134] Contrato entre Subtel y CADEM, suscrito el 10 de agosto de 2018. Cláusula 3. p. 5.

CADEM, o cualquier otra empresa que contrate con el Estado para realizar un estudio de este tipo, debe cumplir con la Ley sobre Protección de la Vida Privada. Esto significa que durante todo el período que tenga los datos debe atenerse a los preceptos legales y, una vez finalizada la encuesta, debe desprenderse de la información que recibió para su realización. En ese sentido, se considera necesario que en los contratos exista suficientes incentivos y sanciones fuertes para una correcta observancia de la ley y la normativa constitucional por parte de las empresas que contraten con el Estado.

3. Realización y resultados de la encuesta

El 15 de enero de 2019, la Subsecretaría publicó en su página web que "entregó los resultados del Estudio de Satisfacción de Usuarios de Telecomunicaciones, informe elaborado junto a CADEM y correspondiente al segundo semestre de 2018"[135]. Respecto del informe elaborado, se analizará dos cuestiones, primero, la cantidad de encuestas realizadas, segundo, la utilización de la información cualitativa entregada por la autoridad al privado que realizó la encuesta.

3.1. Encuestados desde una perspectiva cuantitativa

Según el resumen ejecutivo del Ministerio de Transportes, en octubre de 2018, se realizó un total de 14.092 encuestas telefónicas a nivel nacional[136]. La distribución de las encuestas realizadas se detalla en el Informe Final de CADEM, que definió una muestra de 700 casos por compañía y un total de 3.500 encuestas por servicio (Telefonía Móvil, Internet Móvil, Televisión de Pago e Internet Residencial), a partir del requisito de error muestral y nivel de confianza exigido por la Subsecretaría de Telecomunicaciones[137].

Según se adelantó en el apartado sobre el proceso de licitación, para la realización de la encuesta el error muestral debía ser igual o menor a un 3,7% y el nivel de confianza debía ser de un 95%; ambas condiciones fueron determinadas previamente por la Subsecretaría en las Bases de Licitación. El tamaño de la muestra necesaria para cada una de las mediciones fue

[135] Subsecretaría de Telecomunicaciones. MTT entregó resultados de estudio de satisfacción de usuarios en telecomunicaciones: internet fijo es el servicio peor evaluado. [En línea] <https://www.subtel.gob.cl/mtt-entrega-resultados-de-estudio-de-satisfaccion-de-usuarios-de-telecomunicaciones-internet-fijo-es-el-servicio-peor-evaluado/> [Consulta 10 de agosto de 2020]

[136] Ministerio de Transportes y Telecomunicaciones. Resumen Ejecutivo y Plan de Acción Estudio de Satisfacción de Usuarios de Servicios de Telecomunicaciones. 2019. Diapositiva 2 [En línea] <https://www.subtel.gob.cl/wp-content/uploads/2019/01/estudio_sat_diciembre_2018.pdf> [Consulta: 10 de agosto de 2020].

[137] CADEM. 2018. Informe II Resultados Medición 2018. [En línea] <https://www.subtel.gob.cl/wp-content/uploads/2019/05/Informe_II_2018.pdf> [Consulta: 10 de agosto de 2020].

propuesto por la contratista en su Oferta Técnica, a partir de los valores requeridos por la autoridad.

Lo anterior significa que, antes de que se firmara el contrato a través del cual se encargó a CADEM la realización del estudio de satisfacción y, tras el cual, la Subtel hizo entrega de las bases de datos de las empresas de telecomunicaciones que contenían la información de la totalidad de sus clientes persona natural, ya se conocía que se realizarían alrededor de 14.000 encuestas telefónicas.[138-139]

El tamaño muestral, o sea, las 14.000 encuestas, debe ponerse en relación con el tamaño de la población o universo que se pretendía representar en el sondeo. En este caso, respecto del servicio de telefonía móvil, entre clientes con contrato y prepago, el total de usuarios era de 21.593.264; en el servicio de internet móvil, el número de conexiones alcanzaba un total de 15.056.049; por su parte, el servicio de televisión de pago tenía 3.318.512 suscriptores y; el servicio de internet residencial o fija llegaba a un total de 2.789.822 clientes.[140]

En estadística, la muestra corresponde al "subgrupo de elementos de la población seleccionado para participar en el estudio"[141], por su parte, la población es la "suma de todos los elementos que comparten un conjunto común de características y que constituyen el universo para el propósito del problema de la investigación de mercados"[142]. De esta forma, se distingue claramente entre el grupo que será encuestado y el grupo que se pretende representar en el sondeo y como, en ningún caso es necesario ni eficiente, encuestar a la totalidad de la población, por lo que no tiene sentido que la Subsecretaría haya hecho entrega de la totalidad de las bases de datos con la información de los usuarios de telecomunicaciones.

Aquello no significa que debía entregarse una cantidad de información por usuario idéntica al tamaño muestral, porque es claro que para arribar al "tamaño final de la muestra, debe hacerse contacto con un número mayor de encuestados potenciales (…) porque comúnmente las tasas de incidencia y de terminación son menores al 100 por ciento"[143]. La tasa de incidencia corresponde a la "tasa de ocurrencia de personas elegibles para participar en el estudio

[138] Contrato entre Subtel y CADEM, suscrito el 10 de agosto de 2018. p. 2.
[139] Por lo demás, estos números son coherentes con las muestras de las últimas versiones de la encuesta (al menos desde el año 2017), según se extrae de la Gráfica 1. "Muestras reales en mediciones desde 2013" aportado por CADEM en su Informe, en la página 14.
[140] Datos a la fecha de la realización de la encuesta, según consta en el contrato entre CADEM y Subtel, en sus páginas 4, 5 y 6.
[141] Malhotra, Naresh K. Investigación de mercados, Pearson, quinta edición, 2008. p. 335.
[142] Malhotra, Naresh K. Ibid. p. 335.
[143] Malhotra, Naresh K. Ibid. p. 376.

expresada como porcentaje"[144], mientras que, la tasa de terminación es el "porcentaje de los encuestados calificados que concluyen la entrevista"[145].

Para una empresa que se dedica a realizar sondeos como CADEM, es relativamente razonable asumir que, son capaces de determinar el tamaño inicial de la muestra, para arribar a la cantidad deseada de encuestas, sobre todo considerando que, este estudio en particular, ya se había realizado años anteriores. De este modo, se pudo haber precisado con antelación la cantidad de datos sobre los cuales realizar la encuesta, evitando entregar la información de la totalidad de la población.

Así, el que el tamaño de la muestra necesaria para la realización del sondeo correspondiera a un total de 14.000 usuarios y que esta información fuese conocida por la Administración previo a la realización de la encuesta, sumado a que, era posible calcular con relativa exactitud el tamaño de la muestra inicial que se requería para practicar el estudio, nos lleva a afirmar que no se justifica y, por tanto, es contrario al principio de proporcionalidad, que se haya solicitado la información de la totalidad de los usuarios a las empresas de telecomunicaciones y que, posteriormente, estas bases de datos se entregaran sin filtro al tercero CADEM.

La Subsecretaría conocía o, al menos, podía conocer la cantidad de información que se necesitaría para llevar practicar el sondeo y pudo haber ajustado su solicitud, para, de este modo, minimizar el impacto sobre los titulares de derechos. La Subtel incumplió con el principio de proporcionalidad, pasando a llevar la garantía fundamental a la protección de los datos personales.

3.2. Los encuestados desde una perspectiva cualitativa

El requerimiento de información que hizo la Subsecretaría de Telecomunicaciones, no se limitó a pedir números de teléfono de los usuarios, al contrario, se solicitó que se especificara la región y comuna, el tipo de plan o prepago, si el cliente tenía tráfico de datos en un período de tiempo determinado, si contaba con multi servicio y el tipo de tecnología contratada.

Toda esa información es útil para construir una muestra representativa, pero el entregarla a la empresa que realizaría la encuesta representa un riesgo a la protección de los datos personales, porque claramente, dicha información permite realizar un perfilamiento socioeconómico. En un caso como este, era preferible requerir a las empresas que enviaran

[144] Malhotra, Naresh K. Ibid. p. 376.
[145] Malhotra, Naresh K. Ibid. p. 377.

una muestra representativa, lo que hace sentido desde la óptica del principio de proporcionalidad, por cuanto, es preferible utilizar el mínimo óptimo de información para alcanzar el objetivo propuesto al tratar datos personales.

Por otro lado, la información no fue utilizada en la realización de las encuestas telefónicas. Los datos obtenidos en el estudio se entregaron desagregados por género, edad y región del usuario encuestado y, lógicamente, se preguntó sobre esos criterios en los cuestionarios aplicados en las entrevistas[146].

Se ve que, en definitiva, hubo un incumplimiento de variados requisitos de la Ley 19.628 en el requerimiento de información de la Subtel.

IV. La controversia abrió la puerta a una discusión

La controversia iniciada por Entel ha sido revivida durante al año 2020, a propósito de una nueva realización de la encuesta de satisfacción. Además, nuevos cuestionamientos se han realizado respecto de las facultades de tratamiento de datos de la Subsecretaría de Telecomunicaciones, tras la publicación de la norma técnica de la ley de velocidad mínima garantizada de acceso a internet.

Estas acciones muestran cómo el caso ha servido en los hechos para poner atención a las acciones del órgano administrativo en materia de datos personales.

1. Reparos a la realización más reciente de la encuesta

La encuesta de satisfacción sobre el servicio de telecomunicaciones se ha seguido realizando y la versión de 2020 fue adjudicada a la empresa de investigación de mercados Ipsos.

La Subsecretaría ha seguido solicitando a las compañías la información de todos sus clientes[147]. En este contexto, las firmas de telecomunicaciones, reunidas en la Asociación de Empresas de Telecomunicaciones, hicieron presente su disconformidad con el requerimiento, por considerarlo innecesario y peligroso[148].

---

[146] Lo que se puede ver en el Informe Final entregado por CADEM, en las páginas 232 (cuestionario para telefonía móvil), 239 (cuestionario para internet móvil), 247 (cuestionario para Internet fija) y 255 (cuestionario para televisión de pago).

[147] Como se puede ver en las bases de licitación del proceso. Resolución exenta N° 880 de la Subsecretaría de telecomunicaciones, de 28 de mayo de 2020, llamado a licitación pública, aprobación de bases y de sus correspondientes anexos.

[148] Según indicó Alfie Ulloa, presidente de la Asociación de Empresas de Telecomunicaciones (“Atelmo”), en entrevista con el diario El Mercurio, jueves 6 de agosto de 2020. [En línea] <https://www.emol.com/noticias/Economia/2020/08/06/994139/Empresas-telecomunicaciones-Subtel-datos-clientes.html> [Consulta: 9 de agosto de 2020]

2. Reparos a la norma técnica de la ley de velocidad mínima garantizada

Además de los reparos a la realización de la encuesta de satisfacción, las compañías de telecomunicaciones se opusieron a la Norma Técnica de la Ley N° 21.046, que establece la obligación de una velocidad mínima garantizada de acceso a internet[149-150].

Esto se fundamentaría en que la norma, en su artículo 24, establece que se proveerá a la Subsecretaría de "acceso en línea a través de una herramienta de software a todos los repositorios de información, incluyendo datos administrativos, tales como fechas y horas, actividad de los usuarios habilitados, mediciones individuales y de calidad de red", según la norma, la información se entregaría, además, georreferenciada.

Refiriéndose sobre el caso, el entonces presidente del Consejo para la Transparencia, señaló que "sólo muy indirectamente podría sostenerse que solicitar a las empresas este tipo de información personal de sus clientes está relacionado con el cumplimiento de las funciones de la Subtel, precisamente por aplicación de los principios de finalidad y proporcionalidad"[151] agregando que "si uno revisa la jurisprudencia europea, que tiene los más altos estándares en esta materia, encuentra que este tipo de dilemas ya han sido debatidos y zanjados, en el sentido de que no se les permite a las autoridades recabar ese tipo de datos, porque resulta excesivo para sus funciones y podrían formarse conclusiones precisas sobre los hábitos de los clientes, siendo estos un dato sensible incluso en nuestra actual legislación"[152].

V. Conclusiones

A modo de conclusión del capítulo, se señalarán una serie de debilidades a nivel legal; de juzgamiento, tanto en la toma de decisiones por la administración, como por parte de los tribunales de justicia; y, en el comportamiento de los privados involucrados.

Respecto de las debilidades legislativas, se puede ver al menos dos problemas con el diseño regulatorio de la protección de datos. El primero, tiene que ver con la apertura con que la

[149] Resolución Exenta N° 1.251, de 29 de julio de 2020, de la Subsecretaría de Telecomunicaciones, que fija norma técnica de la ley N° 21.046, que establece la obligación de una velocidad mínima garantizada de acceso a internet.
[150] Según se lee en El Mercurio del 6 de agosto de 2020, Atelmo habría recurrido a la Contraloría General de la República, sin éxito. [En línea] <https://www.emol.com/noticias/Economia/2020/08/06/994139/Empresas-telecomunicaciones-Subtel-datos-clientes.html> [Consulta: 9 de agosto de 2020]
[151] Jorge Jaraquemada en El Mercurio, Empresas de Telecomunicaciones se enfrentan con la Subtel por dos casos que involucran entregar datos de sus clientes. Jueves 6 de agosto de 2020. [En línea] <https://www.emol.com/noticias/Economia/2020/08/06/994139/Empresas-telecomunicaciones-Subtel-datos-clientes.html> [Consulta: 9 de agosto de 2020]
[152] Jorge Jaraquemada en El Mercurio, Empresas de Telecomunicaciones se enfrentan con la Subtel por dos casos que involucran entregar datos de sus clientes. Jueves 6 de agosto de 2020. [En línea] <https://www.emol.com/noticias/Economia/2020/08/06/994139/Empresas-telecomunicaciones-Subtel-datos-clientes.html> [Consulta: 9 de agosto de 2020]

norma habilita el tratamiento de datos por parte de órganos de la Administración. Por otro lado, también es problemática la ausencia de un órgano de control del cumplimiento de la normativa de protección de datos personales.

La Ley sobre Protección de la Vida Privada establece que el tratamiento de datos personales por parte de un organismo público será legítimo, en la medida que lo efectúe respecto de las materias de su competencia[153]. De esta forma, la ley no establece criterios específicos que limiten el tratamiento de información por parte de la Administración, sino que, para determinar su legalidad, reenvía a las normativas que especifiquen las funciones de los organismos.

En el caso de la Subsecretaría de Telecomunicaciones, nos encontramos con una situación en que, ninguna norma, considerando todas las diversas disposiciones que regulan al órgano[154], establece específicamente una facultad de tratar datos de los usuarios de los servicios de telecomunicaciones. Por otro lado, la norma que, supuestamente, fundamentaría la realización de la encuesta de satisfacción que, a su vez, permitiría el tratamiento de los datos, es increíblemente amplia y se refiere simplemente a proponer políticas de telecomunicaciones[155]. Se puede apreciar, como esta técnica de reenvío expone la información de los titulares de datos, al no establecer criterios claros que limiten, en algún término, las facultades que tendrá el Estado al respecto.

Además, la ley no hace referencia a la forma en que un órgano de la Administración podrá entregar datos a terceros para que estos realicen su tratamiento. De esta manera, situaciones como las que ocurrió con la empresa CADEM, no están apropiadamente reguladas, lo que es particularmente negativo, porque el Estado continuamente externaliza labores.

Por otra parte, se aprecia la ausencia de un organismo que se dedique a velar por el cumplimiento de la normativa de datos personales es una de las fallas más acusadas de la legislación vigente. Al respecto, se ha señalado que uno "de los consensos que existe en materia de protección de datos es que Chile requiere de una autoridad de control que se haga cargo de promover, educar e informar a los ciudadanos sobre su derecho a la vida privada y a

[153] Artículo 20 de la Ley N° 19.628 sobre Protección de la Vida Privada.
[154] Considerando: (1) Decreto Ley 1.762 de 1977, en sus artículos 4°, 6° y 7°; (2) Ley 18.168 General de Telecomunicaciones, en sus artículos 2° y siguientes (Título II "De las Concesiones y Permisos"), 24° letra l), 28° A y siguientes (Título IV "Del Fono de Desarrollo de las Telecomunicaciones"), 28° bis, 29° y siguientes, (Título V "De las Tarifas") 34°, 36° y siguientes (Título VII "De las Infracciones y Sanciones"), 39 A (Título VIII "De las Infraestructuras Críticas de Telecomunicaciones"); y (3) Ley 18.838 que Crea el Consejo Nacional de Televisión, en sus artículos 23° y 30°.
[155] Facultad que se puede encontrar en los artículos 4° y 6° letra a) del Decreto Ley 1762 de 1977.

la protección de sus datos personales, fiscalizar el cumplimiento de la ley y sancionar las infracciones"[156].

La normativa vigente, que ha sido descrita como deficiente en proteger los derechos de los titulares de datos, se ve aún más debilitada por las interpretaciones y aplicación, que las autoridades de la administración y tribunales de justicia hicieron.

La primera gran falta de juicio por parte de la administración viene en la solicitud de información. Si bien, es posible argumentar que la Subsecretaría tiene facultades para hacer encuestas a los usuarios de los servicios de telecomunicaciones, el requerimiento de información de ninguna forma se adecua a los estándares de protección de datos; porque, junto a las razones que fueron desarrolladas previamente, los datos solicitados fueron demasiados desde un punto de vista cuantitativo y cualitativo. Es más, parece evidente que la Subtel no tuvo en cuenta esta regulación al momento de realizar la petición.

Por otro lado, en la impugnación de Entel, que fuera resuelta por la Ministra de Transportes y Telecomunicaciones, son claros los errores interpretativos y de aplicación de la normativa de protección de datos, yerros que inician con la definición misma de dato personal que excluyó del análisis la posibilidad de un titular identificable.

Por su parte, la Corte de Apelaciones de Santiago omitió referirse al conflicto adoptando una perspectiva de protección de datos personales, aun cuando todo el litigio giró en torno a la regulación de la Ley sobre Protección de la Vida Privada. Lo mismo ocurrió con la Corte Suprema, aunque su competencia estaba limitada por la estructura del recurso procesal a través del cual conoció la controversia.

Además, una de las primeras cuestiones que saltan a la luz al analizar el caso, tiene que ver con la colisión entre las normas que establecen incentivos para la actuación de las empresas, o sea, entre la regulación sectorial de telecomunicaciones y la normativa de protección de datos personales.

En un mercado relativamente regulado como el de las telecomunicaciones, es lógico que existan multas por incumplimientos frente a los requerimientos de la Subsecretaría que actúa como órgano fiscalizador. Sin embargo, en el estudio de este caso se puede apreciar como la

[156] ALVAREZ VALENZUELA, Daniel. 2016. Acceso a la información pública y protección de datos personales: ¿puede el Consejo para la Transparencia ser la autoridad de control de materia de protección de datos? *RDUCN* vol.23, n.1. p. 76. [En línea]. <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-97532016000100003&lng=es&nrm=iso>. [Consulta: 10 de agosto 2020]

cuantía de estas multas es de tal magnitud que puede servir para desalentar el cumplimiento de otra normativa igualmente relevante, como la regulación de datos personales, que adolece de falta de elementos disuasivos importantes.

Como se estableció, todas las empresas de telecomunicaciones están sometidas, al menos, al estándar que impone la Ley N° 19.628 en cuanto a la protección de datos, por ello, no se puede justificar que hayan procedido a entregar los datos requeridos por la Subsecretaría, sin reparar en la especial protección que la información merecía.

Por ello, frente a una regulación como la chilena, que está al debe en diversos aspectos relevantes y no constituye una protección eficaz para las garantías de los titulares de datos, el cumplimiento de parte de las empresas se torna fundamental; de esta forma, la adopción de planes de *compliance* efectivos reporta beneficios para la sociedad, impactando positivamente no sólo en los titulares de datos, sino también en los negocios que realizan las empresas. En este contexto, los recientes reparos a las solicitudes de la Subtel representan un avance.

En definitiva, el caso es la muestra perfecta de las diversas falencias de nuestra regulación vigente en materia de protección de datos personales y, a la vez, evidencia la poca atención que ponen los actores relevantes a la hora de hacer tratamiento de información de la cual no son titulares.

Capítulo IV: Administración del Estado y datos personales

I. Necesidad de un ajuste regulatorio

El caso analizado en el presente trabajo pone en evidencia una serie de fallas y debilidades normativas que es absolutamente necesario atender, dada la importancia que tiene la protección de datos en la sociedad actual. En el caso de la administración pública, esto cobra especial relevancia considerando que este caso no es el primero ni el único en que se pueden ver problemas en el tratamiento de la información de las personas.

1. Sociedad de la información, economía digital y protección de datos

La mejor manera de mostrar la necesidad de un ajuste regulatorio en materia de protección de datos personales es entendiendo su valor en el contexto actual. Comprendiendo que hoy, la información es la moneda que mueve a la economía, se puede llegar a entender por qué es fundamental que la regulación sea una forma efectiva para la protección de las garantías de los titulares de datos.

Dos conceptos aparecen al intentar caracterizar a la sociedad actual, estos son los de sociedad de la información y economía digital. Primero, se "entiende por sociedad de la información 'el desarrollo social, heredero de la sociedad industrial, alcanzado por la implantación de las tecnologías de la información y comunicaciones, que permite a todas las partes implicadas (personas físicas y jurídicas, administraciones, organismos, instituciones, industrias, etc.) enviar, recibir, solicitar distribuir, obtener, almacenar, evaluar, compartir y procesar cualquier información de forma instantánea, ubicua e interactiva'."[157]. Por su parte, "la definición de economía digital se puede resumir en una transformación de todos los sectores de la economía mediante la digitalización de la información"[158].

Es en este contexto, en el que los medios tecnológicos permiten traspasos y almacenamiento de información de forma más rápida y eficiente, que los datos son un activo fundamental. Se señala que, los datos pueden ser utilizados de diversas formas para generar valor en todo tipo de industrias, funcionando como herramienta para microtargeting comercial, optimización de sistemas, toma de decisiones, modelación de probabilidades, servicios digitales y para

[157] MONTECINOS GARCÍA, Alejandro. 2012. La sociedad de la información y el gobierno electrónico. Revista chilena de derecho y tecnología. Vol. 1 n 1. p. 173. Revista chilena de derecho y tecnología. [En línea] <https://rchdt.uchile.cl/index.php/RCHDT/article/view/24029> [Consulta: 8 de noviembre 2020]

[158] Consejo para la Transparencia, Dirección de estudios. Cuaderno de Trabajo N° 15: Protección de Datos Personales en la era de la Economía Digital. p. 8. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Economi%CC%81a-digital-V4.pdf> [Consulta: 8 de noviembre 2020]

aumentar el valor de otros activos[159]. Por ello, es importante revisar nuestra regulación actual, para modernizarla, estableciendo estándares que protejan adecuadamente a los titulares de datos y a la vez permita el desarrollo.

Adicionalmente, la administración pública también se ha visto afectada por el fenómeno presentado, y se aprecia una tecnologización de los procedimientos administrativos. Así, el gobierno digital, definido como la utilización de tecnologías de la información y comunicación para otorgar servicios gubernamentales a los ciudadanos y los negocios de forma más eficiente y efectiva[160], se vuelve una realidad.

Al respecto, se ha señalado que "no se trata de un mero cambio formal: el gobierno electrónico es un cambio de paradigma en la forma en que se relaciona el Estado con los ciudadanos"[161] y es en este cambio, el que, en cierta medida, justifica que el sector público maneje "determinados tipos de información relacionados con los fines específicos que encomienda la Constitución como motor teórico jurídico del desarrollo de una comunidad"[162].

2. La administración pública y el tratamiento de datos personales

Es posible identificar dos formas de tratamiento de datos personales que realiza la administración. Por un lado, existe procesamiento de datos que el Estado obtiene de forma directa en su relación con el titular de los datos; esta información, en ocasiones, puede ser compartida entre distintos organismos. Por otro lado, los gobiernos pueden obtener información de los titulares, de forma indirecta, recurriendo a bases de datos que otras entidades privadas mantienen.

2.1. Tratamiento de datos "directo" por parte de la administración

Parece interesante revisar algunas de los problemas que trae aparejado el tratamiento de casos que, en este trabajo, se ha caracterizado como directo. Al respecto, diversos casos, relativamente recientes, nos pueden mostrar situaciones en que algún órgano del Estado ha

[159] Al respecto, ver Consejo para la Transparencia, Dirección de estudios. Cuaderno de Trabajo N° 15: Protección de Datos Personales en la era de la Economía Digital. p. 10 y 11. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Economi%CC%81a-digital-V4.pdf>
[160] Traducción libre del original: "E-government can thus be defined as the use of ICTs to more effectively and efficiently deliver government services to citizens and businesses.". En: UN E-Government Knowledgebase. What is e-government. [En línea] <https://publicadministration.un.org/egovkb/en-us/about/unegovdd-framework> [Consulta: 9 de octubre 2020].
[161] MONTECINOS GARCÍA, Alejandro. Op. Cit. p. 188.
[162] MONTECINOS GARCÍA, Alejandro. Ibid. p. 201.

tomado decisiones difícilmente aceptables desde el punto de vista de la protección de datos personales.

Sin ánimo de hacer un recuento exhaustivo, se puede mencionar el tratamiento de información por parte del Servicio Electoral, quien debe entregar la información completa del padrón electoral a través de solicitudes de transparencia, pero "no lleva el control del acceso a datos personales vía solicitudes de acceso a la información de acuerdo a lo mandatado por la ley de datos personales"[163] y tampoco "fiscaliza los segundos usos de la información, la que si bien es pública según la ley no puede usarse con fines comerciales"[164].

Otro caso particularmente grave, lo constituye la exposición de datos sensibles de gran parte de la población nacional, el año 2016, por las vulnerabilidades de la red del Ministerio de Salud[165]. También referente al desconocimiento de la protección de datos sensibles de salud, encontramos las solicitudes de información realizadas por alcaldes de diversas comunas del país a propósito de la pandemia de COVID-19, durante el año 2020[166].

En el mismo sentido, la desprotección de datos sensibles ha ocurrido respecto de un sector particularmente vulnerable de la población, al firmarse un convenio entre la Agencia Nacional de Inteligencia y el Servicio Nacional de Menores, para que la primera entidad accediera a información de niños, niñas y adolescentes[167].

---

[163] GARRIDO, Romina, MATUS, Jessica, RAYMAN, Danny y BECKER, Sebastián, en Datos Protegidos. Datos personales e influencia política en Chile. p. 25. [En línea] <https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf> [Consulta: 3 de octubre 2020].

[164] GARRIDO, Romina, MATUS, Jessica, RAYMAN, Danny, BECKER, Sebastián, en Datos Protegidos. Ibid. p. 25.

[165] Según constata una investigación de CIPER, "Pacientes con VIH, mujeres que pidieron la píldora del día después, enfermos mentales. Todos con nombre, RUT y domicilio estaban disponibles hasta el viernes 4 de marzo en la plataforma computacional del Ministerio de Salud. Cualquiera de sus 100 mil funcionarios, e incluso externos, podían acceder a esa información privada. Se trata de la peor vulneración de la seguridad informática en salud, pues hubo al menos 3 millones de archivos desprotegidos durante meses. Lo grave es que la falla se alertó hace 10 meses. Ni la seguridad del Minsal ni ENTEL, empresa que presta el servicio de la red, actuaron." En: CARVAJAL, Víctor y JARA Matías para CIPER. Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes. 05 de 03 de 2016. [En línea] <https://www.ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/> [Consulta 5 de noviembre 2020].

[166] La Contraloría General de la República, en el dictamen N°008113N20, del 20 de abril de 2020, se pronunció al respecto, señalando que "considerando que ni la referida ley N° 20.584 -que no admite otras excepciones que las descritas- ni otro texto legal vigente, autorizan expresamente a las municipalidades o sus respectivos alcaldes para realizar el tratamiento de datos sensibles, no resulta procedente la entrega a tales entidades o autoridades de información de salud relativa a los pacientes que hayan sido diagnosticados con el denominado COVID-19, sin su consentimiento. Cualquier medida en contrario requerirá de la aprobación de la correspondiente ley modificatoria que así lo permita".

[167] La Defensora de la Niñez, Patricia Muñoz, "manifestó su absoluto rechazo al convenio entre la ANI y el SENAME luego que, esta mañana el Sindicato de Trabajadores Subcontratados del SENAME, Sintrasub, le hiciera llegar la información de que el pasado 21 de febrero se aprobó por el SENAME un acuerdo denominado 'Convenio de Colaboración y Coordinación con la Agencia Nacional de Inteligencia' cuyo objetivo sería facilitar información a la ANI que ésta considere relevante o pertinente para generar inteligencia y efectuar apreciaciones globales y sectoriales". [En línea] <https://www.defensorianinez.cl/noticias/defensora-de-la-ninez-evalua-acciones-

Adicionalmente, se puede mencionar el reciente requerimiento de información del Ministerio de Hacienda a la Superintendencia de Pensiones a propósito del retiro de fondos de las Asociaciones de Fondos de Pensiones[168].

A través de estos casos, se puede ver que los principales problemas que aparecen tienen que ver con la exposición de la información, que puede ocurrir por aplicación de la normativa de transparencia o por vulnerabilidades de seguridad de los sistemas usados por los órganos de la administración; o bien, con el traspaso infundado de información entre organismos que tienen distintas atribuciones legales.

2.2. El acceso a datos del sector privado por parte de la administración

A diferencia de los ejemplos anteriores, el caso estudiado en este trabajo constituye un acceso masivo, por parte de la administración, a datos que están en poder del sector privado. De este modo, la solicitud de información de la Subtel puede ser enmarcada en el acceso sistemático de datos por parte de los gobiernos; un artículo[169] se refiere a este fenómeno en los siguientes términos:

> *"Governments around the world have always demanded that commercial entities disclose data about their customers in connection with criminal investigations, enforcement of regulatory systems, and national security matters. Companies have always felt an obligation -and oftentimes are under legal compulsion- to cooperate, but they have also felt a business need and sense of responsibility to protect their customers' personal data and, in most*

constitucionales-de-no-revertirse-el-convenio-entre-la-ani-y-el-sename/> Por su parte, el Consejo para la Transparencia, a través de su presidente, Jorge Jaraquemada, se refirió a esta situación y señaló que "dicho acuerdo sobrepasa la garantía constitucional de la protección de datos en niños, niñas y adolescentes ya que requiere consentimiento de titulares, una ley que lo autorice o ser objetos de beneficios de salud (…) por las características del servicio que entrega SENAME y atendiendo sus atribuciones legales se desprende que los datos que el organismo posee 'constituyen datos personales y sensibles, por cuanto sus titulares son los niños, niñas y adolescentes que tiene a su cuidado y resguardo'". [En línea] <https://www.consejotransparencia.cl/cplt-el-convenio-entre-sename-y-la-agencia-nacional-de-inteligencia-no-se-ajusta-a-la-garantia-constitucional-de-proteccion-de-datos-en-ninos-ninas-y-adolescentes/>

[168] Este caso es increíblemente similar a la solicitud de información de la Subtel, con la diferencia de que este último se produce entre dos órganos del sector público. En resumen, lo que sucedió es que el Ministerio de Hacienda "solicitó información a la Superintendencia de Pensiones con fines netamente estadísticos, para evaluar el potencial impacto de la medida del retiro de fondos de pensiones sobre el sistema financiero del país y su impacto fiscal y tributario asociado", la Cartera de Estado señala que este requerimiento se enmarca en sus facultades y agrega que "para enriquecer este análisis resultó necesario solicitar las nóminas de afiliados que permiten cruzar información con otras fuentes de datos disponibles para el Ministerio de Hacienda. De esta forma, se puede evaluar y modelar conjuntamente esta y otras medidas de apoyo económico, que han surgido en el contexto de la crisis producida por la pandemia de COVID-19". Al respecto, ver declaración Ministerio de Hacienda, del 4 de noviembre 2020. [En línea] <https://www.hacienda.cl/noticias-y-eventos/noticias/declaracion-ministerio-de-hacienda>

[169] Basado en los simposios sobre el acceso sistemático del gobierno a datos del sector privado, contenidos en el Volumen 2 N° 4 y el Volumen 4 N° 1 del *International Data Privacy Law Journal* de la Universidad de Oxford.

cases, have diligently sought to balance those interests. In recent years, there has been an increase worldwide in government demands for data held by the private sector, driven by a variety of factors. This has included an expansion in government requests for what could be called 'systematic access'. This term encompasses both direct access by the government to private-sector databases, without the mediation or interaction of an employee or agent of the entity holding the data, and government access, whether or not mediated by a company, to large volumes of private-sector data"[170].

El trabajo mencionado, que revisó el acceso de datos por parte del gobierno en trece países[171], expone que, "en la mayoría, si no en todos los países estudiados, las estructuras legales dan una base inadecuada para la conducta de acceso sistemático, tanto desde una perspectiva de derechos humanos, como a un nivel práctico"[172].

Además, se determinó que "en cada país estudiado, incluso en aquellas naciones con leyes de protección de datos que de otro modo serían integrales, el acceso para propósitos regulatorios, de aplicación legal y seguridad nacional es comúnmente excluido de tales leyes; alternativamente, se tratan como fines aceptados, para los que el acceso está autorizado bajo leyes separadas que pueden o no proporcionar salvaguardias adecuadas contra posibles abusos."[173].

[170] RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. 2014. Systematic government access to personal data: a comparative analysis. *International Data Privacy Law,* Vol. 4. n. 2. p. 98. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipu004> [Consulta: 13 de noviembre 2020]. Traducción libre: Los gobiernos de todo el mundo siempre han exigido que las entidades comerciales divulguen datos sobre sus clientes por investigaciones penales, aplicación de sistemas regulatorios y asuntos de seguridad nacional. Las empresas siempre se han sentido obligadas y, a menudo, están bajo la obligación legal de cooperar, pero también han tenido una necesidad y sentido empresarial de responsabilidad para proteger los datos personales de sus clientes y, en la mayoría de los casos, han buscado diligentemente, equilibrar esos intereses. En los últimos años, ha habido un aumento mundial en las demandas gubernamentales por datos almacenados en el sector privado, impulsado por una variedad de factores. Esto ha incluido una expansión en las solicitudes de los gobiernos, de lo que podría llamarse un 'acceso sistemático'. Este término abarca tanto el acceso directo del gobierno a bases de datos del sector privado, sin la mediación o interacción de un empleado o agende de la entidad titular de los datos, y acceso gubernamental, sea mediado o no por una empresa, a grandes volúmenes de datos del sector privado.

[171] Australia, Brasil, Canadá, China, Francia, Alemania, India, Israel, Italia, Japón, Corea del Sur, Reino Unido y Estados Unidos.

[172] RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. Op. Cit. p. 97. Traducción libre de: "First, that in most, if not all countries studied, existing legal structures provide an inadequate foundation for the conduct of systematic access, both from a human rights perspective and at a practical level."

[173] RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. Ibid. p. 97. Traducción libre de: "in every country studied, even those nations with otherwise comprehensive data protection laws, access for regulatory, law enforcement, and national security purposes is often excluded from such laws; alternatively, they are treated as accepted purposes for which access is authorized under separate laws that may or may not provide adequate safeguards against possible abuses."

Por su parte, se señala que "el acceso sistemático plantea preguntas difíciles para las compañías que enfrentan demandas de acceso, por parte del gobierno, a los datos que mantienen"[174], frente a esta situación, las empresas "deben decidir si la demanda o solicitud es legal, aunque la ley sea vaga"[175].

De esta forma, este segundo tipo de acceso por parte del gobierno también reviste de una serie de complejidades, tanto para el órgano público que hará procederá al tratamiento de la información, como para el privado que mantiene las bases de datos que deberá juzgar el mérito del requerimiento. Por ello, plantea desafíos regulatorios importantes, que difieren de aquellos casos en que el problema está centrado entre la persona natural titular de datos y la entidad de la Administración que hará uso de la información.

II. Propuestas para un ajuste regulatorio

1. Adopción de un enfoque de derechos fundamentales

En primer lugar, es primordial que toda la normativa tenga como objeto otorgar una protección adecuada de los datos, considerando que esta es una garantía fundamental. Para esto, es importante que se la reconozca como un derecho que, si bien está relacionado con la privacidad, tiene ciertas particularidades que lo diferencian. Además, se requiere considerar la directa relación que el derecho a la autodeterminación informativa tiene con el desarrollo de la persona humana.

1.1. Privacidad y autodeterminación informativa

El derecho a la protección de datos personales ha sido conceptualizado como íntimamente ligado al derecho a la privacidad, pero desde su constitucionalización como un derecho distinto, se ha comenzado a escribir respecto de aquellas diferencias que agregan valor a la autodeterminación informativa.

Así, por ejemplo, tras la inclusión de la garantía en la Carta de Derechos Fundamentales de la Unión Europea, autores han señalado que "ha llegado el momento de que la protección de datos opere como un verdadero derecho fundamental, desde una perspectiva positiva y negativa. La protección de datos debería ser capaz de no sólo regular, sino también, de prohibir al poder. Esto significa que las infracciones al derecho a la protección de datos

[174] RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. Op. Cit. p. 96. Traducción libre de: "Systematic access raises hard questions for companies that face demands for government access to data they hold".
[175] RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. Ibid. p. 96. Traducción libre de: "They must decide whether the demand or request is lawful, though the law may be vague". Systematic government access to personal data: a comparative analysis. P. 96.

personales deben determinarse solamente sobre la base de los principios relevantes para la protección de datos, con aplicación del principio de proporcionalidad, sin la necesidad de recurrir al derecho a la privacidad."[176].

En este sentido, se debe tener en cuenta todos aquellos principios que la transforman en una garantía que

Por otra parte, la protección de datos personales también está relacionado con la dignidad humana, por ser considerado necesario para el desarrollo de la personalidad de sus titulares. En este sentido, en su pronunciamiento del año 1983, el Tribunal Constitucional Federal Alemán determinó que:

> *"The general right of personality encompasses, based on the notion of self-determination, the power conferred on the individual to, in principle, decide themselves whether and to what extent to disclose aspects of their personal life.*
>
> *If individuals cannot, with sufficient certainty, determine what kind of personal information is known to their environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this may seriously impair the freedom to exercise self-determination. In the context of modern data processing, the free development of one's personality therefore requires that the individual is protected against the unlimited collection, storage, use and sharing of personal data."*[177]

[176] TAZNOU, Maria. 2013. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law.* Vol. 3. n. 2. P. 99. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipt004> Traducción libre del siguiente texto: "The time has come for data protection to operate as a real fundamental right both positively and negatively. Data protection should be able not only to regulate, but also prohibit, power. This means that infringements of the right to data protection should be determined solely on the basis of the relevant data protection principle themselves, with the application of the principle of proportionality, without the need to recourse to the right to privacy."

[177] Bundesverfassungsgericht. Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209/83. [En línea] <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html> Traducción libre: El derecho general de personalidad abarca, basado en la noción de autodeterminación, el poder conferido al individuo para, en principio, decidor por sí mismo sí y en qué extensión revelar aspectos de su vida personal. Si los individuos no pueden, con suficiente certeza, determinar qué tipo de información personal es conocida para su ambiente, y si es difícil averiguar qué tipo de información tienen los posibles socios, esto puede afectar de forma seria la libertad a ejercer la autodeterminación. En el contexto del procesamiento moderno de datos, el desarrollo libre de la personalidad requiere, por tanto, que el individuo esté protegido de la recopilación, almacenamiento, uso e intercambio de datos personales ilimitado.

1.2. Criterios mínimos de una regulación que protege derechos fundamentales

Dado que la protección de datos personales es una garantía fundamental que busca proteger la dignidad humana, propendiendo al libre desarrollo de la personalidad de sus titulares, corresponde que la regulación a considere ciertos elementos esenciales. En este sentido, se ha escrito que, aquellos criterios son "(a) el establecimiento de principios y deberes que legitimen el tratamiento de los datos personales, consistentes con la evolución social y tecnológica; (b) el reconocimiento de los derechos de los interesados y los procedimientos para garantizar su ejercicio, con el fin de que se les permita un control efectivo respecto de su información y; (c) la existencia de autoridades independientes de control, en el sentido de que sean ajenas a cualquier influencia externa, tanto directa como indirecta."[178].

1.3. Limitaciones legítimas a la autodeterminación informativa

Por otra parte, como todo derecho, la protección de datos personales admite restricciones que deben cumplir con ciertas condiciones mínimas que aseguren su legitimidad. Así, la protección de datos podrá ser restringida, mientras "las limitaciones sean establecidas por ley, persigan una finalidad legítima, sean necesarias en una sociedad democrática, se ajusten al principio de proporcionalidad y respeten la esencia del derecho a la protección de datos"[179].

2. Balance del derecho a la protección de datos con otros principios de la administración

Para poder regular correctamente el tratamiento de datos personales en la administración, se requiere conocer con qué otras funciones y principios, propios del sector público, esta garantía fundamental colisiona. De este modo, se debe tener en cuenta que los órganos públicos, en cuanto proveedores de servicios y en sus funciones reguladora y fiscalizadora deben manejar determinada información. Además, se debe considerar los principios principales principios a los que está sujeta la actividad pública para ver como interactúan con el derecho a la protección de datos.

2.1. Función pública y datos personales

Tal como lo indica la Constitución "el Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones

[178] MAQUEO, María, MORENO, Jimena, RECIO, Miguel. Op. Cit. p. 95.
[179] TAZNOU, Maria. Op. Cit. p. 98. Traducción libre del extracto: These restrictions, however, will be permissible, insofar as they meet the following conditions: (i) they are provided by law; (ii) they pursue a legitimate aim; (iii) they are necessary in a democratic society; (iv) they conform with the principle of proportionality; and (v) they respect the 'essence' of the right to data protection.

sociales que permitan a todos y cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respeto de los derechos y garantías"[180]. Esto es profundizado en la Ley Orgánica Constitucional sobre Bases Generales de la Administración del Estado, que establece que "la Administración del Estado está al servicio de la persona humana; su finalidad es promover el bien común atendiendo las necesidades públicas en forma continua y permanente y fomentando el desarrollo del país a través del ejercicio de las atribuciones que le confiere la Constitución y la ley, y de la aprobación, ejecución y control de políticas, planes, programas y acciones de alcance nacional, regional y comunal"[181].

De esta forma, a la administración le corresponderá promover el bien común, atendiendo necesidades públicas. La cantidad de información de individuos que los organismos requerirán para cumplir sus funciones variará dependiendo de cuáles sean estas. Además, es fundamental recordar que, "en muchos casos, la acción del Estado está orientada hacia sectores de la población que presentan algún tipo de vulnerabilidad social"[182], por lo tanto, debe haber altos estándares para el manejo de la información, para evitar posibles discriminaciones o cualquier otro perjuicio hacia los titulares de datos. Al respecto, se ha señalado que:

> *"Son adecuadas las constataciones que se han hecho en cuanto a que el Estado es el principal tenedor de información personal (posee lo que la Ley 19.628 denomina 'registros, recopilaciones o bancos de datos'), ya que, efectivamente, i) por razones de planificación, gestión y orden público, almacena y registra hechos y documentos que constituyen información personal de los ciudadanos; ii) porque el Estado realiza tratamiento de datos personales sin necesidad de autorización expresa de los ciudadanos titulares sino por mandato legal; iii) porque se requiere manejar y procesar información nominativa al elaborarse políticas públicas y al desempeñar sus funciones los servicios públicos; y vi) porque el Estado trata o procesa electrónicamente datos sensibles como los antecedentes de salud.*

[180] Artículo 1° inciso 4° de la Constitución Política de la República.
[181] Artículo 3° inciso 1° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
[182] Consejo para la transparencia. Unidad de estudios y publicaciones. 2015. Cuaderno de trabajo N° 3. Protección de datos personales en el manejo de datos de investigación realizado por organismos públicos. p. 11. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/proteccion_datos_final.pdf> [Consulta: 13 de noviembre 2020]

> *Al derecho público le corresponde establecer 'límites' y 'restricciones'. Los primeros, para que no se vulnere la intimidad de las personas cuyos datos se procesan. Las segundas, para que sólo se usen los datos personales dentro de la competencia exclusiva de los servicios públicos y para sus fines específicos."*[183]

En ese sentido, es importante que existan leyes especiales que regulen los casos particulares en los que hay tratamiento de datos sensibles, como ocurre, por ejemplo, en la Ley N° 20.584 que regula los derechos y deberes de los pacientes que, en conjunto con su reglamento, contienen disposiciones respecto de las condiciones bajo las cuales debe procesarse la información contenida en las fichas clínicas.

Por otro lado, desde el punto de vista de la creación de políticas públicas y fiscalización de su cumplimiento, es claro que los órganos de la administración deben contar con información de los sectores regulados, ahora bien, se debe prestar especial atención cuando la información de la industria corresponde a datos personales de titulares individuales, como ocurrió en el caso de Entel con la Subsecretaría de Telecomunicaciones, en el cual, al intentar recabar información sobre el funcionamiento del mercado de las telecomunicaciones, se terminó requiriendo una cantidad desproporcionada de datos personales.

Otra de las funciones que debe cumplir el aparato estatal tiene que ver con el resguardo de la seguridad nacional y la protección de la población. Al respecto cabe señalar que, "en el caso de la Agencia Nacional de Inteligencia, es posible constatar que no hay autorización en su ley orgánica que les habilite recolectar, procesar y comunicar datos personales en el ejercicio de sus funciones. En la Ley N° 19.974 que regula el funcionamiento del sistema de inteligencia del Estado (LSIE) -a cuya cabeza, aunque con escaso mando- se encuentra la Agencia, no hay norma que habilite a ésta ni a las instituciones que forman parte del sistema a recolectar, solicitar ni procesar datos personales. De esta manera, carecen de la habilitación requerida por la ley, lo que afecta el principio de legalidad en la actuación de los órganos del Estado."[184].

[183] JIJENA, Renato. 2013. Tratamiento de datos personales en el Estado y acceso a la información pública. *Revista Chilena de Derecho y Tecnología.* Vol. 2. n. 2. p. 52. [En línea] <https://rchdt.uchile.cl/index.php/RCHDT/article/view/30309> [Consulta: 13 de noviembre 2020].

[184] ÁLVAREZ VALENZUELA, Daniel y VERA HOTT, Francisco, en CIPER. 24 de junio de 2020. Datos personales y las necesidades de un sistema de inteligencia. [En línea] <https://www.ciperchile.cl/2020/06/24/datos-personales-y-las-necesidades-de-un-sistema-de-inteligencia/> [Consulta: 29 de noviembre 2020].

2.2. Principios a los que debe someterse la administración

Como lo indican la Constitución y la ley N° 18.575, los órganos del Estado "deberá observar los principios de responsabilidad, eficiencia, eficacia, coordinación, impulsión de oficio del procedimiento, impugnabilidad de los actos administrativos, control, probidad, transparencia y publicidad administrativas y participación ciudadana en la gestión pública"[185].

El debate doctrinario sobre los principios que informan a la administración en relación con la protección de datos personales se ha centrado en la necesidad de compatibilizar esta garantía con el principio de transparencia y el acceso a la información. A este respecto, en un estudio de derecho comparado se indica que "no identificamos modelos normativos en donde se evidencie una tendencia absoluta por favorecer el acceso a la información pública por sobre la protección de la información personal, o viceversa, un problema a resolver consiste en determinar cuál derecho debe aplicarse en la relación entre estas dos garantías"[186].

En nuestro sistema, es menester comprender las limitaciones que estos derechos se imponen mutuamente, sobre todo porque el Consejo para la Transparencia, órgano llamado a velar por el acceso a la información pública, tiene también la función de garantizar la protección de datos personales en el sector público.

Por ello, se ha señalado que es necesario reflexionar sobre la idea de que "la protección de datos personales de los ciudadanos (y de los propios funcionarios públicos) debe ser un límite al derecho de acceso a la información, pero considerando caso a caso y la especial naturaleza del dato personal involucrado"[187]; el planteamiento según el cual "las leyes de acceso a la información necesariamente deben ser compatibles con las de privacidad y datos personales"[188]; y la propuesta de que, "la protección de datos personales no debe usarse 'de manera general y sistemática' para no abrir información del Estado, ya que la restricción al acceso de ciertos y determinados antecedentes referidos a los ciudadanos y a los funcionarios públicos puede amparar actos de corrupción, lo que, por cierto, también debe resolverse caso

[185] Artículo 3° inciso 2° de la Ley Orgánica Constitucional N° 18.575 de Bases Generales de la Administración del Estado.
[186] SANZ SALGUERO, Francisco. 2016. Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. *Revista ius et praxis.* Vol. 22. n. 1. p. 372. [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122016000100010&lng=es&nrm=iso> [Consulta: 20 de noviembre 2020].
[187] JIJENA, Renato. Op. Cit. p. 65.
[188] JIJENA, Renato. Ibid. p. 65.

a caso o en forma individual según la especial naturaleza del dato personal pedido de acceso"[189].

3. Algunas notas para la reforma normativa

Como se ha visto, es fundamental mejorar la legislación vigente para poder abarcar los problemas que se han revisado en este trabajo, porque, pese a que ha habido algunos avances en la interpretación de la normativa de protección de datos personales, esta se ha mostrado insuficiente para proteger la información de los titulares cuando el tratamiento de la información la hacen órganos de la administración. Por ejemplo, se ha señalado en doctrina que:

> *"En este contexto, resulta evidente que la Administración Pública ha tenido avances y retrocesos en la materia. Si bien la labor que el Consejo [para la Transparencia] ha realizado, mediante la dictación de sus recomendaciones de protección de datos y diversos dictámenes, ha permitido un progreso, los organismos públicos no han alcanzado el debido cumplimiento a la normativa de protección de datos. La falta de sensibilidad en esta materia se une al retraso normativo que Chile mantiene respecto a sus pares latinoamericanos y legislaciones europeas"[190].*

En este sentido, se debe comenzar por revisar la normativa emitida por el Consejo para la Transparencia, con la finalidad de establecer algunos de los criterios a nivel legal. También, se debe tener a la vista la regulación comparada y la normativa nacional especial sobre protección de datos.

La revisión de esos instrumentos permitirá fundamentar la necesidad de modificar la actual ley 19.628 en el sentido de normar de mejor manera las facultades de la administración e incluir un órgano de control específicamente diseñado para velar por la protección de datos.

3.1. Tomar las Recomendaciones del Consejo para la Transparencia como punto de partida

El Consejo para la Transparencia en sus Recomendaciones se refiere tanto a los principios orientadores de la protección de datos, como a los derechos que tienen sus titulares. Además,

[189] JIJENA, Renato. Op. Cit. pp. 65 y 66.
[190] MATUS, Jessica. 2013. Derecho de acceso a la información pública y protección de datos personales. *Revista chilena de Derecho y Tecnología.* Vol. 2. n. 1. P. 221. [En línea] <https://rchdt.uchile.cl/index.php/RCHDT/article/view/26959> [Consulta: 9 octubre 2020].

y en lo que aquí interesa, señalaron las obligaciones específicas de los organismos de la Administración.

De este modo, en las Recomendaciones se clarifican las condiciones de licitud del tratamiento de datos, señalando que "los organismos de la Administración del Estado pueden realizar tratamiento de datos personales, sólo y exclusivamente respecto de las materias de su competencia y con sujeción a las reglas que la ley establece (…) los órganos públicos no podrán efectuar tratamientos de datos personales en materias ajenas a su competencia, ni siquiera recabando el consentimiento de su titular"[191].

Por otro lado, el Consejo para la Transparencia incluye recomendaciones que van más allá de interpretar la normativa vigente. Señalan, por ejemplo, que los órganos del Estado deben tener una política de datos accesible al público y un encargado de protección de datos dentro de la organización.

Así, señalan que "los órganos de la Administración del Estado deben informar al titular de los datos (…) el propósito del almacenamiento de sus datos personales, es decir, la finalidad perseguida con el tratamiento de la información, y la posible comunicación de terceros"[192]. En ese sentido, sugieren "especialmente a los órganos o servicios públicos que dispongan de una política proactiva de difusión de información en esta materia a fin de dar cabal cumplimiento al deber de informar"[193].

También se indica que "para facilitar el cumplimiento de las obligaciones establecidas en la Ley N° 19.628 y una mejor observancia de las presentes recomendaciones, se sugiere que las distintas autoridades, jefaturas o jefes superiores de los órganos o servicios de la Administración del Estado, designen a un funcionario o funcionaria de dicha repartición para desempeñarse como encargado o encargada de protección de datos y constituya un contacto efectivo en la materia con el Consejo para la Transparencia"[194].

---

[191] Según lo indicaba la versión de 2011 de las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado. Versión que fue actualizada por la Resolución Exenta N° 304, que ya no contiene la disposición.
[192] Resolución exenta N° 304 del Consejo para la Transparencia, de 2020, que aprueba 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 Sustituye texto que indica.
[193] Resolución exenta N° 304 del Consejo para la Transparencia, de 2020, que aprueba 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 Sustituye texto que indica.
[194] Resolución exenta N° 304 del Consejo para la Transparencia, de 2020, que aprueba 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 Sustituye texto que indica.

Sin embargo, parte de la doctrina se ha referido a la ilegalidad de estas Recomendaciones porque el Consejo para la Transparencia sería incompetente para recomendar, se ha dicho que "esa competencia que le asignó el artículo 33 letra m) de la Ley 20.285 (…) consistente en 'velar por la aplicación de la Ley 19.628 en los servicios públicos', no puede leerse sino como un complemento de las otras normas de la ley de acceso a la información y transparencia. No es, de modo alguno, un mandato abierto para 'instituir' ahora bajo la denominación de 'recomendación', reglamentar y establecer nuevos requisitos no contemplados en el texto de la Ley 19.628, crear procedimientos de reclamo de *habeas data* ilegales, y autoasignarse competencia para conocer alternativamente de los recursos del artículo 12 de la Ley 19.628, lo que nunca estuvo ni en el espíritu ni en el debate del legislador de la Ley 20.285."[195].

Es claro que publicar una política de privacidad y tener un encargado de datos personales son recomendaciones útiles; por eso, es necesaria una modificación a la legislación vigente, que regule el tratamiento de datos por parte de la Administración de una forma más comprensiva, además de incluir un órgano fiscalizador del cumplimiento de la normativa que pueda generar instrumentos normativos cuya legitimidad no sea discutida, que incluya una interpretación clara de las normas de datos personales y puedan producir instrucciones vinculantes para las instituciones.

3.2. Reglamento General de Protección de Datos de la Unión Europea

Es innegable que el Reglamento Europeo se ha transformado en el estándar mundial en cuanto a protección de datos[196] y, por ello, es ideal que sus principios sean integrados en la normativa del país, porque de esta manera se facilitaran las relaciones comerciales entre empresas chilenas y extranjeras, al ser ambas receptoras no riesgosas de datos.

Las administraciones públicas europeas están sujetas a las disposiciones del Reglamento General de Protección de Datos y por ello deben cumplir con las diversas normas y principios.

---

[195] JIJENA, Renato. Op. Cit. p. 88.

[196] Incluso antes de su entrada en vigor, los autores ya predecían que el Reglamento General de Protección de Datos elevaría el estándar de protección de datos en el mundo, se señaló incluso que "la regulación promete un ámbito más amplio de cooperación entre las autoridades y controladores de datos, tanto dentro de la UE como a nivel internacional. Debería impulsar los esfuerzos para alcanzar cláusulas contractuales estándar más consistentes, agilizar los procesos de validación para las normas corporativas obligatorias y ayudarlas a encajar con acuerdos similares en otras partes del mundo". Traducción libre de: The regulation promises a wider scope for cooperation between authorities and data controllers both within the EU and internationally. It should galvanise efforts for a more consistent standard contractual clauses, speed up the validation process for binding corporate rules, and help them dovetail with similar arrangements elsewhere in the world. En: BUTTARELLI, Giovanni. 2016. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law.* Vol. 6. n. 2. p. 77. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipw006>

Se considera importante destacar las reglas sobre limitaciones al derecho de protección de datos, que deben ser establecidas en la ley, respetando en lo esencial los derechos y libertades fundamentales[197]. Otro aspecto relevante regulado de forma extensa en la norma europea es la garantía de seguridad de los datos[198].

Además, el Reglamento hace referencia a las comunicaciones de información hacia autoridades públicas. Se señala al respecto:

> *"Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento."*[199]

Es fundamental considerar las normas que refieren a las autoridades de protección de datos[200], instituciones públicas independientes con competencias y funciones definidas, que "ofrecen asesoramiento experto en cuestiones relacionadas con la protección de datos y tramitan reclamaciones presentadas por la violación del Reglamento general de protección de datos y las legislaciones nacionales pertinentes"[201].

---

[197] El listado completo de limitaciones se encuentra en el artículo 23 del Reglamento General de Protección de Datos de la Unión Europea.
[198] Ver el artículo 23 del Reglamento General de Protección de Datos de la Unión Europea.
[199] Razón 31 del Reglamento General de Protección de Datos de la Unión Europea.
[200] Ver Capítulo VI, artículos 51 y siguientes, del Reglamento General de Protección de Datos de la Unión Europea.
[201] Comisión europea. ¿Qué son las autoridades de protección de datos (APD)? [En línea] <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_es> [Consulta: 30 noviembre 2020]

Como nota adicional, el Reglamento también regula las decisiones automatizadas, señalando, como regla general que "todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar" [202]. Es importante tener en cuenta este tipo de regulación en el contexto de la tecnologización de la administración pública y la aplicación de inteligencia artificial en este ámbito[203].

Así, para modificar la normativa chilena vigente, que debe incluir, como mínimo, disposiciones sobre las restricciones legítimas al derecho a la protección de datos, la seguridad de la información, la comunicación de información a autoridades y establecer una institución que se dedique específicamente a velar por el cumplimiento de la normativa, resulta útil considerar el estándar europeo y adaptarlo a la realidad nacional.

III. Conclusiones

En este capítulo se revisó la importancia de los datos personales en el contexto actual, comprendiendo su valor en la sociedad de la información. Además, se subrayaron los efectos que tiene el hecho de que la protección de datos sea una garantía fundamental, considerando que el respeto a la autodeterminación informativa contribuye a asegurar el completo desarrollo de la personalidad de los seres humanos.

En ese marco, se diagnostica la urgencia de una modificación legislativa en materia de protección de datos personales y, en particular, la necesidad de regular de mejor forma la manera en que los órganos de la administración realizan tratamiento de la información, considerando que, en Chile, el sector público ha fallado en reiteradas ocasiones en la materia.

Para guiar una modificación normativa se revisaron las interpretaciones e innovaciones incluidas en las Recomendaciones del Consejo para la Transparencia y, más importante aún, se revisó algunas de las reglas contenidas en las normas de la Unión Europea.

De ahí, es posible concluir que se requiere una modificación en la normativa vigente, tendiente a profundizar en los estándares que se le exigen a la administración y que, a la vez, instituya

[202] Al respecto ver el artículo 22 del Reglamento General de Protección de Datos de la Unión Europea. Se debe notar que el artículo admite excepciones.

[203] En este sentido, se ha señalado que, "en un Estado de Derecho, es obvio que la regulación de la IA, en general, y, por lo que nos interesa aquí, de la toma de decisiones administrativas automatizadas debería tener un importante papel, asumiendo, como hacemos aquí, que la misma encuentra acomodo en las categorías clásicas de órgano administrativo y acto administrativo.". En: SOLÉ, Juli. 2019. Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo.* n. 50.

normas de seguridad de datos, las comunicaciones de información y que cree una autoridad de control.

Al respecto, es importante notar que el proyecto de ley en actual tramitación que busca modificar la normativa, mejora sustantivamente la regulación actual. En lo que interesa a este trabajo, se hace cargo de especificar el tratamiento de datos en la Administración, señalando que se deberán aplicar tanto los principios de protección de datos, como aquellos propios de los órganos del Estado; además, establece normas sobre la comunicación de información; e, importantemente, faculta al Consejo para la Transparencia para velar por la protección de los datos personales.

Finalmente, se debe considerar que, aunque hay una norma marco en creación que mejora en parte la situación general de desprotección de los datos personales, no es suficiente. Tal vez, sería interesante reflexionar sobre la necesidad de incorporar normativa de protección de datos personales en las leyes orgánicas de las instituciones de la administración que notoriamente, hagan más tratamiento de datos, asegurándose de que el tratamiento de la información sea legítimo, a la vez que seguro y limitado.

Conclusiones generales

En este trabajo se analizó la solicitud de información de la Subsecretaría y sus consecuencias desde la perspectiva de la protección de los datos personales. Así, se concluye, en primer término, que la información requerida por la Subtel se debe calificar jurídicamente bajo la categoría de datos personales, lo que tiene consecuencias tanto para la empresa Entel, que debe cumplir con ciertos deberes de protección de la información y para la administración, que debe respetar determinados requisitos para poder proceder al tratamiento de los datos.

Para Entel, y las empresas de telecomunicaciones en general, el que los números de teléfono solicitados sean datos personales implica que la información debía ser resguardada y no compartida a la Subsecretaría sin justificación. Así, la negativa de Entel a entregar la información no fue una acción sin fundamento, al contrario, era la única forma correcta de proceder respetando la normativa vigente en materia de protección de datos personales.

Por su parte, para la Subsecretaría de Telecomunicaciones, el que los números de teléfono y demás datos requeridos sean datos personales, significa que debe someterse a la Ley sobre Protección de la Vida Privada para su tratamiento. Esto implica, que sólo puede proceder sin consentimiento de los titulares si la ley lo habilita expresamente y, como se vio, las facultades de la Subtel no incluyen de forma directa la realización de estudios de satisfacción. Así al no tener la facultad legal para tratar la información sin el consentimiento de sus titulares, debió requerirlo para poder procesarlos, respetando, claro, las demás disposiciones de la normativa de protección de datos.

Por otro lado, en la contratación con el tercero CADEM para la realización de la encuesta se verificó una serie de complicaciones adicionales, tanto al nivel de las disposiciones contractuales, que no son suficientes para resguardar de forma correcta la seguridad de la información, como en la realización misma del estudio, para la que se entregó una cantidad de datos desproporcionados e innecesarios.

En definitiva, todas las acciones seguidas por la administración para la realización de la encuesta de satisfacción de usuarios en materia de telecomunicaciones desconocieron la normativa de protección de datos personales, poniendo en riesgo la información de prácticamente toda la población nacional.

Como se mostró, el actuar de la Subsecretaría de Telecomunicaciones, no es un hecho aislado. Al contrario, se puede encontrar una gran cantidad de ejemplos en los que el sector público afecta negativamente las garantías de los titulares de datos personales. Eso es grave, dado que, el que las personas tengan control sobre la información que terceros manejan sobre ellos, es fundamental en un Estado democrático.

Por ello, en este trabajo se defendió la necesidad de un ajuste regulatorio, que considere realmente el carácter de derecho fundamental de la protección de datos personales y dote de una eficacia real a la garantía, lo que implica que la normativa debe ser lo suficientemente fuerte como para disuadir a entidades privadas y, quizás más importantemente, debe ser efectiva en controlar al aparato estatal, porque es evidente que es uno de los actores que más tratamiento de datos hace.

A la vez, se debe reconocer lo difícil que resulta el balance entre las facultades que debe tener la Administración para regular y fiscalizar y la necesaria protección de datos personales. Dicha dificultad es visible en el caso presentado; la Subsecretaría de Telecomunicaciones es un órgano necesario que debe velar por el debido funcionamiento de uno de los mercados más relevantes, cuyas facultades al respecto no pretendieron cuestionarse en este trabajo, pero que, a la vez, realizó un requerimiento altamente cuestionable desde la perspectiva de protección de datos, mostrándose ciega a atender su principal función en cuanto órgano de la Administración, esto es, estar al servicio de la población.

La necesaria actualización de la Ley 19.628, en el sentido de elevar los estándares de actuación de órganos privados y públicos, tendrá efectos positivos no sólo para los titulares de los datos, sino que también servirá para incorporar a Chile de forma efectiva y segura en la economía digital. El aumento de los estándares de protección de la información permitirá que las empresas nacionales sean consideradas socias seguras por compañías internacionales, potenciando de esta forma la economía e innovación.

Por otro lado, si bien, actualmente existe un proyecto de ley para modificar la Ley 19.628, no se puede esperar a que este sea finalmente aprobado y publicado para comenzar a tomarle el peso a la protección de datos personales. En ese sentido, es vital que, como mínimo, los órganos administrativos que toman decisiones sobre el tratamiento de datos y los órganos jurisdiccionales que eventualmente revisan esas decisiones, tengan presente la normativa vigente, considerando al respecto, no sólo la ley, sino también la disposición constitucional que eleva el derecho a la protección de datos personales a garantía fundamental, los diversos

tratados de derechos humanos que pudieran ser aplicables, adoptando, en definitiva, la interpretación que sea más favorable a los derechos de los titulares de datos personales.

Finalmente, ad-portas de un proceso de cambio constitucional, es importante que adoptemos una nueva visión de la relación del Estado con sus ciudadanas y ciudadanos, de modo tal que este se vuelva un verdadero garante de los derechos. Se debe aprovechar esta instancia de debate democrático para poner sobre la mesa la necesidad de protección eficaz y completa de los datos personales de las chilenas y chilenos, no sólo porque la toma de decisiones en el país se debe hacer basándose en la información de las personas que se verán afectadas por ellas, sino también, porque el control de la información permite un adecuado desarrollo de la personalidad y, en definitiva, garantiza la dignidad.

Bibliografía

ÁLVAREZ, Daniel, 2020, El sistema constitucional de protección de la privacidad en el derecho chileno. Revista del Departamento de Ciencias de la Computación de la Universidad de Chile, Edición N° 19.

ÁLVAREZ, Daniel. Acceso a la información pública y Protección de Datos Personales. 2016. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *RDUCN.* Vol. 23. n. 1. [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-97532016000100003&lng=es&nrm=iso>.

ÁLVAREZ VALENZUELA, Daniel y VERA HOTT, Francisco, en CIPER. 24 de junio de 2020. Datos personales y las necesidades de un sistema de inteligencia. [En línea] <https://www.ciperchile.cl/2020/06/24/datos-personales-y-las-necesidades-de-un-sistema-de-inteligencia/>

Bundesverfassungsgericht. Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209/83. [En línea] <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html>

BUTTARELLI, Giovanni. 2016. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law.* Vol. 6. n. 2. p. 77. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipw006>

CERDA, Alberto, 2012, Legislación sobre Protección de las Personas frente al tratamiento de Datos Personales. Apuntes de clases, Centro de Estudios de Derecho Informático. Universidad de Chile.

CAMACHO, Gladys. 2014. La protección de datos como frontera del derecho de acceso a la información en la legislación chilena. *Revista de Gestión Pública*. Vol. 3, n. 1.

CANALES, María Paz, en Derechos Digitales. 2019. ¿Quién defiende tus datos? La problemática acción de Subtel. [En línea] <https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/>

Comisión europea, ¿Qué datos podemos tratar y en qué condiciones? [En línea] <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_es>

Comisión europea. ¿Qué son las autoridades de protección de datos (APD)? [En línea] <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_es>

Consejo para la Transparencia, Unidad Normativa, 2011. Protección de Datos Personales: Jurisprudencia relevante del Consejo para la Transparencia en relación a la Protección de Datos Personales. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/proteccion_de_datos_web.pdf>

Consejo para la Transparencia, Dirección de estudios. Cuaderno de Trabajo N° 15: Protección de Datos Personales en la era de la Economía Digital. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Economi%CC%81a-digital-V4.pdf>

Consejo para la Transparencia. Unidad de estudios y publicaciones. 2015. Cuaderno de trabajo N° 3. Protección de datos personales en el manejo de datos de investigación realizado por organismos públicos. [En línea] <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/proteccion_datos_final.pdf>

Entel. 2019. Política de Privacidad Clientes Entel. [En línea] <https://www.entel.cl/legales/pdf/Pol%C3%ADtica-de-Privacidad-Clientes-Entel.pdf>

European Commission. Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation. [En línea] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264>

GARRIDO, Romina, MATUS, Jessica, RAYMAN, Danny y BECKER, Sebastián, en Datos Protegidos. Datos personales e influencia política en Chile. [En línea] <https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf>

JIJENA, Renato. 2013. Tratamiento de datos personales en el Estado y acceso a la información pública. *Revista Chilena de Derecho y Tecnología.* Vol. 2. n. 2. [En línea] <https://rchdt.uchile.cl/index.php/RCHDT/article/view/30309>

Malhotra, Naresh K. Investigación de mercados, Pearson, quinta edición, 2008.

MAQUEO RAMIREZ, María Solange; MORENO GONZALEZ, Jimena y RECIO GAYO, Miguel. 2017, Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Rev. derecho (Valdivia)*, vol.30, n.1, [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004>

Ministerio de Transportes y Telecomunicaciones. Resumen Ejecutivo y Plan de Acción Estudio de Satisfacción de Usuarios de Servicios de Telecomunicaciones. [En línea] <https://www.subtel.gob.cl/wp-content/uploads/2019/01/estudio_sat_diciembre_2018.pdf>

MONTECINOS GARCÍA, Alejandro. 2012. La sociedad de la información y el gobierno electrónico. *Revista chilena de derecho y tecnología.* Vol. 1 n 1. [En línea] <https://rchdt.uchile.cl/index.php/RCHDT/article/view/24029>

Organisation for Economic Co-operation and Development, 2013, The OECD Privacy Framework. [En línea] <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

Organización de Estados Americanos, AG/RES. 2842 (XLIV-O/14) Acceso a la Información Pública y Protección de Datos Personales. [En línea] <http://www.oas.org/es/sla/ddi/docs/AG-RES_2842_XLIV-O-14.pdf>

Organización de Estados Americanos, Ley Modelo Interamericana sobre protección de Datos Personales (en elaboración). [En línea] <http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp>

PECES-BARBA, Gregorio, Curso de Derechos Fundamentales Teoría General, Imprenta de la Universidad Carlos III de Madrid.

QUEZADA RODRÍGUEZ, Flavio, 2012, La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile, *Revista Chilena de Derecho y Tecnología*, Universidad de Chile, Vol. 1 N°1.

RUBINSTEIN, Ira S., NOJEIM, Gregory T., LEE, Ronald D. 2014. Systematic government access to personal data: a comparative analysis. *International Data Privacy Law,* Vol. 4. n. 2. p. 98. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipu004>

SANZ SALGUERO, Francisco. 2016. Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. *Revista ius et praxis.* Vol. 22. n. 1. p. 372. [En línea] <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122016000100010&lng=es&nrm=iso>

SOLÉ, Juli. 2019. Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo.* n. 50.

Subsecretaría de Telecomunicaciones. MTT entregó resultados de estudio de satisfacción de usuarios en telecomunicaciones: internet fijo es el servicio peor evaluado. [En línea] <https://www.subtel.gob.cl/mtt-entrega-resultados-de-estudio-de-satisfaccion-de-usuarios-de-telecomunicaciones-internet-fijo-es-el-servicio-peor-evaluado/>

Subsecretaría de Telecomunicaciones. Quienes Somos. [En línea] <https://www.subtel.gob.cl/quienes-somos/>

TAZNOU, Maria. 2013. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law.* Vol. 3. n. 2. P. 99. [En línea] <https://doi-org.uchile.idm.oclc.org/10.1093/idpl/ipt004>

UN E-Government Knowledgebase. What is e-government. [En línea] <https://publicadministration.un.org/egovkb/en-us/about/unegovdd-framework>

VIOLLIER, Pablo, 2017, El Estado de la Protección de Datos Personales en Chile. [En línea] <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

Referencias a normativa chilena

Constitución y leyes

Constitución Política de la República.

Ley N° 19.628 sobre Protección de la Vida Privada.

Ley N° 18.168 General de Telecomunicaciones.

Decreto Ley N° 1762, de 1977, que crea la Subsecretaría de Telecomunicaciones dependiente del Ministerio de Transportes y organiza la dirección superior de las telecomunicaciones del país.

Ley N° 19.469 que Establece normas sobre Protección de los Derechos de los Consumidores.

Ley Orgánica Constitucional N° 18.575 de Bases Generales de la Administración del Estado.

Tratados internacionales

Declaración Universal de Derechos Humanos.

Declaración Americana de los Derechos y Deberes del Hombre.

Pacto Internacional de Derechos Civiles y Políticos.

Convención Americana de Derechos Humanos.

Proyectos de ley

Proyecto de reforma constitucional, que consagra el derecho a la protección de los datos personales. Ingreso de Proyecto. Boletín N° 9.384-07.

Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11144-07.

Referencias a actos administrativos

Ministra de Transportes y Telecomunicaciones

Resolución de la Ministra de Transportes y Telecomunicaciones, de 24 de septiembre de 2018, en autos Rol N° 10.629-2018.

Resolución de la Ministra de Transportes y Telecomunicaciones, de 24 de septiembre de 2018, en autos Rol N° 10.628-2018.

Subsecretaría de Telecomunicaciones

Oficio circular N° 108/DAP N° 47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 mayo 2018, que solicita base de números telefónicos de clientes de telefonía móvil para estudio de satisfacción de usuarios de telecomunicaciones y fija plazo.

Oficio circular N° 106/DAP N°47.182/F-67 de la Subsecretaría de Telecomunicaciones, de 16 de mayo de 2018, que solicita base de números telefónicos de clientes de televisión de pago para estudio de satisfacción de usuarios de telecomunicaciones y fija plazo.

Ordinario N° 10629/DJ-3 N° 244, de la Subsecretaría de Telecomunicaciones, de 25 de junio de 2018, que formula cargo e imparte instrucciones bajo apercibimiento legal.

Ordinario N° 10628/DJ-3 N° 244, de la Subsecretaría de Telecomunicaciones, de 25 de junio de 2018, que formula cargo e imparte instrucciones bajo apercibimiento legal.

Informe Técnico N° 26655/F-67, de fecha 18 de junio de 2018, de la División de Fiscalización de la Subsecretaría de Telecomunicaciones.

Informe Técnico N° 26658/F-67, de fecha 18 de junio de 2018, de la División de Fiscalización de la Subsecretaría de Telecomunicaciones.

Resolución Exenta N° 1.079, de la Subsecretaría de Telecomunicaciones, de 1 de junio de 2018, llamado a licitación pública, aprobación de bases y sus correspondientes anexos, de la Subsecretaría de Telecomunicaciones, del 01 de junio de 2018

Contrato suscrito entre la Subsecretaría de Telecomunicaciones del Ministerio de Transportes y Telecomunicaciones y Consultores Asociados de marketing CADEM S.A., el 10 de agosto de 2018.

Contraloría General de la República

Contraloría General de la República, Dictamen N° 25682 del 27 de septiembre de 2019.

Contraloría General de la República, Dictamen N° 8113 de 20 de abril de 2020.

Consejo para la Transparencia

Resolución exenta N° 304 del Consejo para la Transparencia, de 2020, que aprueba 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 Sustituye texto que indica.

Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado, 2011.

Sentencia del Consejo para la Transparencia de fecha 26 de octubre de 2010, en la causa Rol N° C-611-2010.

Referencias jurisprudencia judicial

Sentencias de Corte de Apelaciones

Sentencia de la Corte de Apelaciones de Valdivia, del día 21 de marzo de 2019, en autos rol N° 379-2019 caratulados Soto/Yoliquido S.A. p. 5.

Sentencia de Corte de Apelaciones de Santiago, de 27 de mayo de 2019, en Causa Rol N°2095-2019, caratulado Entel Telefónica Local S.A./Ministerio de Transportes y Telecomunicaciones.

Sentencia de Corte de Apelaciones de Santiago, de 27 de mayo de 2019, en Causa Rol N°2811-2019, caratulado Entel PCS Telecomunicaciones S.A./Ministerio de Transportes y Telecomunicaciones.

Sentencias de Corte Suprema

Sentencia de Corte Suprema, de fecha doce de noviembre de 2019, en Causa Rol N°14607-2019, caratulada Fisco CDE. (Palma)

Sentencia de Corte Suprema, de fecha doce de noviembre de 2019, en Causa Rol N°14609-2019, caratulada Fisco C.D.E. (Entel PCS Telecomunicaciones S.A. con Ministerio de Transporte y Telecomunicaciones).

Sentencia Corte Suprema, de 19 de julio de 2018. Causa Rol N° 2479-2018, caratulada Muñoz/Televisión Nacional de Chile.

Referencias a normativa internacional

Normas de la Unión Europea

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Disponible en línea en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?d1e3109-1-1=&uri=CELEX%3A32016R0679>

Carta de los Derechos Fundamentales de la Unión Europea. Disponible en línea en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A12012P%2FTXT>

Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. Disponible en línea en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012E&from=EN>