UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

ESTADO SITUACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE, REGULACIÓN JURÍDICA Y ALCANCES.

TESIS PARA OPTAR AL GRADO DE
MAGISTER EN GESTIÓN Y POLÍTICAS PÚBLICAS

TANIA ISABEL BARRERA QUINTANILLA

PROFESOR GUIA:
ALVARO AGUSTÍN VÁSQUEZ VALDIVIA

MIEMBROS DE LA COMISIÓN:
LORENA DONOSO ABARCA
MARÍA PÍA MARTIN MUNCHMEYER

SANTIAGO DE CHILE
2013

RESUMEN DE LA TESIS
PARA OPTAR AL GRADO DE MAGISTER EN GESTIÓN Y POLÍTICAS PÚBLICAS
POR: Tania Isabel Barrera Quintanilla
FECHA: 2013
PROFESOR GUÍA: Álvaro Agustín Vásquez Valdivia

En el año 2009, sobresalió en los medios de comunicación un caso emblemático concerniente a la legislación chilena sobre la protección de Datos Personales. Sara Castro, una profesional diagnosticada con depresión, enfermedad catalogada bajo la cobertura GES, acudió a una sucursal de la Farmacia Cruz Verde para adquirir medicamentos no relacionados con dicha enfermedad. Sara se encontraba inscrita en la Isapre Banmédica y a la vez, ésta institución sostenía un convenio con dicha farmacia para hacer efectiva la asignación de medicamentos, trasladando datos sensibles, como el diagnóstico médico de los afiliados, situación que se descubrió a raíz de la participación de Sara Castro. El dependiente de la farmacia le explicó que los descuentos en medicamentos solo eran efectivos para tratar su depresión, situación que ocurrió de forma pública frente a los demás clientes. Sara Castro observó no sólo como el vendedor hacía pública su enfermedad, sino que los datos personales catalogados como sensibles y confidenciales de su estado de salud, entregados y resguardados por la Isapre, se encontraban en manejo de una red de farmacias, a quien no había otorgado permiso alguno para el tratamiento de dicha información.

Este caso demostró la ineficiente protección de datos personales que se observa en Chile, no obstante tener una ley especial en la materia. Paradójicamente, Chile fue una de las primeras naciones de Latinoamérica en redactar un cuerpo legal que busca salvaguardar el tratamiento de los Datos Personales, con la promulgación en agosto de 1999 de la Ley 19.268, también conocida como "Sobre la Protección de la Vida Privada".

Con el tiempo, Chile ha promulgado una serie de leyes complementarias y reformas que buscan generar un mayor marco de protección de los Datos Personales. Un ejemplo de esto es la reciente puesta en marcha de la Ley 20.575 intitulada "Establece el Principio de Finalidad en el Tratamiento de Datos Personales", más conocida como Ley Dicom. No obstante, estas medidas no se encuentras acorde con el veloz avance de las tecnologías de información y comunicación así como del comercio, siendo posible la producción múltiple de nuevos casos en cuanto al inadecuado tratamiento de Datos Personales.

Asimismo, resalta el hecho que en el año 2010, Chile ingresó a la OCDE (Organización para la Cooperación y el Desarrollo Económicos). Dicha Organización posee una serie de Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales para que sean retomados por sus miembros. De igual forma se encuentran lineamientos sobre el tema emitidos por organizaciones internacionales, como la Directiva 95/46/CE del Parlamento Europeo y del Consejo, las Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados y las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.

El presente estudio, es de carácter descriptivo y cualitativo. Primeramente se establece un marco conceptual con la finalidad de establecer los conceptos básicos así como la pertinencia e importancia del tema de Protección de Datos, los retos existentes en torno al avance tecnológico y de las múltiples relaciones comerciales entre países, posteriormente efectúa un análisis comparativo de las directrices antes mencionadas con la legislación chilena, permitiendo determinar brechas que requieren una corrección urgente. El análisis del caso de Sara Castro, demuestra las actuaciones de los involucrados, abordando deficiencias en cuanto a la protección actual, y posible *trade off* para asegurar la cobertura de salud y la protección de datos sensibles.

DEDICADO A.

Mi ángel desde siempre, mi amada Rhibel, mi madre.

AGRADECIMIENTOS.

Amigos como Kristin, Mauricio, Ricardo, Martina, Jana, Alex y Marcela, quienes de diversas formas me apoyaron y animaron en la elaboración de este documento.

Compañeros del Magíster, por los momentos compartidos y las experiencias adquiridas durante el tiempo que viví en Chile.

A mis profesores Álvaro Vásquez, Lorena Donoso y María Pía Martin, por su continuo aliento en la realización de esta tarea.

TABLA DE CONTENIDO.

I. INTRODUCCIÓN.

Bajo el contexto de la sociedad de la información, la conjunción de la tecnología, comunicaciones e información han introducido y continúan incorporando cambios significativos en la vida cotidiana de las personas e instituciones. Es por todos conocido, que las tecnologías de la información y comunicación (TIC) facilitan la recolección, procesamiento, almacenamiento, recuperación y comunicación de grandes cantidades de datos, en ese sentido han trascendido de tal forma que hoy conforman un medio imprescindible en la actuación y actividades de las empresas, gobiernos y de los diversos actores de la sociedad, apoyando de forma significativa el crecimiento acelerado de la globalización. (Rico Carillo, 2007; 147).

El desarrollo de las técnicas de la informática ha permitido la creación de grandes bancos de datos que almacenan, entre otra información, aquellos de carácter personal, por lo que aunado a la alta competitividad que impera en las empresas de Chile y en concordancia con el despliegue y crecimiento de los servicios del gobierno electrónico, surge la necesidad de invertir y desarrollar sistemas de información automatizados para la atención de los requerimientos organizacionales y productivos. (Matus Arenas y Montecinos García, 2006).

Bajo tal aspecto, se afirma que las TIC han mejorado el logro de las diversas y complejas metas propuestas por el hombre moderno, sin embargo, y a pesar de los beneficios que la tecnología proporciona, no se presenta un adecuado manejo de la información, la cual puede verse afectada vulnerando derechos al ser compartida ó modificada sin el consentimiento expreso de su titular. Este fenómeno se ha originado, por el desconocimiento que tienen las personas sobre el tratamiento de sus datos personales. Cabe recalcar que un tratamiento inadecuado puede constituirse en una invasión a la privacidad de las personas.

Como una medida para prevenir este tratamiento ilegal e inadecuado de información, diversas legislaciones internacionales están preocupadas de este tema dentro del derecho actual.

Ejemplos de estos textos son la Directiva 95/46/CE de la Comunidad Europea, las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, las Directrices de la ONU para la regulación de los archivos de datos personales informatizados y las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.

El interés en mención por la protección de datos que se encuentra en las legislaciones internacionales, se ha recogido también en América Latina donde la protección de este bien jurídico no sólo se encuentra en códigos internos ó legislación secundaria, sino también en sus respectivas constituciones.

A manera de ejemplo citamos la legislación Colombiana, cuya Constitución en su artículo 15 recoge el derecho a la intimidad personal y familiar de las personas, debiendo el Estado respetarlos y hacerlos respetar, así como el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, especificando que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

A partir de dicho precepto constitucional, Colombia emitió la Ley Estatuaria[1] No. 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, Ley que según el artículo 1, "(…) *tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países".*

La protección de datos personales tiene una relación directa con el derecho a la vida privada y la intimidad. En la actualidad es posible afirmar que se ha convertido en un derecho autónomo, lo que implica que cada persona tiene la posibilidad de tutelar y salvaguardar la circulación de aquellos datos que le conciernen. De esta forma, la protección de datos personales se convierte en un elemento esencial de un ciudadano que vive inmerso en una sociedad donde la información y la comunicación adquieren cada vez más importancia, teniendo un desarrollo sin precedentes.

Esta protección de datos personales, por tanto, se orienta a una utilización legítima de las bases de datos. En el último tiempo, las bases de datos, tanto públicas como privadas, han realizado intercambios de datos de forma masiva, desmedida e invasiva contra la privacidad de las personas. Datos tan sensibles como el historial clínico, la situación financiera, las convicciones políticas o religiosas y la vida sexual, se encuentran almacenados frecuentemente en sistemas tecnológicos que presentan un control débil sobre esos datos, permitiendo que una violación a estos sistemas haga pública información que se refiere a la vida privada, amenazando así el derecho de la intimidad de los afectados.

El Derecho de privacidad se encuentra de forma explícita en casi todas las constituciones de la región. Textos como el Pacto de San José de Costa Rica y la Declaración Universal de los Derechos Humanos también lo incluyen en su articulado. El primer texto la incorpora en el artículo 11 y el segundo texto en el artículo 12, como una protección de la Honra y de la Dignidad, al indicar que Nadie será objeto de interferencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y a su reputación.

Chile no ha estado ajeno a esta discusión. En Chile la Protección de datos personales encuentra su sustento en una garantía constitucional. El artículo 19 No. 4 de la carta fundamental expresa: *"La Constitución garantiza a todas las personas (...) El respeto y protección a la vida privada y a la honra de la persona y su familia".* Bajo este principio, se puede reforzar que todo aquel dato personal que pertenezca a la vida privada de la persona debe respetarse y protegerse. Tratándose de una persona natural, cuando su información sea transada en contravención a este precepto deberá recurrir al Habeas Data, sin que proceda un "Recurso de Protección".

El Habeas Data permite ejercitar el derecho a la cancelación, bloqueo y gratuidad en todas aquellas operaciones ligadas al tratamiento de datos.

[1]De Acuerdo con el Congreso de la República de Colombia, las Leyes Estatuarias, son aquellas que la Constitución establece taxativamente. Tienen una categoría superior a las demás clases de leyes y se establece un trámite especial para su expedición por su importancia jurídica. Para su aprobación requiere mayoría absoluta y revisión previa por parte de la Corte Constitucional.

En efecto, en la legislación chilena, desde 1999, se encuentra vigente una ley específica que regula el tratamiento de datos personales. Se trata de la Ley No. 19.628 titulada "Sobre la Protección de la Vida Privada". A esta ley se le han incluido una serie de enmiendas y reformas para fortalecer la protección de los datos personales de la mejor forma posible. Dos últimos proyectos de ley se encuentran en estudio en el Congreso, bajo números de boletín 7831-07 y 8143- 03, los cuales buscan endurecer las penas y multas de quien hiciere uso ilegal y sin consentimiento de datos de carácter personal.

Existen, a su vez, otra normativa complementaria donde es posible destacar el Reglamento del Registro de bancos de datos personales a cargo de organismos públicos, que está contenido en el Decreto No. 779 del Ministerio de Justicia; como otras normas dispersas que se refieren relativas a la protección de datos personales en el ámbito de las obligaciones económicas, financieras, bancarias o comerciales.

Sin embargo, y dada la relevancia a nivel internacional del tema de la privacidad y protección de datos, Chile ha incluido diversos instrumentos, mecanismos y recomendaciones que favorecen la generación de transacciones de datos confiables. Tal es el caso del Acuerdo de Asociación Económica, Concertación Política y Cooperación firmado entre Chile y la Comunidad Europea, que en su artículo 30, se refiere a la protección de datos.

Otro acuerdo internacional importante en Chile, es el firmado con la Organización para la Cooperación y el Desarrollo Económico (OCDE) en el año 2010. Al momento de que Chile se incorpora como trigésimo primer miembro al "Club de los países Desarrollados", debe respetar y cumplir los documentos de la OCDE, entre los que se destacan las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.

En ese sentido, observando la importancia del tema de la protección de datos personales en Chile, el presente estudio de caso tiene como finalidad exponer su tratamiento y aplicación, mediante un caso emblemático y de alto impacto. Se trata de la transferencia de datos personales referentes a una patología de un usuario, desde una Isapre a una cadena farmacéutica. Esta transferencia no contó con el consentimiento de la persona afectada. Este caso pone, además, en debate los tratamientos y mecanismos de salvaguarda de datos personales de las autoridades gubernamentales en quienes recae la obligación de normar y fiscalizar este tipo de procedimiento.

II. METODOLOGÍA.

El enfoque utilizado en el estudio de caso es de carácter descriptivo y cualitativo.

Para lo anterior, se realizó una sistematización de la información teórica que revela la importancia de una adecuada legislación de protección de datos personales.

Posteriormente, se realizó un levantamiento de las directrices y lineamientos indicados por organismos internacionales vanguardistas.

De igual forma, se previó efectuar entrevistas con actores relevantes vinculados a la propuesta de reforma a la legislación chilena, con la finalidad de proceder a efectuar un análisis de la misma, sin embargo, únicamente se concretó una entrevista al diputado, señor Pedro Araya, debido a que otros miembros del Congreso Nacional -entre diputados y senadores- a quienes se solicitó entrevistar, no pudieron atender la solicitud, manifestando diversas razones para su excusa.

Finalmente, se encontrará un caso emblemático en cuanto al tratamiento de datos personales, sobre la base de su impacto y la actuación de los organismos del Estado que debieran hacerse parte en la mitigación en este tema. Cabe resaltar que se previó entrevistar a la señora afectada, a los representantes de las empresas y autoridades vinculadas al caso, pero la gestión fue denegada.

A partir de la información sistematizada se extraen conclusiones que permitan incidir en la importancia de reformar la legislación chilena, considerando prudente puntualizar, que el presente estudio realizará un repaso de la evolución de esta legislación, así como del estado actual en este campo.

CAPITULO I.
MARCO CONCEPTUAL PARA LA PROTECCIÓN DE DATOS PERSONALES.

Para desarrollar el tema en cuestión, se requiere en primer lugar definir los conceptos básicos presentes tanto en las legislaciones internacionales como legislación interna. Se buscará por tanto, explicar y definir de forma clara y puntual los conceptos que han desarrollado tanto los estudios académicos, como la jurisprudencia sobre esta materia.

En primer lugar creemos necesario definir el concepto jurídico de intimidad, dado que este es la base que nos permitirá comprender cómo el tratamiento de los datos personales afecta directamente este bien jurídico.

1. Concepto Jurídico de Intimidad y Derecho de Autodeterminación Informativa.

La protección de datos personales ha presentado un origen muy distinto en las legislaciones de los diversos países. Sin embargo, si analizamos su historia, descubriremos que el concepto jurídico de intimidad fue expuesto por los abogados Samuel D. Warren y Louis D. Brandeis, en la obra "The Rigth to Privacy", publicada en 1890, en la Harvard Law Review. En este texto se delimitó como el derecho a la soledad y se sugirió una garantía frente a cualquier invasión privada o doméstica.

Bajo esta óptica, se discutió la facultad de cada persona de mantener un ámbito de privacidad, donde pudiesen controlar aquella información que no debía conocerse por terceras personas, desarrollándose así una corriente de protección al individuo, donde ya se mencionaba una nueva expresión jurídica: el derecho de privacidad o intimidad.

Posteriormente, este "nuevo derecho" fue reconocido por la jurisprudencia del Tribunal Supremo Federal de los Estados Unidos de Norteamérica como el derecho "To be let alone", es decir "ser dejado solo", obteniendo así la protección de la vida interior y de su privacidad. [2]

Por tanto, la evolución del concepto de intimidad, de conformidad a lo expuesto por los referidos autores, se trata de un derecho subjetivo referido al ámbito propio del ser humano, el cual es un presupuesto para la libre realización de la personalidad y en cuya manifestación al exterior es posible ejercer control, encontrándose cubierto de una protección jurídica.

El autor Enrique Becerra Palomino, en un artículo sobre "Derechos a la Intimidad", indica que la protección de la privacidad debe ser entendida como el "Derecho Secreto" lo que es amplio ya que incluye no sólo aspectos o manifestaciones de la vida particular del sujeto, sino también impone una actitud de prudente discreción, a efecto de no atentar contra las costumbres o sentimientos concernientes a esa vida intima. En tal sentido, el derecho a la intimidad tutela no sólo la reserva de la persona en cuanto a lo que concierne a un ser como psicofísico, sino también aquellos aspectos que son inherentes a sus comunicaciones, relaciones afectivas más profundas y cercanas, y todo el entorno en el que desarrolla su existencia como individuo. [3]

De conformidad con Diego Fabio Piacenza en el artículo el Derecho a la Intimidad y los Medios de Comunicación, establece que, "El Dr. Cifuentes, englobando la esencia conceptual de la figura, define a los derechos personalísimos como "derechos subjetivos privados, innatos

[2] El objetivo de la obra fue establecer un límite jurídico al derecho de la intimidad por la injerencia de los medios de comunicación.
[3] Lo relativo al autor a través de la obra "Conflicto entre Intimidad y Libertad de Información" de Aldo Vásquez.

y vitalicios que tienen por objeto manifestaciones interiores de la persona y que, por ser inherentes, extra patrimoniales y necesarios, no pueden transmitirse ni disponerse en forma absoluta y radical".

Cabe señalar que existe una confusión en esta materia. Algunos juristas y académicos usualmente distinguen dos dimensiones, la vida privada y la vida pública ó la vida íntima y la vida pública. Asimismo, tampoco ha existido una diferenciación de los conceptos de intimidad y privacidad, que si bien son similares, presentan distintos niveles de análisis.

Para el académico Carlos Soria[4] estas categorizaciones son insuficientes y restrictivas, por lo que sugiere definir tres esferas en la vida humana: una dimensión íntima, una dimensión privada y una dimensión pública. Cada una de estas esferas tiene una importancia trascendental no sólo para el ser humano, sino para definir qué información puede ser compartida y bajo qué criterios.

En primer lugar, la esfera intima se refiere a aquella área que se desea dejar fuera del escrutinio público. Es el deseo de soledad, de no compartir con otros aquello que se encuentra en lo más profundo de la persona, como los sentimientos, la vida familiar, las amistades, el amor¸ etc.

Se resalta que la intimidad se destruye en el mismo momento que es compartida. Este acto de compartir lo más íntimo de la persona se realiza en situaciones extremas y sólo cuando la persona lo hace libre y voluntariamente. *A esta esfera corresponderían datos tan sensibles como el estado civil de la persona, su estado de salud, su sexo, entre otras.*

Un segundo ámbito corresponde a lo privado, donde recaen aquellas acciones que la persona realiza en espacios reservados y/o restringidos, y que desea mantener en secreto o lejos de la vista y opinión pública. Asimismo esta persona solo hará público estas acciones o información con su consentimiento explícito. Sin embargo, existen algunas excepciones donde información referida a la esfera privada podría divulgarse sin el consentimiento del afectado. Por ejemplo, algunas de las legislaciones encargadas de la protección de datos, no requieren el consentimiento de la persona cuando se presentan casos extraordinarios en los que pudiera verse afectada la salud pública, la seguridad de la nación ó el orden interno.

La mayoría de los datos personales pueden ingresar en esta categoría, información como la filiación política, el trabajo, el lugar de residencia, es información que su titular puede no desear que se divulgue, ni que sea tratada sin su consentimiento mínimo.

Por último, tenemos el ámbito de lo público. En esta esfera todo debiese comunicarse e informarse. A este ámbito corresponde datos que nos identifican como nuestro nombre, sin embargo, aún así, el tratamiento de datos personales debe cuidar que la identidad de las personas no se comparta si no ha existido el consentimiento explícito de la persona y sólo si el uso de esta información de carácter público se realizara cuando el sujeto tiene clara conciencia de su finalidad.

Este espacio público está directamente ligado a la llegada de la sociedad en masas, donde la información muchas veces no posee límites definidos, y amenaza y perturba las esferas íntima o privada del sujeto, lesionando, a su vez, el ámbito de la inviolabilidad de la personalidad individual.

[4] La información de lo público, lo privado y lo íntimo. Carlos Soria. Valladolid, 1936. Director del Departamento de Ética y Derecho de la Información. Universidad de Navarra.

Ahora bien, con los avances tecnológicos existentes, encontramos un tipo de expresión al derecho a la intimidad, que se define como el derecho a la autodeterminación informativa. La Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador, señala en la sentencia definitiva de fecha tres de marzo de dos mil cuatro, emitida en el proceso de Amparo con referencia 118-2002 que, el derecho a la autodeterminación informativa es una manifestación del derecho de la intimidad. Indicándose que si la intimidad personal hace referencia al ámbito que se encuentra reservado *al interior* de cada persona, en el ámbito informático tal derecho implica la protección de todo individuo frente a la posibilidad de acceso a la información personal que se encuentre contenida en bancos informatizados.

Y es que según la Sentencia en comento, el derecho a la autodeterminación informática o derecho a la intimidad informática *es aquel que tiene por objeto preservar la información individual que se encuentra contenida en registros públicos o privados, especialmente la almacenada a través de los medios informáticos, frente a su utilización arbitraria. De modo que a partir del acceso a la información, exista la posibilidad de solicitar la corrección, actualización, modificación y eliminación de los mismos.*

El derecho en referencia implicaría la posibilidad y facultad de toda persona a controlar, de forma razonable, la transmisión o distribución de la información personal que lo afecte o que le pudiere afectar en el futuro.

Hoy en día, con el desarrollo y uso masivo de las tecnologías de información y comunicación, TIC, se otorga una mayor urgencia a la necesidad de proteger y salvaguardar la intimidad, pareciendo que para la adecuada regulación de datos personales, se debe partir del acontecimiento de un suceso relevante de invasión a la privacidad, para que la entidad encargada de emisión de leyes tome la decisión de proteger el derecho a la intimidad a través de una ley de protección de datos personales, teniendo por bien jurídico protegido la autodeterminación informativa, que abarca la reserva y control de la información de carácter personal en aras de la preservación de la propia identidad, dignidad y libertad, lo que se ha dado en denominar "derecho de la tercera generación"[5].

Adicionalmente a lo anterior, es necesario resaltar que las legislaciones sobre la materia, no solo deben procurar regular clasificar aquella información privada que el titular desea compartir, sino también, debe establecer e incorporar los mecanismos necesarios para que la protección de estos datos personales, no implique un posible riesgo el mal uso de éstos.

2. El tratamiento de Datos Personales.

Los datos personales son una parte esencial de la esfera íntima y privada de la persona. Un mal uso de estos no sólo permite identificar a una persona, sino también entregan datos sensibles de la vida privada a terceros que acceden a ellos sin el consentimiento del afectado.

Retomando nuevamente la Sentencia antes mencionada, se advierte que existe una manifestación del derecho a la intimidad, que es precisamente el derecho a la protección de

[5] (…) las novedades informáticas y telemáticas están obligando a una nueva clasificación de los derechos fundamentales, no bastando la distinción entre derechos individuales o libertades y derechos sociales o prestacionales, naciendo así derechos o libertades llamados de "tercera generación", constituidos por las garantías de los individuos frente a la contaminación o deterioro que las libertades pueden sufrir por las nuevas tecnologías. Entre esos derechos se incluirían el secreto de las comunicaciones informáticas y telemática, la intimidad informática y el derecho a la autodeterminación informativa, formando un conjunto que me atrevería a denominar de "libertades informáticas". MARTINEZ ESCRIBANO, ALFONOS. "Los Derechos Fundamentales y las nuevas tecnologías en el trabajo". Fuente: Matus Arena y Montecinos García. "La Cesión de Datos Personales".

los datos y consiste en que el individuo pueda controlar el uso o tratamiento de los mismos, a fin de impedir una lesión a su esfera jurídica.

El concepto de protección de datos personales puede definirse como "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento autorizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad". (Davara Rodríguez, 2004:3).

Al analizar esta definición, el jurista Emercio Aponte identifica aquellos elementos claves que la integran. Por un lado, tenemos al "ciudadano", en otras palabras, la persona natural ó física a quien pertenece la información que será automatizada.

En segundo término encontramos, el concepto fundamental "los datos personales", es decir toda la información que pertenece a un sujeto, que lo hace identificable y que puede ser tratada de forma automatizada.

Otro elemento es el denominado "Tercero" que se refiere a toda persona natural o jurídica que sola o en forma conjunta es la encargada de realizar el tratamiento de datos personales. Aquí es importante señalar que un tercero si podría ser una persona jurídica, mientras que el ciudadano es necesaria y únicamente una persona natural.

Muy ligada al concepto anterior se encuentra la palabra "Tratamiento" que identifica la acciones u operaciones, sean manuales o automatizadas, que recogen, graban, conservan, modifican, elaboran, bloquean, cancelan o ceden datos de carácter personal.

Es importante recalcar que el tratamiento de datos, no sólo se refieren a los procesos de carácter automatizado, sino también a aquellos de origen manual. Este detalle es importante, dado que se debe proteger también los ficheros manuales, dado que podrían ser automatizados en el futuro, y hasta que eso no ocurra, los datos recogidos requieren de una protección mínima independientemente de la forma en que son almacenados y tratados.

La protección de datos personales, señala el jurista Emercio Aponte, "*busca garantizar la privacidad de las personas, el resguardo y protección de su intimidad de las personas, lo cual supone fundamentalmente, la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a los datos personales de cada individuo, y la facultad de oponerse a su utilización, de manera tal de impedir que esa información sirva a propósitos no aceptados por su titular".*

Asimismo, y siguiendo la línea argumental de Aponte, podemos afirmar que la protección de datos personales descansa en cinco principios fundamentales ó rasgos característicos, que sirven de sustento jurídico a este concepto. Estos principios son de carácter transversal, por lo que se encuentran en la mayoría de las legislaciones nacionales que protegen el bien jurídico de la identidad de las personas y los datos que permitieren que ésta se hiciese pública.

El primer principio es fundamental y consiste en que *"el titular de los datos entregue su consentimiento".* Esta persona es la única que tiene la facultad de decidir qué datos quiere compartir, a quién y cuándo los quiere entregar y cuál será el destino de esta información. Este consentimiento debe ser explicito, claro e inequívoco.

En segundo término, se encuentra el principio de la *"Calidad de los datos".* Se busca, por tanto, que los datos que serán objeto de tratamiento, sean pertinentes, adecuados y que no

excedan las finalidades por las cuales estos datos fueron recogidos. Asimismo, la calidad de los datos está íntimamente ligada con la actualización permanente de esta información.

El tercer principio de, *"Información en la recolección de datos",* por su parte, consiste en la obligación del responsable del tratamiento de datos, de informar al titular de esa información, previamente a que los datos se utilicen, sobre qué información se guardará en los ficheros, cuál será la finalidad del tratamiento y a qué destinarios se entregarán los datos personales.

Asimismo, el titular tiene la facultad de abstenerse de entregar su información personal o responder cierto tipo de preguntas por parte del encargado del tratamiento, como a su vez, posee el derecho de acceso, rectificación y cancelación de los datos personales que ha entregado.

En cuarto lugar, el principio de *"Cesión de datos",* expresa que sólo se comunicará esta información cuando el titular de esos datos entregue su previo consentimiento y sólo para cumplir con fines que se relacionan con las funciones propias de quien recibe esos datos y la persona que los entrega.

Por último, se encuentra el Principio de *"No Discriminación".* Este principio busca prohibir que los datos que se recaben, puedan originar una discriminación arbitraria, sobre todo aquella información que se refiera a la raza, color, vida sexual, creencia religiosa, afiliación política o cualquier otra ideología, creencia o convicción.

3. El flujo transfronterizo de Datos Personales.

Cabe destacar, que el tratamiento de datos no sólo se presenta a nivel interno, existe también un flujo internacional de información personal entre diversas instituciones y países, siendo este punto de vital importancia en las relaciones comerciales entre muchos países.

Matus Arenas y Montecinos García definen la Transferencia Internacional de Datos como: *"Un tratamiento que consiste en la transmisión o transporte de datos, fuera de un Estado, realizado por el responsable del tratamiento directamente a una persona natural (física) o jurídica, que los recibirá en un tercer país, para someterlos a un nuevo tratamiento de datos, bien sea o por cuenta propia o por cuenta del transmitente de los datos".*

Asimismo, sostienen que en este proceso de transmisión encontramos dos sujetos, quien envía los datos (exportador) y quien los recibe (importador). El exportador será el responsable del tratamiento de los datos personales transferidos, mientras que el Importador aceptará recibir del exportador una cantidad de datos, para desarrollar el respectivo tratamiento. Existe un tercer caso, donde el importador conviene en recibir los datos del exportador para realizar un tratamiento de datos personales, pero ésta acción se realizará con instrucciones entregadas por el exportador de los datos.

Un elemento importante al analizar las transferencias internacionales de datos, se relaciona por un lado con las legislaciones internacionales que, por un lado, protegen este flujo transfronterizo y, por otro, la capacidad que tenga quien reciba los datos de adecuarse a disposiciones jurídicas que velen por un tratamiento adecuado de estos datos.

Se encuentra, en primer lugar, el ejemplo de la Unión Europea. En el antiguo continente se ha logrado establecer un mercado común para los Estados miembros. Quienes integran la Unión Europea se ven obligados a garantizar la libre circulación de mercancías, personas, servicios,

capitales, y por último, los datos personales de un Estado miembro a otro. Derribar las fronteras que impedían el libre flujo de personas europeas de un país de la Unión a otro, requería necesariamente que algunos datos personales mínimos también realizaran un flujo transfronterizo para facilitar este traslado de las personas. Asimismo este libre flujo permitía favorecer los intercambios económicos entre diversas empresas e instituciones de dicho continente.

El caso de la Unión Europea nos permite apreciar que una legislación común para una región facilita el flujo transfronterizo, sin embargo no siempre se presentan estas situaciones. Muchas veces el flujo internacional de datos se da entre un país con una fuerte legislación de protección de datos personales a uno donde esta salvaguarda de la información es mínima o débil.

Cuando ocurre esta situación las legislaciones internacionales como la Directrices de la OCDE ó la Directiva 95/46/CE de la Unión Europea, recomiendan que esta transferencia sólo exista cuando se presente un nivel de protección adecuada en el país que recibe esa información, es decir que exista reciprocidad jurídica.

En términos de legislación internacional, el concepto *"Protección adecuada"* es fundamental. Por un lado, previene a los países a que el país que recibe los datos personales no sólo debe garantizar efectivamente una serie de principios básicos de protección de datos personales, sino también que se salvaguarde este derecho a través de un *organismo independiente y autónomo* con capacidad de sancionar y fiscalizar las infracciones que se cometan contra este bien jurídico, y de una legislación que defina y juzgue las violaciones a estos derechos, determinando las responsabilidades pertinentes.

Para complementar esta idea, se retoma el artículo 25 de la Directiva Europea que sugiere que se preste especial atención al nivel adecuado de protección de datos personales que ofrece un país tercero el cual, *"(…) se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

4. Globalización y Competitividad en la Sociedad de la Información.

En la actualidad el flujo transfronterizo de datos personales indiscutiblemente está relacionado con las denominadas tecnologías de información.

Las tecnologías de la información se definen como: *"Aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones." (Bologna y Walsh, 1997: 1).*

Se puede afirmar que el avance de las tecnologías de la información ha permitido muchas ventajas, como, por ejemplo, realizar acciones inmediatas, donde el tiempo y el espacio ya no son obstáculos para acceder a cierta información que se encuentra almacenada en internet y otros soportes no físicos.

Esta irrupción de las tecnologías de la información se ha dado en el marco de un mundo cada vez más globalizado.

Al consultar en distintas fuentes sobre la definición de Globalización, se infiere que no existe una definición claramente aceptada. Sin embargo, una aproximación podría ser el significado que entrega el Banco Mundial sobre este concepto, el cual es retomado para el presente caso. Este organismo explica que la globalización *"se relaciona con el hecho de que en los últimos años una parte de la actividad económica del mundo que aumenta en forma vertiginosa, parece estar teniendo lugar entre personas que viven en países diferentes (en lugar de en el mismo país)".*

Dicha entidad mundial indica que este aumento de la actividad económica transfronteriza se ha manifestado en tres áreas de la economía. Por un lado en el Comercio Internacional, por otro, en la Inversión Extranjera Directa, y finalmente, en el flujo del mercado de capitales, he aquí que se avista sobre la injerencia del tema en estudio para la economía de un país.

Asimismo y siguiendo el pensamiento de Daniels (1993), las compañías, en casi todas las empresas, adoptan una visión y estrategia global, en la medida en que se abran nuevas instalaciones productivas en todo el mundo y se exportan bienes nuevos en el mercado. De este modo, el desarrollo de las economías nacionales en los mercados globales ha impuesto nuevos desafíos y oportunidades para la participación en la integración trasnacional.

La dinámica del proceso de globalización se encuentra determinada, en gran medida, por el carácter desigual entre los actores participantes. Por ello en su evolución ejercen una influencia preponderante los gobiernos de los países desarrollados, así como las empresas trasnacionales, y en una medida mucho menor los gobiernos de los países en desarrollo y las organizaciones de la sociedad civil.

Bajo ésta perspectiva, nos enfrentamos a múltiples empresas mundiales que recolectan información inherente a la intimidad de las personas, ya sea para vincularlas a un mercado laboral o productivo, servicios empresariales a distancia o simplemente diversión y socialización.

Estas industrias, están convirtiéndose en uno de los impulsores más importantes del comercio y de la inversión extranjera directa en América Latina y el Caribe, lo que representa una importante oportunidad para la creación de empleo, difusión tecnológica, la innovación, y diversificación de las exportaciones de la región. Sin embargo estas industrias son las que generan grandes problemas por el tratamiento abusivo de los datos personales.

A manera de ejemplo citamos el caso de la empresa EQUIFAX[6], con sede en Atlanta, Georgia, Estados Unidos, entidad que opera desde hace más de un siglo, teniendo más de

[6] En Chile opera desde 1979, entregando servicios a más de 14 mil empresas de distintos sectores, principalmente financieras, comerciales, retail y servicios; que sumada a la experiencia global de EQUIFAX, agiliza las transacciones comerciales y otorga respaldo a la decisión, a los servicios de marketing e informes comerciales de personas naturales y jurídicas. EQUIFAX está presente en el ámbito de negocios ofreciendo soluciones para los más variados sectores de la economía.

Fuente: sitio WEB http://www.dicom.cl/efx/hcl.01/pag/p.efx.hcl.div-new-acerca-equifax.html.

6,900 empleados y presencia en 16 países de América del Norte, América Latina, Asia y Europa, empresa que forma parte del Standard & Poor's (S&P) 500® Index, cotizando sus valores en la bolsa de Nueva York bajo el símbolo EFX.

Dicha empresa recopila y consolida información personal de carácter económico, financiero, bancario y comercial, a través de diversas fuentes de acceso público y privado, obteniendo dicha información a través de fuentes públicas y privadas como las agencias de gobierno, las empresas que publican en los sistemas de información de dicha empresas respecto a las deudas morosas de las cuales son acreedores y los mismos consumidores que se contactan con Equifax Chile para solicitar cambios o actualizaciones en sus archivos de datos.

Castells (2005:1), advierte que la globalización apunta al mismo tiempo a la revolución tecnológica informacional, la cual constituye la base material de un proceso de transformación de forma multidimensional, incluyendo la evolución del sistema productivo, de la estructura social, de la cultura, de las instituciones y de la política.

De igual forma Ocampo (2008), indica que, algunos aspectos integrales de las agendas de reforma para los nuevos Gobiernos, ha sido la liberalización comercial y la consecuente integración a la economía mundial a partir de las ventajas comparativas, así como la apertura generalizada a la inversión extranjera directa.

En ese sentido, se determina que la globalización repercute en diversos ámbitos, para el caso puede ayudar o afectar la competitividad de un país en los mercados internacionales, ya que la distancia y tamaño son importantes debiendo construir activos y plataformas que hagan posible la incorporación y posicionamiento de la economía nacional.

En el texto, Colombia: estructura industrial e internacional de Luis Jorge Garay encontramos una definición pertinente sobre el concepto "Competitividad":

"Significa la capacidad de las empresas de un país dado para diseñar, desarrollar, producir y colocar sus productos en el mercado internacional en medio de la competencia con empresas de otros países. (Alic, 1997)".

Esta capacidad competitiva en una sociedad global en definitiva requiere del uso de las tecnologías de la información. De este modo, es posible sostener que los avances de la tecnología actual, nos permiten recoger y utilizar información desde el preciso momento en que ésta se genera, estos son los denominados procesos en línea. Este fenómeno ha cambiado radicalmente no sólo el cómo y dónde se trabaja y el lugar de trabajo, sino que también ha impactado en la forma en la que las empresas compiten. (Alter, 1999).

Con base a lo anterior, podemos afirmar que un país al tener una adecuada regulación e institucionalidad respecto al manejo de la protección de datos, le brinda obtener un mejor posicionamiento a sus empresas en el ámbito de competitividad tanto a nivel nacional como internacional, mejorando las relaciones comerciales existentes con otros países.

5. La seguridad del país. Institucional. Acuerdos Internacionales.

Hoy en día observamos, diversos debates sobre Internet y como dicha red tiene efecto sobre la privacidad y sobre la capacidad de control de nuestra vida íntima.

En ese sentido, se considera oportuno retomar lo expuesto por Manuel Castells en el artículo denominado *"La privacidad en Internet".* Al respecto, Castells indica que es posible advertir dos relaciones que surgen en dicha actividad: la relación gobierno-ciudadanos y la relación privacidad-internet.

Castells indica que en la primera, existe algo que no es posible aún para los gobiernos en la actualidad, y es el control verdadero y efectivo del internet. Esto se debe a diversas razones, en algunas ocasiones se ha mencionado que técnicamente es posible y en otras que no lo es. A modo de ejemplo encontramos el conocido caso de China y Singapur, ambos países se abrieron al exterior por razones estratégicas, económicas y financieras, utilizando la plataforma para negocios, China funcionó la restricción realizada, porque, aunque no controlan la difusión de información en internet, pueden posteriormente buscar a la persona que recibido o difundido la información y llevarla a tribunales, siendo una forma de control posterior. En Singapur dicha figura no funcionó ya que se intentó la utilización para fines comerciales sin menoscabar los derechos de los ciudadanos de libre difusión.

Sin embargo, Castells manifiesta que internet es tan difícil de controlar, teniendo no sólo una razón técnica para hacerlo sino también *institucional*. Así observamos el caso de Estados Unidos, donde no es posible realizar control alguno por decisiones diversas de los tribunales de justicia federales, resaltando la que eliminó el Acta de Decencia en la comunicación que el ex-Presidente Clinton presentó en 1995 para la censura de internet, argumentando la pornografía infantil.

El Tribunal Supremo de Estados Unidos, declaró que es cierto que en Internet hay toda clase de problemas, es cierto que en Internet la libre expresión conduce a excesos, es cierto que Internet es el caos de la expresión. Pero, añade textualmente: "los ciudadanos tienen un derecho constitucional al caos".

Adicionalmente al hecho actual que los gobiernos no controlan el internet, las personas están tomando conocimiento de que existe un problema mucho más profundo que el control de los gobiernos sobre la libertad de expresión, el cual es la desaparición de la privacidad de sus datos a través del mundo en el que vivimos conectados la red.

CAPITULO II.
LINEAMIENTOS INTERNACIONALES SOBRE EL TRATAMIENTO DE DATOS PERSONALES.

A nivel mundial existen diversas organizaciones encargadas de promulgar textos y avances en cuanto a la protección de datos personales, tenemos entre ellas a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, la Directriz sobre la protección de la vida privada y flujos transfronterizos de datos personales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados, las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana de la Red de Iberoamericana.

A continuación, se intentará retomar los aspectos más relevantes que cada documento posee.

1. Directiva 95/46/CE del Parlamento Europeo y del Consejo.

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo de la Comunidad Europea emitieron la Directiva 95/46/CE. Este texto se refiere específicamente al tratamiento de datos personales y a la libre circulación de estos datos.

La Directiva Europea enfatiza los objetivos fundamentales del Tratado de la Unión Europea. Estos objetivos se orientan a favorecer una unión más estrecha entre los pueblos que componen Europa; que se establezcan relaciones más fuertes entre los Estados que componen la Comunidad; asegurar, de forma colectiva, el progreso económico y social de este continente, eliminando, de paso, las barreras que dividen esta región; fomentar una mejora continua en las condiciones de vida de los pueblos; consolidar la paz y la libertad y promover un concepto de democracia que se base en los derechos fundamentales reconocidos en las constituciones y leyes de sus Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.

Para que estos objetivos se cumplan, la Directiva de la Unión Europea considera indispensable el cumplimiento de una serie de condiciones, como que, por ejemplo, los sistemas de tratamiento de datos personales estén al servicio del hombre y que, independiente de la nacionalidad y residencia, se respeten sus derechos fundamentales, específicamente el Derecho a la intimidad. Por otro lado, este documento recalca que el tratamiento de Datos Personales debe contribuir al progreso económico social, y a facilitar los intercambios y el bienestar de las personas.

Esta Directiva establece, además, que cada Estado miembro de la Comunidad Europea debe designar a una o varias autoridades públicas independientes en quienes recaerá la misión de controlar que se aplique en su respectivo país las disposiciones que se adopten por los Estados miembros con respecto a esta Directiva.

Asimismo, la Directiva se destaca por la creación de un grupo que protege a las personas en relación al tratamiento de sus datos personales. Específicamente este grupo tendrá como miembros a:

a) Representantes de las autoridades de control nacionales,
b) Representantes de las autoridades control de las instituciones,
c) Organismos Comunitarios, y
d) Un representante de la Comisión.

Un elemento interesante a destacar son los elementos legislativos de esta Directiva. Este texto se fija como objetivo principal la protección de los derechos y libertades en lo relativo al tratamiento de datos personales. Para cumplir con este planteamiento, la Directiva presenta no sólo una serie de alcances, excepciones, sino también la utilización de determinados recursos y la transferencia de datos.

Los alcances de la aplicación de este texto se aplican a las personas físicas, los datos personales que se refieran a éstas y, por último, el soporte donde se encuentran estos datos, recogiéndose ésta información tanto en medios automatizados, como en ficheros no automatizados o manuales.

Por otro lado, se establecen excepciones en la aplicación de esta Directiva. Estas excepciones se referirán, en primer término, a los datos efectuados por la persona física que se relacionen, exclusivamente, en el ejercicio de actividades particulares o domésticas; en segundo lugar también quedarán exentas aquellas actividades que no se encuentren comprendidas por el Derecho comunitario, entre las que se encuentran áreas como Seguridad Pública, la Defensa o la Seguridad del Estado.

En relación a la utilización de recursos, la Directiva propone que las legislaciones nacionales de los países miembros, contengan un recurso judicial que vele por aquellos casos donde un responsable del tratamiento de datos no respete los derechos de los interesados, para estos efectos se establece que estos recursos reparen el o los perjuicios que sufra una persona por el tratamiento ilícito de sus datos.

Por último, la Directiva permite y autoriza que se realice una transferencia de datos personales de un país miembros a una tercera nación, siempre que se garantice un nivel adecuado en el tratamiento de estos datos. En cambio, no se autorizarán las transferencias de datos a terceros países que no cuenten con un nivel de protección para los datos que se reciben, salvo excepciones que se recogen y se enumeran en dicho texto, es decir se establece un piso de garantías en cuanto al tratamiento de datos.

Cabe resaltar que la Directiva de la Comunidad Europea se basa en 10 principios esenciales.

El primer principio que recoge este texto es la *Calidad de los datos.* Con respecto a este punto, indica que el tratamiento de la información personal debe realizarse de forma leal y lícita, que su recolección sea con fines claros, precisos, explícitos y legítimos, y que los datos que se recojan sean exactos, y, en la medida de los posible, actualizados.

Un segundo principio presente en la Directiva se refiere a la *Legitimación del Tratamiento de los Datos Personales*. Este texto expresa que esta acción solo se efectuará si el interesado entrega el consentimiento en forma inequívoca o, si bajo ciertas circunstancias el tratamiento es esencial para la ejecución de un contrato, donde el titular de los datos personales es parte, o para el cumplimiento de una obligación jurídica donde se involucre el interesado. Asimismo se busca la protección del interés vital del titular de esos datos personales, el cumplimiento de una misión de interés público y, por último, la satisfacción del interés legitimo que persiga el responsable del tratamiento de estos datos.

Un tercer principio hace relación con las *Categorías especiales de Tratamiento* ó datos sensibles. En este punto se establece la prohibición del tratamiento de datos personales, si éste revela información sensible como el origen racial o étnico de la persona, sus opiniones políticas, sus creencias religiosas o convicciones filosóficas, la pertenencia a un sindicato u

organización gremial, como aquellos datos que se refieren a la salud del interesado o a su orientación sexual.

Para reforzar el punto anterior, se hace expresa mención a las reservas en su aplicación. Por ejemplo, si el tratamiento de estos datos personales se encuentra en directa relación con la salvaguarda del interés vital del interesado o para la prevención de una enfermedad o un diagnóstico médico.

En cuarto lugar, se encuentra el principio que establece la *entrega de información a los afectados de dicho tratamiento de datos personales.* Bajo este punto, establece que el responsable del tratamiento, le facilitará a las persona de quien se recojan los siguientes datos: la identidad del responsable del tratamiento de los datos, cuál es la finalidad del tratamiento de esta información, quiénes serán los destinatarios de los datos, entre otros.

Un quinto principio es *el derecho de acceso del interesado a sus datos.* Bajo este principio la persona que ha entregado sus datos, podrá exigirle al responsable del tratamiento de sus datos personales:

- La confirmación de que existe o no un tratamiento de los datos que le conciernen y que se le comunique qué datos personales están en tratamiento.

- La posibilidad de rectificar, suprimir o bloquear los datos cuyo tratamiento no se encuentre ajustada a las disposiciones de esta Directiva. Específicamente, cuando se presenten datos incompletos o inexactos, cómo en aquellos casos donde se notifique y comuniquen dichas modificaciones a los terceros que hacen un tratamiento de esos datos.

El sexto principio se refiere a las *excepciones y limitaciones* del tratamiento de la información. Bajo este punto, se estipula que se podrá limitar tanto el alcance de los principios relativos a la calidad de los datos, como la información del interesado y el derecho de acceso y la publicidad de estos tratamientos. Esta limitación está íntimamente ligada con la salvaguarda de, por ejemplo, la seguridad del Estado, la defensa nacional, la seguridad pública, la represión de infracciones penales y, finalmente, el interés económico y financiero importante que se refiera a un estado miembro de la Unión Europea o la protección del interesado.

El séptimo principio estipula *El derecho del interesado a oponerse al tratamiento.* De esta forma, el sujeto podrá oponerse, por razones legitimas a que los datos que le conciernen sean objeto de tratamiento. Asimismo, podrá oponerse- si realiza una petición previa y gratuita- al tratamiento de datos, respecto de los cuales se pudiese aplicar un tratamiento que se destine a la prospección. Por último, se le informará al interesado previamente, cuando sus datos se comuniquen a terceros a efectos de prospección y poseerá el derecho a oponerse a dicha comunicación.

El octavo principio se refiere a *la confidencialidad y la seguridad del tratamiento de los datos.* La redacción de este principio sostiene que toda persona que se encuentre bajo la autoridad del responsable o encargado del tratamiento de datos, solo podrán manejar datos personales a los que tengan acceso y sólo cuando sea por expresa orden del responsable del tratamiento de datos.

Asimismo, se estipula que el responsable del tratamiento de datos, deberá aplicar aquellas medidas que sean adecuadas para la Protección de Datos Personales contra eventualidades

como la destrucción accidental o ilícita de los datos, la perdida accidental de estos, la alteración de los datos personales y la difusión o el acceso no autorizado.

El noveno principio hace relación con la *notificación del tratamiento a la autoridad de control.* De este modo, se establece que el responsable del tratamiento de los datos, debe notificar a la autoridad encargada del control nacional de datos, previamente a la realización de un tratamiento de datos. Esta autoridad, a su vez, estará encargada de realizar comprobaciones previas, que especifiquen que los derechos y libertades de los interesados no se encuentran en riesgo, cada vez que haya recibido la notificación del encargado de los datos.

Finalmente, el décimo principio, hace relación con la *Publicidad,* estableciéndose así debiese procederse acorde a la publicidad de los tratamientos y que las autoridades de control deben llevar un registro claro y pertinente de los tratamientos notificados.

Para reforzar la aplicación de esta Directiva, la Unión Europea ha redactado una serie de informes complementarios. Entre estos, podemos destacar seis documentos.

El primer informe es el denominado COM (2007) 87, y que fue firmado en 7 de marzo de 2007. Se trata de una Comunicación de la Comisión al Parlamento Europeo y del Consejo. Este documentó no sólo examinó el trabajo que se había realizado para mejorar la aplicación de la Directiva sobre datos personales, sino también indicó las mejoras en la aplicación de esta Directiva, recordando, de paso, que todos los países miembros están observando este texto.

Asimismo, la COM (2007) 87 precisa que la Directiva no debiese sufrir modificaciones y sugiere que en el futuro se debe trabajar en torno a temas como los procedimientos oficiales de infracción; la comunicación interpretativa sobre ciertas disposiciones; la aplicación del programa de trabajo; el reforzamiento de una legislación sectorial para la Unión Europea, específicamente en el área de la evolución tecnológica; y la cooperación con socios exteriores, particularmente con Estados Unidos, del cual veremos que posteriormente surgió un acuerdo.

Un segundo informe de la comisión es el documento COM (2003) 265, con fecha 15 de mayo 2003 y que es el primer informe que versa sobre la aplicación de la Directiva 95/46/CE.

Este texto concluye que la Directiva ha cumplido su principal objetivo, dado que ha eliminado los obstáculos que impedían la libre circulación de datos personales entre los estados miembros de la Unión Europea y ha garantizado un alto nivel de protección de la información de carácter personal en la comunidad.

El documento se refiere, además, a los obstáculos que se aprecian en la aplicación de esta Directiva, recordando que la legislación sobre datos personales mostraba, para esa fecha, graves divergencias entre los estados miembros de la Unión Europea. Este obstáculo, afirma el texto, ha impedido que las organizaciones multinacionales desarrollen políticas paneuropeas sobre la protección de datos.

En otro aspecto importante, este informe enumera una serie de dificultades que se han apreciado en la legislación del tratamiento de datos personales, estás son:

i) Se ha contado con recursos insuficientes en cuanto a su aplicación.

ii) Se ha presentado una conformidad muy irregular en aquellos responsables a cargo del tratamiento de datos personales.

iii) Ha existido un conocimiento escaso por parte de los afectados en relación de sus derechos. Esta dificultad podría originar el fenómeno anterior.

Asimismo, este documento adoptó un programa de trabajo que se compone por una serie de actuaciones que deberían realizarse desde este informe hasta 2004. Estas actuaciones se relacionaban con las siguientes iniciativas:

a) La realización de Debates con los Estados miembros y las autoridades encargadas de la protección de datos personales sobre los cambios necesarios para que se adecuen plenamente la legislación nacional con los requisitos de la Directiva de la Unión Europea.

b) Los países candidatos a la Unión Europea deben también realizar esfuerzos para lograr una mejor y más uniforme aplicación de esta Directiva.

c) Mejoramiento de la notificación de todos los actos jurídicos de transposición de esta Directiva.

d) Simplificar las condiciones de transferencias internacionales de datos.

e) Promover el uso de tecnologías que refuercen la protección de la intimidad.

f) Fomentar la autorregulación y los códigos de conducta europeos.

Un tercer documento es la Directiva del Parlamento Europeo, relacionada con el sector de las Comunicaciones Electrónicas que fue firmada 12 de julio de 2002 y se identifica como Directiva 2002/56/CE.

Este informe se refiere a temas de gran importancia como, por ejemplo, la conservación de los datos de conexión en los Estados miembros de la Unión Europea, a efectos de facilitar la vigilancia policial (en otras palabras la retención de datos); el envío de mensajes electrónicos que no han sido solicitados (o SPAM); el uso de las denominadas “cookies” y el incluir datos personales en las guías públicas.

El cuarto informe es la Decisión de la Comisión con número 2004/915/CE, 27 de diciembre de 2004, que modifica la Decisión 2001/497/CE, específicamente en el tema de la introducción de un conjunto alternativo de cláusulas contractuales tipo que se refieren a la transferencia de Datos Personales a terceros países.

Un quinto documento es la Decisión 2001/497/CE, con fecha 15 de junio de 2001. Este texto define las cláusulas contractuales tipo que deben garantizar un nivel adecuado de Protección de Datos Personales que sean transferidos de la Unión Europea a terceros países.

Esta decisión obliga, además, a que los Estados miembros reconozcan que las sociedades u organismos que utilicen esas cláusulas tipo en contractos, y que garanticen, además, un adecuado nivel de protección de los datos.

En sexto lugar se encuentra el Reglamento 45/2001/CE que fue firmado en diciembre de 2000. Este reglamento se relaciona a la protección de las personas físicas, específicamente en lo que respecta al tratamiento de datos personales por instituciones y organismos comunitarios y a la libre circulación de estos datos.

Este Reglamento expresa:

-Disposiciones que garanticen un elevado nivel de protección elevado para aquellos datos personales que sean tratados por instituciones y organismos comunitarios, y,

-La creación de un organismo de vigilancia independiente que sea la encargada de controlar la aplicación de estas disposiciones.

Como es posible inferir, la Comunidad Europea articula de forma específica, puntual y amplia el tema de la protección de datos personales, el cual es considerado como un derecho importante en cuanto a la concepción de sus ciudadanos.

2. Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.

Redactadas el 23 de septiembre de 1980, las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales son otro texto interesante.

La Directrices de la OCDE, en primer término, les recuerda a los gobiernos integrantes de esta organización que adquirieron el compromiso de desarrollar enfoques comunes frente al tratamiento y el flujo de datos transfronterizos. Asimismo el texto solicita que se implementen soluciones armonizadas con respecto a este tema. Finalmente, esta legislación solicita un compromiso a sus miembros con respecto a la protección de la privacidad de las redes globales, compromiso que buscará garantizar el respeto de los derechos, generar una confianza en las redes globales y, por último, que se eviten determinadas restricciones innecesarias en los flujos transfronterizos de datos personales.

Las Directrices de la OCDE definen dos alcances de aplicación. Por un lado el ámbito nacional e internacional, y por otro, la esfera del Sector Público y el Sector Privado. En este segundo ámbito, el texto enfatiza que los datos personales del sector público o privado que, suponen un peligro a la privacidad y las libertades individuales a causa de la forma en que se procesa la información, la naturaleza de estos datos y el contexto en que se utilizan.

Por último, las directrices de la OCDE, solicita la consideración de estándares mínimos que se complementen con otras medidas de protección tanto de la privacidad, como de las libertades individuales.

En su aspecto legislativo, las Directrices de la OCDE incluyen tres excepciones de aplicación. Estas excepciones están relacionadas con la soberanía, la seguridad nacional y el orden público. Sin embargo se recomienda que debe limitarse lo menos posible y siempre que estas limitaciones sean de conocimiento público.

Las directrices de la OCDE contienen 8 principios. El primero de estos se refiere a la *Calidad de los datos*. Este principio afirma que los datos deben ser relevantes para el propósito de su utilización y, en la medida de lo posible para este propósito, debiesen ser una información exacta, completa y actualizada.

Un segundo Principio se denomina *Limitación de recogida* y que expresa que deben existir claros límites al momento en que se recaban datos personales y que cualquiera de estos datos deberá obtenerse por medios justos y legales y, siempre que sea apropiado, con consentimiento o conocimiento del afectado.

En tercer lugar, se encuentra el Principio de *Especificación del propósito*. Este punto señala claramente que a más tardar en el momento en que se recaben los datos personales, debe especificarse claramente el propósito por el cual fue recogida esta información. Asimismo, la utilización de los datos personales se limitará al cumplimiento de los objetivos que no sean incompatibles con el propósito original por el cual se solicitaron estos datos y, si fuera el caso, especificando en cada momento si existe un cambio de objetivo.

El cuarto principio se refiere a *Limitación de uso* y expresa que no deben divulgarse, entregarse o utilizar datos personales para propósitos que no cumplan con lo que se expuso en el apartado noveno de estas directrices, salvo, en primer lugar si se tiene el consentimiento del afectado y, en segundo término, que esto obedezca a una imposición legal o exigida por las autoridades.

El Quinto Principio se denomina *Salvaguardia de la Seguridad* y solicita que se empleen métodos de control y seguridad, que sean capaces de proteger los datos personales contra riesgos como la pérdida de éstos, el acceso no autorizado, la destrucción u mal uso de esta información y, por último, que éstos se modifiquen y se divulguen sin consentimiento.

En sexta posición se ubica el *Principio de Transparencia*. Este principio afirma que debe existir una política general sobre transparencia en cuanto a la evolución, prácticas y políticas relativas a datos personales. Asimismo, se contará con medios ágiles que determinen la existencia y naturaleza de los datos personales, como también el propósito principal para su utilización y la identidad y lugar de residencia habitual del encargado de controlar esta información.

El séptimo principio se refiere a la *Participación Individual*. Este principio expresa que todo individuo tendrá derecho a, por un lado, que el controlador de datos y otra fuente le confirmen que poseen datos sobre su persona, y, por otro, que le comuniquen estos datos en un tiempo y forma razonable, a un precio que no sea excesivo y de manera inteligible.

Asimismo, se le deben explicar al afectado las razones por las cuales una petición suya fue denegada y si esta reclamación es exitosa, y se confirman las dudas, los datos de ese sujeto serán eliminados, rectificados, complementados o corregidos.

Por último se encuentra el *Principio de responsabilidad*. Este expresa que en todo controlador de datos recaerá la responsabilidad de cumplir con las medidas que hagan efectivos los principios mencionados con anterioridad.

Las Directrices de la OCDE se refieren también a los principios básicos de aplicación internacional en el tema de la restricción en el libre flujo y legitimidad en el tratamiento de datos personales.

En primer lugar, el texto específica sobre las implicaciones en caso de un procesamiento nacional de datos personales. En este caso este documento afirma que los países miembros deben considerar las implicaciones que estén presentes en el procesamiento nacional y la exportación de Datos Personales que se realice con otros países miembros.

En segundo término el texto habla sobre el flujo efectivo de datos personales. Las directrices de la OCDE recuerdan a sus países miembros que deberán adecuarse a todos los pasos razonables y apropiados, asegurando así que el flujos transfronterizo de datos personales, inclusive cuando el transito se realice a través de un país miembro de la OCDE, deberá realizarse de forma e ininterrumpida.

Las directrices de la OCDE también se refieren a la no restricción de intercambio fronterizo.

Las recomendaciones del texto, en este caso, apuntan a que los países miembros no deben restringir el intercambio fronterizo de datos personales con otros países miembros, salvo en dos oportunidades: cuando el país que recibe los datos no observa ni cumple de forma sustancial las directrices y cuando esta exportación de datos burle la legislación nacional sobre la privacidad.

En términos de la protección nacional especifica a los datos personales, la OCDE en sus directrices expresan que sus países miembros pueden imponer restricciones a ciertas categorías de datos personales, sobre los que rijan normativas de carácter especifico y que estén contenidas en la legislación nacional sobre la privacidad, que por su naturaleza no tendrán una protección similar en el país receptor.

Por último, el documento de la OCDE se refiere a aquellas limitantes al acceso de protección. Bajo este punto se afirma que los países miembros deben evitar la elaboración de leyes, políticas y prácticas que se orienten a proteger la privacidad y las libertad individuales, si éstas pusieran obstáculos al flujo transfronterizo de datos personales, excediendo, así, los requisitos de tal protección.

Con respecto a la implantación nacional, las Directrices de la OCDE expresa que se deben realizarse los principios propios de este texto, para ello los países miembros deberán crear una serie de procedimientos o instituciones legales, administrativos o de otro tipo para que se vele por la protección efectiva de la privacidad y de las libertades individuales que se relacionen con los datos personales.

Asimismo, las Directrices de la OCDE solicitan a sus países miembros una especial atención a las siguientes acciones jurídicas: en primer lugar que estos estados adopten una legislación nacional adecuada para la protección de datos personales; en segundo término que se impulse y se apoye la autorregulación, sea ésta a través de códigos de conducta u otro modo; tercero, que se brinden los medios razonables para que las personas naturales puedan ejercer sus derechos; en cuarto lugar que se establezcan mecanismos que no sólo sancionen adecuadamente, sino que también ofrezcan soluciones en caso de fallos, donde se cumplan las medidas de implantación expresadas en los principios de aplicación nacional e internacional; y, por último, que se asegure que no existirá discriminación desleal hacia el sujeto y sus datos personales.

Con respecto al tema de la Cooperación Internacional, las Directrices de la OCDE expresan de que si existiese el caso una solicitud de información sobre la observancia de estas directrices, los países miembros deben dar a conocer a otras naciones integrantes de la OCDE detalles sobre cómo se están cumpliendo los principios incluidos en estas directrices.

Asimismo, se solicita a los países miembros que aseguren los procedimientos para el flujo transfronterizo de datos personales, y de protección de privacidad y libertades individuales sean sencillos y compatibles con otros países miembros que comparten estas directrices.

Otro tema que se relaciona con la cooperación internacional, son procedimientos que facilitan el intercambio de datos personales. Entre estos procedimientos se destacan:

a) Que este intercambio de información esté relacionado con estas directrices, y,

b) Que la cooperación se realice especialmente en asuntos procesales y de investigación.

Para concluir, las directrices de la OCDE solicitan a sus países miembros que orienten su trabajo hacia la elaboración de principios, sean estos nacionales o internacionales, que establezcan una legislación que sea aplicable en el tema de los flujos transfronterizos de datos personales.

3. Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados.

Adoptadas mediante resolución 45/95 de la Asamblea General, del 14 de diciembre de 1990, estas directrices establecen que es iniciativa de cada Estado fijar los procedimientos que pongan en práctica las normas relativas a los archivos de datos personales informatizados, enfatizando que estos procedimientos están sujetos a las orientaciones establecidas en el documento.

Asimismo, y también en términos a la función estatal, las Directrices expresan que acorde a la legislación interna de cada país, se debe designar una autoridad que sea responsable de supervisar que se cumplan los principios que se encuentran en estas directrices.

Quien ocupe este cargo debe cumplir con ciertos requisitos determinados. Los valores que las directrices otorgan a esta autoridad son que este encargado otorgue garantías de imparcialidad, independencia frente a las personas, las agencias que procesen estos datos y que demuestre competencia técnica para el desarrollo de sus funciones.

Las Directrices de la ONU, a su vez, definen claramente el campo de aplicación de los principios contenidos en este texto. De esta forma los principios deben aplicarse, en primer término, a todos los archivos informatizados públicos y privados, así como, mediante la extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales.

Por otro lado, las directrices de la ONU especifican que existe la posibilidad de dictar disposiciones especiales y optativas, para facilitar la aplicación todos o de una parte de los principios a los archivos relativos a personas jurídicas, en especial cuando estos contengan alguna información relativa a individuos.

Las Directrices de la ONU contienen 7 principios esenciales.

En primer lugar, se establece un *Principio de legalidad y lealtad*. Este punto enfatiza que la información que se refiera las personas no debe recogerse ni procesarse por métodos desleales o ilegales, ni se utilizarán para fines que estén en contra de los principios de la Carta de las Naciones Unidas.

El segundo principio recogido en estas directrices de la ONU, es el *Principio de exactitud*. Bajo este precepto se establece que aquella persona que sea responsable de la recopilación de archivos, o las personas responsables de su mantención, están obligados a comprobar periódicamente acerca de si los datos registrados son exactos y pertinentes y garantizar, a su vez, que estos datos se mantengan de la forma más completa posible, evitando así errores por omisión; además deberán actualizarse periódicamente o en los casos en que se use la información que se encuentre en un archivo, mientras esta información esté siendo procesada.

Las Directrices de la ONU agregan también el *Principio de especificación de la finalidad.* Este principio sostiene que un archivo y su utilización deben obedecer a una finalidad especificada y legítima, y una vez que esté establecida, deberá recibir una cantidad

determinada de publicidad o ponerse en conocimiento del interesado, con el fin de que a posteriori se garantice:

> a) Que todos los datos personales que ha sido recogidos y registrados se mantengan pertinentes y adecuados para los fines especificados.
>
> b) Que ninguno de estos datos personales sean utilizados o revelados, con la única excepción de que la persona afectada entregue su consentimiento. Asimismo estos datos no podrán utilizarse para fines incompatibles a aquellos que fueron especificados previamente.
>
> c) Que el período por el cual se guarden estos datos personales, no deba superar aquel que permita la consecución de los fines especificados.

En cuarto lugar se encuentra el *Principio de acceso de la persona interesada*. Las Directrices de la ONU explican que cualquier que pueda ofrecer la prueba de su identidad, tendrá el derecho a saber si la información que le concierne está siendo procesada; además, y si lo desease, obtener sus datos de forma inteligible, gratuita y sin retrasos, y, por último, podrá optar a que se realicen las rectificaciones y supresiones que sean procedentes cuando se hubiesen hecho anotaciones ilegales, innecesarias o inexactas. Estas rectificaciones serán gratuitas para el usuario, y su coste recaerá en la persona responsable del archivo. Asimismo, se le informará al usuario si sus datos han sido comunicados.

Para reforzar este punto, las directrices de la ONU expresan que se debiese de prever un recurso, si el caso lo amerita, ante la autoridad supervisora y responsable que sea designada para hacer cumplir los principios contenidos en estas directrices.

Por último, las directrices de la ONU enfatizan la conveniencia de que todas las disposiciones que se relacionen con este principio sea aplicadas a todas las personas, sea cual sea su nacionalidad o lugar donde resida.

Las Directrices de la ONU incluyen, en quinto lugar, el *principio de no discriminación.* En este punto, el texto afirma que sin perjuicio de los casos que sean susceptibles de excepción restrictivamente contemplados en el sexto principio, no deberán ser recogidos datos que pudiesen originar una discriminación ilegal o arbitraria, incluyendo aquella información referida a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, incluyéndose además si existe información que identifique a su poseedor como miembro de una asociación o sindicato.

El sexto *principio es la Facultad para hacer excepciones*. Las directrices de la ONU especifican que se pueden realizar excepciones a los cuatro primeros principios, sólo pueden autorizarse cuando sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad. Otro caso será cuando se presenten violación de derechos y libertades de otros, en especial aquellas personas que son perseguidas (cláusula humanitaria), siempre que las excepciones sean explicitadas en una ley o norma equivalente que haya sido promulgada acorde al sistema jurídico interno, que expresamente establezca los límites y prevea las salvaguardas adecuadas.

Cabe señalar, además, que las excepciones mencionadas en el quinto principio, deben estar sujetas a las mismas salvaguardas que las prescritas para las excepciones de los principios 1 a 4, y solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional

de Derechos Humanos y en el resto de aquellos instrumentos que se aplican en materia de protección de los derechos humanos y en la prevención de la discriminación.

En séptimo lugar se encuentra el *Principio de seguridad.* Este punto recalca que debiesen adoptarse medidas adecuadas para la protección de los archivos, tanto contra peligros naturales (como para la pérdida o la destrucción accidental), como los de origen humano (como el acceso no autorizado, la utilización fraudulenta de datos o su contaminación por virus informáticos.)

Existirá una sola excepción a estos principios denominada cláusula humanitaria, esta se aplicará cuando la finalidad de esta recolección de datos personales se relacione con la protección de los derechos humanos y libertades fundamentales del interesado, como también si está ligada a la ayuda humanitaria. Asimismo, se debe prever de una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales, donde el acuerdo organizativo no impida que se ponga en práctica la referida legislación nacional, así como en el caso de las organizaciones internacionales no gubernamentales a quienes se aplique esta ley.

En relación al Flujo Transfronterizo de datos, las directrices de la ONU expresan que si se presentase el caso en que la legislación de dos o más países que se vean afectados por un flujo transfronterizo de datos sean capaces de ofrecer salvaguardas similares para la protección de la intimidad, en ese caso la información podrá circular tan libremente como ocurre al interior de cada uno de los territorios afectados.

Sin embargo, y si ocurriese el caso contrario, es decir que no existan salvaguardas recíprocas, las directrices de la ONU expresan que no se deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que se exija para velar por la protección de la intimidad.

Asimismo, el texto de la ONU se refiere a cómo aplicar estas directrices a archivos de datos personales que son mantenidos por organizaciones internacionales gubernamentales. En este caso se explica que éstas se encuentran sujetas a cualquier ajuste que sea preciso para observar cualquier diferencia que existiese entre archivos para fines internos, como aquellos ficheros que conciernan a la gestión de personal, y, finalmente, archivos para fines externos, que se relacionan con terceras personas que tengan relación con esa organización.

En otro aspecto relevante, las Directrices de la ONU afirman que cada organización designará a una autoridad que sea legalmente competente, para que ésta supervise el cumplimiento de estas directrices.

En lo que respecta a la implantación nacional, las Directrices de la ONU estipulan tanto una supervisión, como sanciones pertinentes a quienes no respeten los principios contenidos en el texto anteriormente mencionado.

De esta forma, estas directrices expresan que la legislación de cada país debe tener la capacidad de designar a una autoridad responsable de supervisar que se cumplan los principios redactados en este texto. Este encargado debe entregar garantías claras de independencia, imparcialidad frente a aquellas instituciones o personas que sean responsables de procesar los datos, como aquellas organizaciones de corte técnico.

Asimismo, las Directrices de la ONU especifican la posibilidad de que exista una sanción a quienes llegasen a violar este derecho. Estas sanciones deberán estar contenidas en la propia

legislación nacional y estar acorde a los principios redactados en estas directrices. Entre los recursos sancionatorios se incluyen las condenas penales y la utilización de los recursos judiciales adecuados.

4. Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.

En su aspecto legislativo, estas directrices poseen un ámbito de aplicación bien definido que comprende en primer lugar todo tratamiento manual o automatizado de carácter personal. Asimismo, la aplicación específicamente se relacionará con cualquier información que se refiera a personas que puedan ser identificadas o identificables. Finalmente se establece que estas directrices son aplicables a todas la entidades sean de carácter público o privado.

No obstante de lo anterior, estas Directrices poseen límites claramente definidos en su aplicación. De este modo, el texto expresa que se pueden excluir el tratamiento manual o no automatizado de datos personales, si esta información recolectada no se integrará a un fichero estructurado con arreglo a determinados criterios que podrían permitir que se identifique a la persona, cuyos datos se encuentran incluidos en este tratamiento.

Asimismo, estas Directrices no se aplicarán al tratamiento de datos de carácter personal, sea automatizado o manual, que una persona física realice para fines que se relacionan exclusivamente en el ámbito de su vida privada o familiar.

Por otro lado, y también en el marco de la legislación, existe una serie de excepciones de aplicación que se refieren en primer lugar a los principios relacionados con la finalidad y la calidad de los datos tratado, en segundo término a la legitimación para el tratamiento; tercero a la transparencia y la información que se le entrega al interesado, cuarto a los derechos de acceso, rectificación y cancelación de los interesados; en quinto lugar se encuentran otros derechos de los interesados (Salvo cuando éste recurra a tribunales y/o autoridades competentes y a la indemnización que por cualquier daño o lesión que se hubiese sufridos en los bienes o derechos) y, por último, existen limitaciones en la transferencia internacional de datos.

Cabe resaltar que para esta exclusión, debe mediar una ley nacional que proteja y tutele determinados tratamientos de datos personales en la medida que la aplicación de las directrices supusiera un riesgo para la protección de la seguridad nacional, el orden público, la salud pública o la moralidad.

No obstante, esta medida debe ser estrictamente necesaria y no ser excesiva en el marco de una sociedad democrática.

Para reforzar su trabajo, estas Directrices establecen una serie de principios que deben salvaguardarse.

En primer lugar se mencionan un principio que está relacionado con *la finalidad y la calidad de los datos*. En este punto se resalta que el tratamiento de los datos debiese ser leal y lícito, esto es que los datos sólo pueden ser recogidos de buena fe, respetando la ley y los derechos de las personas y, siempre, en conformidad con lo previsto en estas directrices.

Este principio también se refiere a establecer una limitación de la finalidad, donde se establezca claramente que los datos solo pueden ser recabados y tratados para el

cumplimiento de finalidades explicitas, legítimas y claramente determinadas y en estrecha relación con la actividad de quien realice este tratamiento de datos. De este modo, los datos personales no pueden ser motivo de tratamiento para un fin distinto por el cual fueron entregados. Sin embargo, se establecen que podría incurrir la existencia de una legitimación suficiente para esto, pero que de ser éste el caso, debe estar acorde con el marco de legitimación del tratamiento de datos personales que se establece en estas directrices.

Otro principio muy ligado a la finalidad y calidad de los datos, es el *llamado principio de proporcionalidad,* que expresa que solo serán sometidos a tratamiento de datos, aquella información que sea adecuada, pertinente y no excesiva y que esté en estrecha relación con las finalidades mencionadas en el punto anterior.

El *Principio de exactitud* también está contenido en estas directrices. Este principio expresa que los datos deben ser y mantenerse exactos, completos y actualizados, respondiendo, así, a la verdadera situación en que se encuentra la persona a la que se refieren esos datos.

Otro punto importante es el *Principio de conservación.* El principio de Conservación establece que los datos deberán cancelarse o pasar al anonimato, cuando ya no sean necesarios para el cumplimiento de las finalidades bajo las cuales fueron obtenidos para su tratamiento.

Las directrices de la Comunidad iberoamericana establecen, además, cuatro puntos esenciales con respecto a la legitimación del tratamiento de los datos personales.

En primer lugar expresa que los datos solo pueden ser recabados o tratados cuando exista el consentimiento del interesado.

En segundo término, y si no existiese este consentimiento, la Ley podrá establecer supuestos donde no sea necesario este consentimiento expreso para el tratamiento de datos personales, atendiendo a las circunstancias que concurran en cada uno de estos supuestos, y en todo caso, siempre que dicha excepción no perjudique los derechos fundamentales del poseedor de esos datos personales.

Existirá, a su vez, y más en particular, otra excepción donde la Ley podrá permitir que se realice un tratamiento de los datos sin el consentimiento expreso del interesado, cuando éste se desarrolle en el marco de una relación jurídica o por una administración en el ejercicio de las potestades que se le hayan atribuido.

En tercer lugar se expresa que todo aquellos datos que pudiesen revelar ideología, afiliación sindical, religión o creencias del interesado, sólo se podrán tratar con el consentimiento de éste, a menos que el afectado los hubiera hecho manifiestamente públicos.

Un cuarto punto de estas directrices solicita que aquellos datos que se relacionen con la salud, el origen racial y la vida sexual del usuario, sean únicamente recogidos y tratados en los supuestos ya mencionados o cuando una Ley así lo disponga.

Por último, se expresa que en todo caso, las siguientes directrices no deben obstaculizar el adecuado tratamiento médico del afectado, ni la atención frente a una urgencia vital de éste.

5. Acuerdo de Puerto Seguro

El Acuerdo de Puerto Seguro se refiere a una negociación resultante entre Estados Unidos y la Unión Europea. Sin embargo se considera necesario analizar su texto debido a que arroja aspectos de negociaciones fructificadas, teniendo el matiz que la Unión Europea demuestra un avance importante en cuanto al tema.

Las conversaciones de dicho documento fueron iniciadas por Estados Unidos en el año de 1999, con el objeto que la Unión Europea le permitiera acceder a una declaración sobre un nivel adecuado de protección de datos personales. Sin embargo, esta declaración se enfrentó a un gran problema, en Estados Unidos no existe una normativa general sobre el tratamiento de datos personales que se aplique no sólo a todo el territorio, sino también a todos los sectores de actividad, sino, por el contrario, normas muy especificas o dispersas que se refieren a áreas muy concretas. Cabe destacar, que dado que en Estados Unidos, la protección de la intimidad y los datos personales se encuentra inmersa en una regulación de carácter sectorial, que se da tanto a nivel federal como estatal, y que se combina con una autorregulación industrial.

Asimismo, y como una forma de superar los problemas previos que habían surgido en el tema del tratamiento de datos personales en el flujo transfronterizo de información, el Departamento de Comercio de los Estados Unidos redactó un borrador titulado "principios de puerto seguro" y lo presentó para que fuera debatido tanto por las autoridades norteamericanas, como por la Unión Europea. Este texto tenía como finalidad que se garantizara a todos los operadores que se integraran, lo que se denominaba "presunción de adecuación". Esta presunción respondía al nivel de protección que exigía la Directiva 95/46/CE, facilitando, de esta forma, una transferencia internacional y libre de datos personales entre ambas partes. Para que este documento hiciera efecto, se solicitaba no sólo la adhesión a estos principios, sino el compromiso de llevarlos a la práctica. Esta adhesión debía realizarse ante la Oficina Federal de Comercio (u otro organismo designado por esta institución).

El Acuerdo Puerto Seguro presenta siete principios básicos. En primer lugar se encuentra *la notificación a los afectados*; en segundo término la o*pción de oponerse al tratamiento por parte del titular de los datos*; un tercer principio es la *transferencia ulterior a terceras empresas*, un cuarto punto *es el principio de seguridad*; en quinto y sexto lugar respectivamente se encuentran el *principio de finalidad y el principio de proporcionalidad;* y, finalmente se encuentra el *principio que vela por el derecho de acceso y aplicación*, que se refiere a los procedimientos que salvaguarden los derechos de los titulares de esos datos.

Para complementar estos principios, el Acuerdo de Puerto Seguro agregó, a su vez, las denominadas "preguntas más frecuentes", que se relacionan con tipos muy específicos de datos o tratamientos.

Finalmente, mediante la Decisión de 26 de Julio de 2000, y en conformidad a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, la Comisión Europea se pronunció formalmente sobre la adecuación que se confiere a los principios de Puerto Seguro, en materia protección de la vida privada, y reafirmando las preguntas frecuentes sobre este tema que fueron publicadas por el Departamento de Comercio de los Estados Unidos de América.

CAPITULO III.
ANÁLISIS COMPARATIVO DE LAS LEGISLACIONES INTERNACIONALES DE PROTECCIÓN EN EL TRATAMIENTO DE DATOS.

Al efectuar un análisis comparativo de las directrices antes descritas, se determina que son cinco las áreas donde coinciden.

1. Rol del Estado.

Tanto la ONU como la Directiva de la Unión Europea expresan que el rol del Estado es fundamental en la materia y que en ellos recaen los procedimientos que se deben establecer para la protección de datos personales.

De este modo, la Directriz 94/46/CE sostiene que cada estado miembro de la Unión Europea debe escoger a una o más autoridades públicas de carácter independiente, que sean las responsables de controlar que se apliquen en esa nación, las disposiciones que se incluían en esta directiva.

Por su parte la OCDE, también recoge la idea de que cada país integrante, designe una autoridad que supervise que se cumplan los principios establecidos en su texto.

2. Legislación y campo de aplicación.

La Directiva de la Unión Europea, el documento de la OCDE, las directrices de la ONU y el texto de la Red Iberoamericana coinciden en que su campo de aplicación se refiere no sólo al tratamiento de datos personales, sino también a la información que se recoge, sea esta recopilación por medios automatizados como manuales. Sólo las Directrices de la OCDE definen como alcance de aplicación al ámbito nacional e internacional, como a los sectores públicos y privados. Asimismo la Directiva de la Unión Europea especifica que la aplicación debe extenderse a "personas jurídicas".

Otro elemento en común en los lineamientos analizados son las denominadas excepciones en la aplicación. Existe concordancia en estos documentos en establecer ciertos casos especiales donde debe primar un criterio más amplio en el tratamiento de datos personales, sin requerir, necesariamente, del consentimiento del titular de los datos personales.

Tanto la Directiva europea, el texto de la OCDE y las Directrices de la Red Iberoamericana coinciden en que las excepciones de aplicación deben obedecer a la seguridad pública o nacional, a la protección del orden público, o a la defensa o soberanía de la nación. La Red Iberoamericana va más allá y agrega motivos de salud pública y moralidad a estas excepciones y expresa que estas limitaciones deben ser necesarias y no excesivas y siempre enmarcadas en el ámbito de una sociedad democrática

3. Principios que deben respetarse en el tratamiento de datos personales.

Al analizar los principios que se presentan en estos cuatro documentos, es posible encontrar algunas concordancias sobre cuáles deben ser aquellos elementos básicos que deben cumplir estos textos.

En primer lugar, todos los textos analizados sostienen que el tratamiento de datos personales debe será leal, justo, legal y legítimo. En particular la Directiva de la Unión Europea sostiene que un principio de legitimidad de tratamiento basado en el consentimiento del interesado y en que el tratamiento de datos sea necesario. El texto de la OCDE, a su vez, expresa que debe existir una limitación en cómo se recogen estos datos, acto que debe ser legal y justo.

En segundo término, tenemos el Principio de Informar al afectado sobre la finalidad o el propósito por el cual sus datos personales han sido recabados. Este principio es compartido por los cuatro documentos.

Un tercer principio general a todas estas directrices es el de la seguridad y conservación de los datos, sugiriéndose a los países que el responsable del tratamiento de los datos personales, debe velar porque estos datos estén en un lugar seguro, protegidos no solo de desastres naturales, sino también de la acción de terceros. Asimismo la Directriz de la Red Iberoamericana expresa que además de la conservación, es preciso eliminar o cancelar aquellos archivos que ya no son necesarios.

Existen, además, cuatro principios adicionales que se comparten por al menos dos de estos documentos analizados.

Por ejemplo, Tanto la Directiva de la Unión Europea, como la Directriz de la OCDE enfatizan la "calidad de los datos" como un principio fundamental.

En otros ámbitos, las Directrices de la ONU y la Directiva Europea coinciden en redactar principios que protejan el "acceso del interesado a sus datos" y cuáles deben ser las "excepciones de aplicación en el tratamiento".

Finalmente encontramos que el Principio de Exactitud, esto es que los datos se adecuen lo más fielmente a la realidad, se encuentra en los textos de la ONU y de la Red Iberoamericana.

4. Principios básicos de Aplicación en el flujo transfronterizo de datos.

Solamente la Directriz de la ONU y el documento de la OCDE se refieren a este tema y comparten dos planteamientos esenciales.

En primer término el flujo transfronterizo de datos debe seguir pasos razonables y apropiados y la información debiese circular tan libremente como ocurre internamente en los países que realizan esta transferencia.

Además, tanto la Directriz de la ONU, como el texto de la OCDE expresan que no debiese restringirse el intercambio entre países sólo cuando esté en peligro el derecho de privacidad o intimidad. La OCDE, asimismo, agrega una limitante, ésta es que el país receptor no cumpla de manera sustancial las Directrices de esta organización

5. Implantación nacional.

En el texto de la OCDE se sugiere que los países deben realizar una serie de cambios y salvaguardas que permitan que se protejan los datos personales. Por ejemplo la directriz de dicho organismo pide que los países realicen esfuerzos en la adopción de una legislación adecuada; el impulso de una autorregulación en esta materia a través de códigos de conducta u

otros mecanismos; que se ofrezcan los medios razonables para que los afectados hagan valer sus derechos, proteger que no exista discriminación desleal hacia el titular de los datos y, por último, establecer no sólo sanciones adecuadas, sino también entregar soluciones en determinados fallos judiciales.

La Directriz de la ONU coincide en la importancia de un sistema de sanciones. Es por esto que este texto sugiere que cada legislación interna debe contemplar condenas penales y sanciones en caso en que se violente este derecho.

Tanto el documento de la OCDE como el documento de la ONU creen necesario que se ofrezcan a los afectados los medios para que se defiendan en caso de una violación de sus derechos y que estos medios deben ser recursos judiciales específicos.

Asimismo, recoge la idea de que la legislación nacional debe designar una autoridad que sea la responsable de supervisar la observancia de los principios que se incluyeron en el texto de la ONU. Esta sugerencia está en concordancia con las peticiones de la OCDE de una legislación adecuada y el impulsar una autorregulación en esta materia.

CAPITULO IV.
LEGISLACIÓN CHILENA.

La legislación chilena ha entendido la importancia de proteger la vida privada de las personas tan sólo en los últimos treinta años. Fue la discusión de la Carta Fundamental de 1980, la que situó a la vida privada como una de las materias importantes para ser analizada por la Comisión Constituyente en el anteproyecto que se plasmaría en la Constitución. Previo a este texto, la vida privada no se había recogido en la jurisprudencia constitucional como uno de los derechos fundamentales.

Específicamente el artículo 19 numeral 4 de la Constitución de 1980 expresa "*La constitución asegura a todas las personas (…) N°4. El respeto y protección de la vida privada y a la honra de la persona y su familia.*

Cabe recalcar que previo a este debate, dicho ordenamiento constitucional solo contemplaba la salvaguarda de la inviolabilidad del domicilio y el secreto de la correspondencia, figuras que poseen protección penal.

La redacción que se hizo en la Constitución[7] sobre este derecho fundamental presento también otras particularidades.

En primer lugar, la regulación de la vida privada se presentó de una forma muy concisa y acotada. En segundo término, inexplicablemente, se protegía además la "vida pública", hecho sorpresivo en el derecho comparado y que provocó amplios debate hasta que posteriormente ó este concepto se quitó de la redacción del artículo 19 numeral 4. Por último, la regulación en un mismo numeral del derecho a la honra y la vida privada, busca proteger a dos áreas de interés de la persona humana que debiesen tratarse de forma autónoma e independiente.

La redacción y el interés del equipo constituyente se orientaba a la tutela de la vida privada frente al peligro e intromisión de los medios de comunicación, sin embargo es bueno recordar que la Constitución de 1980 se redactó antes de la aparición y expansión del internet, medio que se ha transformado en una nueva fuente de dificultades para la protección de la vida privada.

Es importante señalar, además, que la protección de la vida privada también se ha incluido en otros cuerpos legales. Diversas leyes han venido a colaborar con la constitución en términos de la protección de la vida privada de la persona y todo lo que ello incluye. Tres son los textos que se pueden destacar que se han orientado a la salvaguarda de este derecho, específicamente en el tratamiento de datos personales, entendiendo los datos personales como una parte integrante de la intimidad o privacidad del ser humano.

1. Ley 19.628, "Sobre la Protección de la Vida Privada".

En el año de 1999, el Parlamento chileno aprobó la ley 19.628, denominada "Sobre la Protección de la Vida Privada". Este texto, se transformó en el primer intento de la legislación chilena de dar una tutela efectiva a la vida privada en un cuerpo legal.

[7] Esto se advierte al revisar la historia relativa a la evolución y aprobación del texto de dicha Constitución, recabada en la página web del Congreso.

Desde su ratificación, ha existido un amplio debate sobre los alcances de la misma. De este modo, en el Congreso Nacional se han presentado una serie de modificaciones y enmiendas desde su aprobación. De acuerdo con la base de datos indicada en la página web del Congreso, se cuentan en más de 70 las mociones que ha buscado modificar la ley 19.628, pero a la fecha sólo prosperaron las correcciones propuestas por la ley 19.812 de 2002, la ley 20.463 del 2010, la ley 20.521del 2011 y la ley 20.575 del 2012, cuyas especificamos se encuentran incorporadas en una tabla como anexo del presente documento.

Al analizar la ley 19.628 denota que el texto está dividido en seis títulos.

En el primero de éstos, bajo el concepto de *"Título Preliminar"* y en su primer artículo se expresa claramente que el tratamiento de datos personales queda sujeto a ese cuerpo legal, a excepción de cuando este tratamiento se realice para labores relacionadas en el ejercicio de las libertades de emitir opinión y de informar, las cuales serán reguladas por la ley a que se refiere el artículo 19 numeral 12 de la Constitución chilena, es decir la ley de Prensa o la Ley sobre Libertades de Opinión e Información y Ejercicio del Periodismo, No. 19.733.

Asimismo, se expresa que este tratamiento puede realizarse por cualquier persona, mientras esta acción sea concordante con dicho cuerpo legal y con las finalidades que están permitidas en el ordenamiento jurídico. Complementando lo anterior, se recalca el respeto por el ejercicio pleno de los derechos fundamentales de quienes son los titulares de esos datos, y las facultades que esta ley les otorga.

En este título preliminar, la Ley 19.628 define además, los conceptos básicos que incurren en esta materia, como por ejemplo: Almacenamiento de datos, Bloqueo de datos, Comunicación o transmisión de datos, Datos de carácter personal, Datos sensibles, entre otros términos.

En su *"Titulo Primero"* expresa los lineamientos que orientan este tema. En su artículo cuarto se refiere a la autorización que debe existir para que se realice este tratamiento de datos personales, especificando que al titular de estos datos se le debe explicar claramente cuál será la finalidad de los datos que están siendo recogidos. Más adelante, en el artículo 6, la ley sostiene que, en primer lugar, los datos deben ser eliminados cuando no exista una fundamentación legal para su registro y archivo, en segundo término, se deben corregir cuando la información sea errónea, y, por último se bloquearán aquellos datos inexactos y de dudosa vigencia.

El artículo 9 también es relevante, dado que especifica 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".*

De igual forma, encontramos el artículo 10 que limita el tipo de datos personales que serán objeto de tratamiento, excluyendo los datos sensibles, salvo cuando la ley entregue su autorización, cuando el titular hubiese entregado su consentimiento o cuando se utilice para determinar u otorgar beneficios de salud para los titulares de esos datos. Tal disposición es apreciable en el caso que se desarrollará más adelante.

El Titulo II se denomina *"De los derechos de los titulares de datos".*

En esta sección se especifica, por ejemplo, que el titular de los datos personales tiene el derecho de exigir al responsable del tratamiento de este fichero, que entregue información sobre qué datos de la persona ha registrado, la procedencia de los datos y el destinatario final,

como también el propósito por el cual estos datos fueron almacenados y, por último la identidad de las personas o instituciones donde serán transmitidos estos datos.

Asimismo, otro derecho que se encuentra en este título es el que posee el sujeto para modificar, cancelar o bloquear sus datos personales, acciones que no pueden ser limitadas por ningún acto o convención.

El Titulo III está dedicado a la "*Utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial".* Esta sección ha presentado las mayores modificaciones, destacándose la nueva Ley 20.575 o Ley DICOM que se especializa en el tratamiento de datos personales de carácter económico o financiero.

En el artículo 17 se dispone, que los responsables de registros o bancos de datos personales solamente comunicarán información relativa a obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, entre otras situaciones que pudiesen corresponder a ilícitos o incumplimiento de obligaciones.

Cabe resaltar también el artículo 18 que en su inciso primero expresa que, "*En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible".*

El Titulo IV se refiere *"Del tratamiento de datos por los organismos públicos"* y está constituido por tres artículos.

En primer lugar, en el artículo 20, se especifica que un organismo público realizará el tratamiento de datos personales en materias de su competencia y que, bajo estas condiciones no se requiere el consentimiento del titular. En segundo término, el artículo 21, se prohíbe que los datos personales que se relacionen con delitos o faltas administrativas o disciplinarias se comuniquen cuando haya prescrito la acción penal, a excepción de que estos datos sean solicitados por los tribunales de justicia u otros organismos públicos competentes. Finalmente en el artículo 22 se estipula que el Servicio de Registro Civil e Identificación se encargará de un registro de banco de datos a cargo de organismos públicos. Este registro será público e incluirá no sólo el fundamento jurídico que avala su existencia, sino también su finalidad, qué tipos de datos se han almacenado y una descripción del universo de personas comprendidas en ese registro. Asimismo todos los organismos públicos se verán obligados a hacer llegar al Servicio de Registro Civil e Identificación los cambios que se hicieren en los ficheros y bancos de datos que manejasen.

Finalmente, se encuentra el Título V denominado *"De la responsabilidad por las infracciones a esta ley".* En esta sección, el artículo 23 se refiere a que la persona natural o jurídica privada o el organismo público que sea responsable del registro y acopio de datos personales, debe indemnizar por daño moral y patrimonial al afectado que observare que sus datos han sido tratados indebidamente; asimismo no existirá perjuicio, si se modifican, eliminan o bloquean los datos a petición del titular o, si fuese el caso, por orden del tribunal.

Cabe señalar que el miércoles 11 de Enero de 2012 ingresó a primer trámite constitucional el proyecto de ley "*Modificaciones a ley N° 19.628, sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal",* que es identificado como Boletín 8143-03. Esta Ley se acompañó con el Mensaje Nº 395-359 del Presidente de Chile, Sebastián Piñera, en el que especificó los objetivos que tendría dicho proyecto.

Como objetivo general se busca el establecimiento de "*las condiciones regulatorias que, en primer lugar, permitan a los ciudadanos proteger sus datos personales y controlar su flujo y, en segundo lugar, faciliten a las empresas nacionales y extranjeras desarrollar sus actividades que involucren el flujo de tales datos.*"

Asimismo este proyecto posee 4 objetivos específicos. En primer lugar se busca reforzar los derechos de los titulares de los datos personales; en segundo término, que se cumplan con los compromisos internacionales que firmó Chile, específicamente aquellos que se relacionan con su incorporación a la OCDE; un tercer objetivo se orienta a que se incrementen los estándares legales de Chile en materia de protección de datos personales, para que Chile sea un país que posea un nivel adecuado de tutela de esta información; y por último, mejorar el papel de Chile en la economía mundial, favoreciendo su papel de un país receptor de inversiones extranjeras.

Actualmente dicho proyecto aun se encuentra en la etapa del primer trámite constitucional, siendo el último oficio rendido, el No.171-361 de fecha 11 de enero de 2012[8].

Otra propuesta importante de reforma introducida el 2 de agosto de 2011 es el boletín 7831-07 con título "***Modifica la ley de Protección a la Vida Privada, prohibiendo el traspaso de datos personales por parte de instituciones públicas y privadas"*** teniendo como moción su aprobación durante el período legislativo del año citado, sin embargo a la fecha aún se encuentra en primer trámite constitucional y su estado es catalogado como sin urgencia actual[9]. Este boletín, inspirado en la jurisprudencia nipona que salvaguarda de forma potente los datos personales, solicita que se incorpore un nuevo y único articulo con el N° 12 bis a la ley 19.628 sobre protección de la vida privada.

Este artículo se redacta de esta manera:

"Prohíbase a las instituciones públicas o privadas el traspaso de información relativa a datos personales para fines comerciales sin el consentimiento expreso del titular de les datos, so pena de multa ascendente a 400 UTM, y pena de presidio menor en su grado mínimo a medio para el funcionario infractor.

En caso de que la infracción sea sometida por un funcionario público además se le aplicará la pena de inhabilitación temporal sin goce de remuneración".

Más allá de las modificaciones a la Ley 19.628, existen, además dos leyes que se relacionan fuertemente con este cuerpo legal.

2. La Ley 20.285, denominada Ley de Transparencia.

Este cuerpo legal tiene como principios fundamentales: la transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo y las excepciones referidas a la publicidad de la información.

Dicha normativa se encuentra íntimamente ligada a la Ley de Protección de Datos Personales, aunque a la fecha se han presentado una serie de controversias con respecto al verdadero alcance de la Ley de Transparencia y el Consejo creado por la misma.

[8] http://www.camara.cl/pley/pley_detalle.aspx?prmID=8541
[9] http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=7831-07

Para el caso, retomamos lo expresado por el jurista Renato Jijena en una columna de opinión del Diario La Tercera[10], dicho profesional indico que esta ley: "*desnaturalizó la razón de ser del consejo. Alejándose de los objetivos de transparencia y probidad, le asignó, además, competencia para fiscalizar que los órganos estatales respeten la privacidad de los datos nominativos de los ciudadanos y los procesen computacionalmente dentro del marco de su competencia y para fines de servicio público".*

.

Jijena va más allá y sostiene que esta desnaturalización afecta el ámbito de la confidencialidad y la protección del derecho a la intimidad, donde por ejemplo esta instancia, el Consejo de Transparencia, no ha hecho una protección efectiva de los datos personales, y a pesar que pudo rechazar la solicitud, obligó a revelar datos personales sensibles de millones de ciudadanos a instituciones como el Servicio Electoral o a entregar las calificaciones de centenares funcionaros públicos frente a un requerimiento del Ministerio de la Vivienda y Urbanismo y de Fonasa.

3. Ley 20.575, ó Ley DICOM.

En la actualidad la aprobación de la ley 20.575, también conocida como "Ley DICOM" aporta una nueva arista en la legislación chilena en cuanto a la protección de los datos personales. Esta normativa se caracteriza por restringir la comunicación de datos personales de carácter económico, financiero, bancario y comercial, aportando lineamientos y restricciones sobre el tratamiento de información, debido a que sólo permite el tratamiento de estos datos en la evaluación de riesgo comercial y en durante el proceso de crédito.

En primer lugar, se prohíbe que los datos personales de carácter económico sean exigidos en trámites de selección de personal, admisión a instituciones educativas, atención de salud o la postulación a un cargo público.

En segundo término, se le entrega al titular de los datos la potestad de que requiera su información personal a los distribuidores (de datos) para fines distintos a los que fueron permitidos, si este fuese el caso, se entregará un certificado con la viñeta "para fines especiales", el que contendrá sólo las obligaciones vencidas y que no fueron pagadas por el titular.

Un tercer cambio es establecer que los distribuidores de datos económicos, financieros, bancarios y comerciales, posean un sistema que registre el acceso y la entrega de los antecedentes contenidos, individualizando, además, el nombre del requirente, el motivo de la solicitud, la fecha y hora cuando fueron solicitados.

Una cuarta modificación corresponde a que incorpora un nuevo mecanismo que apoya el ejercicio de los derechos de los usuarios. Este mecanismo obliga a los distribuidores a designar una persona natural que sea la encargada del tratamiento de datos personales, ésta será la responsable de hacer efectivos los derechos de los usuarios, sin perjuicios de que estos titulares inicien acciones legales si fuera el caso.

Asimismo, la Ley invierte la carga de la prueba, estableciendo la obligación del distribuidor o responsable de los registros o bancos de datos de probar ante el juez competente, que dio cumplimiento a las normas que rigen el tratamiento y comunicación de datos, considerando

[10] http://www.latercera.com/contenido/895_146299_9.shtml

que dicha modificación constituye un cambio transcendental y primordial en cuanto a lo que concierne al avance de protección de datos personales, ya que actualmente la prueba muchas veces es una dificultad para el titular, tanto su obtención como presentación.

Finalmente, esta ley modifica el artículo 17 de la ley N° 19.628, restringiendo e impidiendo comunicar información, de dos maneras a saber: intercala en el inciso primero después de la palabra usuarios la siguiente expresión final: "y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentren con alguna modalidad pendiente"; y agrega, en el inciso segundo a continuación de la palabra "gas" este texto: "; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura".

4. Brecha Identificada.

En Chile, la figura del habeas data legal, a pesar de constituir una protección de avanzada en el tema, no alcanza a cubrir todos los problemas de la protección de datos y tiene solo la posibilidad de solucionar algunos de los problemas suscitados, adicionalmente de tener como tropiezo su costo para acceso de toda la población.

Lo anterior debido a que es un tipo de tutela que actúa de forma posterior, es decir ya ocurrido el daño y no como un mecanismo de protección preventiva y efectiva.

Al respecto, Garrido Iglesias[11] señala que *El procedimiento que fija la ley es ante la justicia civil, y hasta hoy en día, quince años desde su vigencia no ha tenido una aplicación práctica, masiva y concreta. Las legislaciones actuales contemplan entes especializados para hacer frente a las transgresiones a este derecho, entes que además fiscalizan y controlan a quienes tratan datos. El procedimiento de la ley chilena, no se condice con la realidad tecnológica actual, y más aún carga el peso de la prueba en el afectado. En definitiva, el costo beneficio de ejercer la acción de habeas data legal, al no traer aparejada sanciones concretas y efectivas, al tener que ejercerse como cualquier acción judicial en tribunales, con defensa jurídica a coste del interesado, desmotiva a los titulares de datos a ejercerlo. Existe ausencia absoluta de la figura de autoridad de control, en cualquiera de sus formas.*

En ese sentido y en concordancia con lo relacionado en el capítulo III y IV del presente estudio, observamos que la ley chilena ha quedado atrás en muchas de sus normativas, las cuales indefectiblemente deben ser adecuadas a la realidad actual que vive la sociedad chilena.

Es claro inferir que lo anterior se traduce en un sistema actual poco eficiente y accesible para la población, produciendo un impacto directo en el menoscabo de sus derechos. Esta afirmación pretende dilucidarse más adelante con el relato y análisis de una experiencia de alto impacto, que tuvo injerencia en los medios de comunicación.

Al respecto, el diputado Pedro Araya en una entrevista presente en este estudio, concuerda que, en relación a esta materia, la legislación Chilena es muy antigua, lo que produce una fuerte debilidad en el sistema de protección de datos, dado que ésta respondía a una realidad chilena del país muy distinto a la actual.

[11] El Habeas Data y la ley de protección de datos en Chile.
http://eprints.rclis.org/19755/1/Serie%20N%C2%B0%2083%20Romina%20Garrido.pdf

Y es que las capacidades para intercambiar información han ido agilizándose, como también los comportamientos y actividades generadas a los entornos económicos. Sin embargo, la legislación quedó relegada, emitiendo otros cuerpos legales que permitieran cubrir ciertas áreas vinculadas, como por ejemplo la Ley Dicom.

Asimismo, el especialista en la materia, Pedro Huichalaf Roa, indica[12] que, "*la nueva ley de datos personales, propone un reto a la hora de legislar un tema de esta complejidad, teniendo en cuenta la existencia de una naturaleza distinta entre el mundo del comercio tradicional, y aquel que se realiza a través de medios propios de la sociedad de la información.*

De esta manera, se recomienda evitar cargas innecesarias sobre los organismos privados, empresas y organizaciones que ejercen sus labores en Internet, ya que las mismas pueden frenar el desarrollo del sector en el ámbito nacional, estableciendo barreras de entrada para el emprendimiento en el sector y, dicho sea de paso, creando situaciones en las que es imposible fiscalizar la ocurrencia de faltas a las normas establecidas en la ley, creando un problema de aplicación y cumplimiento de la ley".

Es por ello que no obstante se encuentra en proceso el boletín 8143-03, mensaje con el que se introducen modificaciones a la ley Nº19.628 sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal (también denominada 'Ley de Datos Personales'), pretende incorporar a Chile en los estándares de la OCDE en el tratamiento de esta materia.

La nueva ley de datos personales, propone un reto a la hora de legislar un tema de esta complejidad, teniendo en cuenta la existencia de una naturaleza distinta entre el mundo del comercio tradicional, y aquel que se realiza a través de medios propios de la sociedad de la información.

De esta manera, se recomienda evitar cargas innecesarias sobre los organismos privados, empresas y organizaciones que ejercen sus labores en Internet, ya que las mismas pueden frenar el desarrollo del sector en el ámbito nacional, estableciendo barreras de entrada para el emprendimiento en el sector y, dicho sea de paso, creando situaciones en las que es imposible fiscalizar la ocurrencia de faltas a las normas establecidas en la ley, creando un problema de aplicación y cumplimiento de la ley.

Uno de los mayores riesgos que la nueva legislación puede incluir en la vida civil de Chile, es la creación de espacios abiertos de censura bajo el escudo de la protección de datos personales, al no contar con normativa especial para los medios de información periodística, o las actividades ligadas a la libre expresión de los ciudadanos

De este modo, la Directriz 94/46/CE sostiene que cada estado miembro de la Unión Europea debe escoger a una o más autoridades públicas de carácter independiente, que sean las responsables de controlar que se apliquen en esa nación, las disposiciones que se incluían en esta directiva.

Por otra parte, y dada la relevancia que cobra el hecho que Chile se haya incorporado como un miembro de la OCDE, es necesario adecuar el marco regulatorio con la finalidad de que se establezca un balance entre un nivel elevado de protección de los datos personales y la libre

[12] Sobre las modificaciones a la Ley Nº19.628 de "datos personales" chilena, publicado en la página web del Observatorio Iberoamericano de Protección de Datos.

http://oiprodat.com/2013/11/13/sobre-las-modificaciones-a-la-ley-no19-628-de-datos-personales-chilena/

circulación de los mismos. Por ello, el objetivo debe encaminarse en que tanto la obtención como la utilización de los datos personales tengan parámetros de preciso cumplimiento, así como la creación de un organismo independiente encargado de la protección de los mismos.

CAPITULO V.
ESTUDIO DE CASO.

El caso a desarrollar fue escogido en razón que versa sobre un dato personal con un mayor grado de particularidad, relevancia y connotación y por ende a partir de su especificidad debe tener una cobertura de protección mucho más rigurosa.

Tal como lo indican Hernández Muñoz, Ana Karina; Palacios Henríquez, Juan Andrés, en su tesis *El dato sensible. Su tratamiento en Chile y en el derecho comparado. (2008): "La información, o para usar el lenguaje de la ley, los datos pueden encontrarse en diversos grados de relevancia: pueden existir datos personales y datos sensibles, cuya diferencia está dada por la relación o cercanía que tengan con el ámbito más íntimo de la persona (dato sensible), o más privado, pero no por ello no importante y no digno de protección (dato personal)".*

Por lo anterior se considera, que el análisis de dicho caso, representa un iceberg de la situación existente en materia de datos personales en Chile, ya que si la protección de este dato sensible posee fisuras e inconvenientes, nos entrega una idea de que la generalidad de protección de datos personales, tendrá muchos más tropiezos y dificultades.

1. Descripción del caso de la señora Sara Castro Pérez. (Nombre cambiado para garantizar la privacidad de la identidad de la reclamante).

En el año de 1996, la señora Sara Castro Pérez se afilió a la Isapre[13] Banamédica, S.A., *-en adelante también Isapre Banmédica ó Isapre-* una de las instituciones que pertenecen al sistema de salud privado en Chile. Por su edad y las diversas patologías que se le habían diagnosticado y habían sido registradas en dicha Isapre, pertenecía al grupo conocido como "afiliados cautivos"[14]. Durante los años comprendidos entre 2003 y 2007 trabajó en la Unidad de Víctimas y Testigos en el Ministerio Público. Cabe señalar, que este cargo conlleva mucha

[13] Las ISAPRE son instituciones privadas que captan la cotización obligatoria de los trabajadores que libre e individualmente han optado. Estas instituciones otorgan servicios de financiamiento de prestaciones de salud a un 16% de la población en Chile. Los servicios de salud y el financiamiento de las licencias médicas por enfermedad se prestan con cargo a las cotizaciones. Las prestaciones de salud se entregan a través del financiamiento de las mismas mediante la contratación de servicios médicos financiados por las Isapres.

Chile cuenta con un sistema mixto de salud. Las instituciones de Salud Previsional ISAPRE nacieron en 1981 en virtud de la dictación del D.F.L. Nº 3 del Ministerio de Salud, dando origen a una de las más trascendentales reformas del sector. Ello permitió la administración privada de la cotización obligatoria de salud de los trabajadores, al mismo tiempo que se reconoció la libertad y capacidad de las personas para optar al Sistema de salud de su preferencia.

Las Instituciones de Salud Previsional, por tanto, sujetas a las reglas de libertad de mercado y a la libre iniciativa en salud, entregan el máximo de beneficios para ofrecer la mejor alternativa de servicios de salud a la población. El Estado, en cambio debe centrar su acción en coordinar las tareas de promover, proteger y permitir el acceso a la salud de las personas más necesitadas, así como velar porque estas acciones se desarrollen de acuerdo al nivel de eficiencia conforme a los avances científicos y tecnológicos disponibles.

Actualmente existen 13 Isapres, de las cuales compiten 7 abiertas.

Fuente: http://isapre.cl/Institucional.html

[14] COTIZANTE CAUTIVO, es aquel cotizante cuya voluntad se ve seriamente afectada por razones de edad, sexo o por la ocurrencia de antecedentes de salud, sea de él o de alguno de sus beneficiarios, y que le impida o restrinja, significativa o definitivamente, su posibilidad de contratar con otra Isapre.

presión psicológica. De este modo, la carga física y emocional afectó la salud de Sara Castro y en Febrero de 2007 se le diagnosticó una depresión severa mayor.

Esto significó que Sara Castro fuera derivada a la Red Cerrada de Atención de la Isapre Banmédica, acogiéndose así a las prestaciones GES[15] (ex AUGE). Esta situación, además, requirió diversos trámites para que se cumpliera con el acceso a las garantías que otorga este plan de salud.[16]

El médico que le diagnosticó la enfermedad estaba asociado a la Isapre. Sin embargo, Sara Castro no quedó conforme con el trato de este profesional y sólo asistió a dos consultas. Asimismo, decidió que seguiría su tratamiento en una consulta particular.

Debido al poco tiempo que hizo uso de la Red Cerrada de Atención, la paciente realizó un copago único a favor de la Isapre. Este copago único se tradujo un beneficio de salud que le aseguró el tratamiento y remedios asociados durante un año. El tiempo efectivo de este beneficio de cobertura cubrió el período de marzo de 2007 a marzo de 2008.

Cabe señalar que durante el tiempo que duró dicha cobertura, la Isapre le indicó a la señora Castro que debía presentarse con su cédula nacional de identidad en una sucursal de la Farmacia Cruz Verde, S.A. *–en adelante también Farmacia Cruz Verde ó la Farmacia-* ya que esta sería la farmacia que le entregaría sus medicamentos GES, situación derivada por la existencia de un convenio suscrito entre ambas entidades, de acuerdo a las averiguaciones realizadas posteriormente por la paciente.

El día 8 de abril de 2009, la señora Castro concurrió a una sucursal de la Farmacia Cruz Verde, se identificó como afiliada a la Isapre Banmédica y solicitó un descuento en la adquisición de medicamentos de otra índole. La dependiente le manifestó que no tenía derecho a dicho descuento y que de acuerdo a su R.U.T, el sistema informático indicaba que el beneficio de descuentos sólo cubría su cobertura de GES para su depresión severa mayor. Este diagnóstico fue repetido en tres ocasiones frente al público presente.

Frente a esta situación, le exigió a la dependiente que le explicará porqué tenía tal información médica catalogada como confidencial. La dependiente le respondió que ante cualquier duda o queja, debía reclamarle directamente a la Isapre. La señora Sara Castro no quedando conforme con dicha respuesta, solicitó conversar con el jefe de la sucursal de la farmacia, quien se limitó a manifestarle que lo comentaría con los abogados.

Hechos en dede administrativa.

Debido a que el diagnóstico de salud catalogado como confidencial, fue escuchado por personas presentes y colegas, la señora Castro argumentó que esta acción afectó gravemente su honra e imagen profesional, dado que dicha enfermedad es vista de forma estigmatizante,

[15] El AUGE-GES es un mecanismo fijado por Ley para priorizar garantías en la prevención, tratamiento y rehabilitación de enfermedades específicas que representan el mayor impacto de salud en la ciudadanía.

Fuente: http://www.supersalud.gob.cl

[16] Las Isapres, están habilitadas legalmente para efectuar tratamiento de datos sensibles relativos al estado o condición de salud de sus beneficiarios y/o ex beneficiarios, con el objeto de proceder a la determinación y otorgamiento de beneficios de salud que corresponda a los titulares de dichos datos.

Como consecuencia de lo anterior, las Isapres deben velar porque dichos datos sensibles sean utilizados sólo para los fines que han sido recolectados, en virtud de lo establecido en el artículo 9 de la Ley 19.628, entre otros aspectos relativos a dicha Ley.

la cual no era pública y había sido reservada por ella tanto a su círculo familiar como laboral y así evitar verse afectada en su vida profesional como abogada independiente y catedrática.

A consecuencia de este evento, el día 15 de abril de 2009, Sara Castro interpuso un reclamo administrativo en la Superintendencia de Salud, que ingresó con el N°. 7.200. Este reclamo era su manera de ejercer el derecho -que le confería la ley como afectada- establecido en el artículo 127 del D.F.L. No. 1 de 2005 del Ministerio de Salud. Este reclamo en lo particular solicitaba la eliminación inmediata del diagnóstico médico en la red de Farmacias Cruz Verde, S.A.

De este modo, el 17 de abril de 2009, la Superintendencia de Salud procedió a la fiscalización, entre otras, a la Isapre Banmédica, y a través ésta, se inspeccionó la plataforma de datos de una sucursal de la farmacia Cruz Verde, constatando la EFECTIVIDAD de la denuncia. Frente a este evento, el día 5 de mayo del mismo año, la Superintendencia instruyó[17] a la Isapre la eliminación de todos los datos sensibles que estuvieran a la vista de los dependientes de esta farmacia[18].

La Isapre respondió este requerimiento con una carta, donde informaba que la institución lamentaba profundamente tanto la situación ocurrida, como la molestia ocasionada. La Isapre en esta misiva enfatizaba que el resguardo de los antecedentes personales y la información que se relacionaba con los beneficiarios era manejado con la debida reserva y confidencialidad, y que para esta institución se trataba de un tema de permanente preocupación.

Aproximadamente un mes después, el día 12 de mayo, personal de la Superintendencia de Salud realizó simulaciones in situ en la venta de medicamentos a personas con beneficio GES. Se buscaba así verificar que en las pantallas donde acceden los vendedores de una sucursal de la farmacia Cruz Verde, se hubiese eliminado la descripción de la patología, y que sólo se mantuviera el código único[19] que identifica a cada problema de salud. La Superintendencia después de estas acciones, emite el oficio SSS/No. 4430 del 15 de mayo de 2009, donde informó al Gerente General de la Isapre Banmédica el debido cumplimiento de lo ordenado, hecho que se le comunicó con posterioridad a la señora Sara Castro.

Hechos en sede judicial.

Paralelamente al reclamo en la Superintendencia, Sara Castro tomó acciones legales. De este modo y según el Ingreso Número 6523-2009 de la Corte de Apelaciones de Santiago, el 8 de mayo de 2009, la señora Castro interpuso un Recurso de Protección, por infracción al artículo 19 N°4 de la Constitución Política de la República. Cabe señalar que este artículo se refiere a

[17] De acuerdo al oficio emitido por la Superintendencia de Salud No. 4443 de fecha 10 de junio de 2009, dicha institución no solo efectuó inspección en la Farmacia Cruz Verde, entidad denunciada, sino que realizó una fiscalización extraordinaria en distintas isapres abiertas, con la finalidad de recabar información sobre los contratos vigentes con farmacias, con el objeto de conocer el flujo de información entre las isapres y éstas para el otorgamiento de beneficios, especialmente de aquella información que puede revestir un carácter sensible según lo dispuesto en la ley No. 19.628.

[18] Con la inspección in situ realizada, la Superintendencia de Salud constató que en una sucursal de la Farmacia Cruz Verde, los encargados de la venta de medicamentos tenía a la vista la información relativa al problema de salud de los beneficiarios GES, específicamente de las ISAPRES BANMEDICA Y VIDA TRES, S.A.

[19] Con la diligencia efectuada, la Superintendencia verificó que al colocar el RUT del beneficiario, se desplegaba en la pantalla todos los convenios vigentes con la cadena de farmacias, dentro de los que se incluye el código GES, posteriormente con el RUT del prestador se capturaba la receta original, eliminándose de esta forma de la glosa descriptiva de la patología GES.

"El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia".

Este recurso se resolvió en la Quinta Sala de la Corte de Apelaciones de Santiago, la sentencia del 2 de noviembre de 2009 expresó: *"que lo reclamado por la parte actora, relativo a la transferencia de toda información sensible a la farmacia recurrida, fue finalizado a través de las gestiones hechas por la Superintendencia de Salud".*

La Corte de Apelaciones, entonces, argumentó que los hechos alegados donde se fundaba la acción habían sido tutelados durante el proceso de tramitación de dicho recurso, y que, ya habiendo finalizado el proceso administrativo, se adoptó por parte de la farmacia Cruz Verde, medidas convenientes para el resguardo de los derechos afectados.

Por otro lado, la Corte de Apelaciones explicó que con esta regularización –específicamente en lo referido al registro de datos confidenciales de Sara Castro- no existía en el momento providencia urgente alguna que la Corte pudiera resolver en protección de la parte actora, habiendo cesado el hecho que motivó a la pretensión incoada, concluyendo que el recurso interpuesto no pudo prosperar por no concurrir en la especie los fundamentos que lo hacen procedente, y en razón de ello, omitió por considerar improcedente, el análisis de las restantes alegaciones de las partes. Esta instancia, por lo tanto, resolvió rechazar la tramitación del recurso de protección de garantías constitucionales, al declararlo extemporáneo.

Posteriormente y según autos identificado con el Rol No. 87-2009, la parte afectada interpuso recurso de Apelación de la sentencia emitida. Esta sentencia fue confirmada en la Tercera Sala de la Corte Suprema, según consta en la sentencia pronunciada con fecha 21 de diciembre de 2009.

2. Derechos conculcados invocados.

La recurrente al interponer las denuncias y demandas correspondientes, principalmente se avocó a invocar la vulneración de lo dispuesto en las disposiciones legales que se indican a continuación:

- Artículo No. 2 letra g) de la Ley 19.628.
  (Concepto de datos sensibles).

- Artículo 10 de la Ley 19.628.

- Artículo 19 No. 4 de la Constitución.
  (Derecho al respeto y protección a la vida privada y honra de la persona y su familia).

3. Mapa de Actores.

GRUPO DE ACTORES SOCIALES	ACTOR	ROL EN EL PROYECTO	RELACION PREDOMINANTE	JERARQUIZACIÓN DE SU PODER
Clasificación de los diferentes actores sociales en un espacio preciso	Conjunto de personas con intereses homogéneos que participan en un proyecto o propuesta NOMBRE	Funciones que desempeña cada actor y el objetivo que persigue con sus accionar	Se define como las relaciones de afinidad (confianza) frente a los opuestos (conflicto) 1. A FAVOR 2. INDIFERENTE 3. EN CONTRA	Capacidad del actor de limitar o facilitar las acciones 1. ALTO 2. MEDIO 3. BAJO
Afectados	Señora Sara Castro (afectada directa) Afiliados de Isapre Banmédica con cobertura GES	Principal afectada por la revelación de información personal. Sin embargo, se determinó que existió un grupo considerable de afiliados a quienes se les había trasladado información sobre sus datos personales sensibles.	En contra Indiferente debido a la falta de conocimiento de la situación ocurrida	Inició diversos procesos administrativos y judiciales a través de la denuncia. Su poder está supeditado a las decisiones de las instituciones del estado participantes. No accionado
Empresas prestadoras de servicios de salud	ISAPRE Banmédica (En la investigación del caso también se evidencio dicha práctica por parte de la Isapre Vida Tres)	Entidad que por ley tiene autorización para resguardar información sensible de sus afiliados. Sin embargo en el caso traslada-cede a terceros tales datos (Farmacia Cruz Verde)	A favor	Las ISAPRES tienen una relación de ventaja ALTA ante un denunciante.
Farmacias	Farmacia Cruz Verde	Empresa que adquiere y conoce información personal de la afectada	A favor	La Farmacia Cruz Verde, tienen una ALTA cuota de poder.
Institución del Estado	Superintendencia de Salud	Ente regulador del sistema de salud chileno	Indiferente	Sólo se encarga de revisar/ verificar el cumplimiento o infracción de la ley. Tiene una cuota ALTA, dado que determina si se ha incumplido la norma.
Tribunales	Corte de Apelaciones de Santiago	Instancia Judical	Indiferente	Determina si hubo comisión de delito ante el caso expuesto. Tiene una cuota ALTA, dado que es quien determina a través de todas las pruebas presentadas, si deben ser sancionadas tanto la ISAPRE Banmédica como la Farmacia Cruz Verde.

Modelo de matriz tomado de Antonio Pozo Solís Lima, Febrero 2007[20]
Elaboración propia tomada a partir del análisis de noticias publicadas y lo resuelto en el caso.

[20] http://intranet.catie.ac.cr/intranet/posgrado/SA-508/1_Los%20actores%20de%20un%20territorio/3%20Mapeo%20de%20actores%20sociales.pdf

4. Descripción, análisis y comentarios de las actuaciones hechas por los vinculados, en cada etapa recurrida.

4.1. Etapa previa a la sede administrativa y a la sede judicial.

Señora Sara Castro.

El mismo día de ocurrida la situación en la sucursal de la farmacia Cruz Verde, la ofendida se presentó en la Isapre Banamédica, sucursal Agustinas 1022, para solicitar una explicación sobre la protección de su diagnóstico médico.

En dicho lugar no tenían formulario de reclamo, debido a dicha situación tuvo que manifestar su inconformidad de forma verbal con el jefe de la sucursal, a quien le solicitó la eliminación inmediata de su diagnóstico médico, de la red de atención de las Farmacias Cruz Verde.

Isapre Banmédica.

La Isapre no le brindó a la señora Castro el formato de reclamo vía escrito.

De conformidad con lo dispuesto en el artículo 127 inciso primero del DFL No. 1 de 2005 de Salud, la Isapre tenía la obligación de recibir por escrito dicho reclamo, violentándose en ese momento el derecho de petición a la usuaria.[21]

Asimismo, de acuerdo con lo establecido en el artículo 6 de la Ley No. 19.628, los datos personales deben ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.

Esta situación converge en el caso de la señora Castro, sin embargo, (no obstante haberse aducido la violación a la ley al transferir un dato sensible a un tercero sin mediar el consentimiento expreso de la titular, situación que se verá más adelante) la misma intentó hacer valer su derecho de cancelación de forma inmediata por constituir un dato caducado, situación que no fue posible debido a que la ISAPRE (la encargada por ley de registrar y proteger la base de datos como tal) no le brindó la oportunidad a la afectada de efectuar tal requerimiento.

En ese sentido se advierte que la Ley, no obstante indicar aspectos primordiales que el encargado de la base de datos debe cumplir, observamos que dicha regulación carece de los mecanismos idóneos para hacerla efectiva. Por lo que se determina la necesidad de tener un organismo competente y especializado que dirima estos conflictos de forma oportuna, que dicte las políticas públicas adecuadas, dejando siempre expedita la vía judicial para la indemnización por daños, establecido en el artículo 11 de la Ley 19.628.

[21] La actuación errónea de la Isapre de no recibir la solicitud de la ofendida, fue subsanada, debido a que el reclamo No. 7200-2009 que la señora Castro presentó directamente ante la Superintendencia de Salud fue derivado a la Isapre para que emitiera respuesta. Dicha respuesta fue brindada el 5 de mayo de 2009 en la etapa administrativa, lo que demuestra que el accionar los mecanismos previos a efecto de salvaguardar los derechos e intereses de los ofendidos no se encuentra suficientemente fortalecido.

Farmacia Cruz Verde.

A través del encargado de la sucursal se limitó a escuchar a la reclamante. Esto debido a que La Farmacia, no tiene la facultad legal para tratar datos sensibles.

En ese sentido la recurrente se encontró con la dificultad de no saber a cuál instancia inmediata recurrir para eliminación de sus datos frente a una entidad que no está facultada para tratarlos.

4.2. Sede Administrativa.

Señora Sara Castro.

El día 15 de abril de 2009, interpuso un reclamo ante la Superintendencia de Salud, marcado con ingreso No. 7200, instancia en la que solicitó la eliminación inmediata de su diagnóstico médico en la red de farmacias Cruz Verde.

El día 2 de mayo del mismo año, concurrió nuevamente a una sucursal (Militares) de la Cruz Verde y dictó su RUT a la dependiente, donde consultó directamente si aún era paciente GES con la patología asociada. Al respecto le respondieron de forma escueta que sí.

Isapre Banmédica.

Participación con la señora Castro.

Brindó la respuesta de fecha 5 de mayo de 2009 mediante nota al reclamo No. 7200-2009, presentada por la señora Sánchez en la Superintendencia de Salud, en los términos siguientes:

"Isapre Banamédica lamenta profundamente dicha situación y la molestia que ésta le ocasionó puesto que ha sido permanente preocupación para esta Isapre el resguardo de los antecedentes e información relativa a los beneficiarios, con el objeto que sea manejada con la debida reserva y confidencialidad.

Analizados los hechos, estos se debieron a la actuación inadecuada de una dependiente de la mencionada farmacia, proceder con el que estamos en absoluto desacuerdo, lo que fue manifestado expresamente por esta Isapre al represente de la Farmacia Cruz Verde."

De este comunicado[22] se deduce que la Isapre se declara como no vinculada por la situación suscitada, planteando que la problemática surgió por un proceder inadecuado de una dependiente de la farmacia y no por su propia actuación de compartición de datos.

De igual forma en la etapa administrativa respondió el reclamo hecho por la señora Castro, por derivación de la Superintendencia de Salud de acuerdo a lo establecido en el artículo 127 inciso primero del DFL No. 1 de 2005 de Salud, debido a que el derecho de petición de la usuaria le fue violentado con anterioridad, sin embargo con esta actuación se determina el mismo fue rehabilitado por Ley.

Participación ante la Superintendencia de Salud.

La señora Sara Castro interpuso dos reclamos:

[22] En dicho comunicado planteó que los procesos o la cadena de manejo de información no fue la adecuada.

1. Referencia 7200-2009, ingresado el 5 de mayo de 2009, cuya respuesta fue brindada por la Superintendencia Mediante nota SS/N° 1626 de mayo del mismo año.

2. Reclamo No. 9272, ingresado con fecha 13 de mayo de 2009, siendo respondido por la Superintendencia mediante el oficio No. 4443 de fecha 10 de junio del mismo año.

En razón de los reclamos planteados así como de la situación mediática y pública generada en torno al caso, con los informes de fiscalización realizados por las Superintendencia de Salud, emitió tres resoluciones exentas, la primera respecto a las situaciones encontradas en el proceso de fiscalización efectuado por dicha entidad, la segunda respecto a un recurso de reposición y la tercera relativa al recurso jerárquico, interpuesto de forma subsidiaria al recurso de reposición. Las dos primeras resoluciones fueron emitidas por el Intendente de Fondos y Seguros Previsionales de Salud y la tercera por el Superintendente de Salud. En dichas resoluciones se determinó principalmente lo siguiente:

Resolución	Contenido	Medida Adoptada	Multa Impuesta
Exenta I.F. No. 163 de fecha 30 de marzo de 2010	Se formuló un único cargo[23] a la Isapre Banmédica S.A.	Multa a la Isapre Banmédica, S.A.	100 Unidades de Fomento (UF) a beneficio fiscal.
Exenta I.F. No. 552 de fecha 16 de septiembre de 2010	Se tramitó el recurso de reposición interpuesto por la Isapre Banmédica, S.A.	Se acogió parcialmente el recurso interpuesto.	Se rebajó la multa impuesta de 100 UF a 30 UF
Exenta SS/No. 1480 de fecha 14 de octubre de 2010	Se rechazó el recurso jerárquico interpuesto de forma subsidiaria por la Isapre Banmédica, S.A. en contra de la Resolución Exenta I.F. No. 552.		

Contenido de las Resoluciones Exentas. Aspectos Destacados.

1) Imposición de la multa como resultado de la fiscalización.

De acuerdo a la resolución Exenta L.F. N° 163, de fecha 30 de marzo de 2010 emitida por la Superintendencia de Salud, durante la tramitación del reclamo administrativo interpuesto por la señora Sara Castro, dicha Superintendencia realizó diversas actividades de fiscalización, lo que derivó a que se formulara un único cargo a la Isapre Banmédica, S.A., consistente en: "*No arbitrar mecanismos suficientes para cumplir con la obligación de cautelar el derecho a la privacidad de la información transmitida a la Farmacia, irregularidad que transgrede lo dispuesto en el artículo N°5 de la Ley 19.628 sobre Protección de Datos de Carácter Personal".*

En ese sentido, tal imputación fue respondida por la referida Isapre, el día 21 de agosto de 2009, basándose esencialmente en cuatro alegaciones:
1. El cargo formulado es vago e impreciso, ya que no detalla los hechos concretos en que habría incurrido.

2. La Isapre está legalmente autorizada para tratar datos personales.

[23] Cargo consistente en *"No arbitrar mecanismos suficientes para cumplir con la obligación de cautelar el derecho a la privacidad de l información trasmitida a la Farmacia, irregularidad que transgrede lo dispuesto en el artículo No. 5 de la Ley 19.628, sobre Protección de Datos de Carácter Personal".*

3. La Isapre ha adoptado resguardos para asegurar el debido tratamiento de los datos personales que trasmite a farmacias Cruz Verde.

4. La situación denunciada más que una infracción, corresponde a una falta de tino del dependiente de la farmacia.

Respecto al primer punto, se determina que existe un Procedimiento que deben adoptar los seguros previsionales de salud frente a requerimientos de datos sensibles de sus cotizantes y beneficiarios, el cual se encuentra formulado en la circular IF No. 51, de fecha 22 de agosto de 2007. Por lo anterior, esta alegación debió haber sido desvirtuada por parte de la ofendida y por parte de la Superintendencia, sin embargo por tratarse de una circular la cual solo es para conocimiento de los vinculados en la misma, la señora Castro no podía estar enterada de su contenido, mas sí la Superintendencia.

En lo que respecta a la segunda alegación, esta carece de fundamento ya que la autorización que legalmente tiene la Isapre como tal para tratar datos personales nunca fue cuestionada por la reclamante, sin embargo farmacia a la cual se dirigió la señora Castro no está legalmente autorizada.

Sobre el tercer punto, y a pesar de ser este el cargo acreditado inicialmente por parte de la Superintendencia, lo importante y fundamental es que la Isapre no ha debido trasmitir datos, dado que la farmacia no está facultada ni legalmente, ni por los titulares de los datos para acceder a datos personales sensibles.

Finalmente en cuanto a la cuarta y última alegación, es posible establecer que la misma no constituye una argumentación válida, ya que la dependiente labora directamente para la farmacia, teniendo vinculación patronal y acceso a la información que dicha entidad le brinda como tal. Por lo que la Farmacia no puede desligarse del hecho que la dependiente tuvo acceso aquella información puesta a disposición para los empleados.

Es oportuno mencionar, que el contenido de la resolución en comento destaca la cláusula novena del convenio suscrito entre la Isapre Banmédica, S.A. y la Farmacia Cruz Verde, titulada "CONFIDENCIALIDAD", el cual se transcribe a continuación, para efecto de un posterior análisis en el presente estudio.

"Tanto las Isapres como la Farmacia reconocen y convienen el carácter confidencial del presente convenio, en especial de toda la información que sean entregado recíprocamente en función de la celebración del mismo. Ninguna de las partes podrá divulgar su contenido sin la autorización expresa de la otra parte.

En relación con la información que recíprocamente se entreguen las Isapres y la Farmacia, las partes declaran que es de propiedad de la parte que la genera, por lo que las Isapres, la Farmacia, sus dependientes o apoderados, no podrán copiar o utilizar la información para fines distintos a los que expresamente se establecen en este instrumento. Del mismo modo les está prohibido entregarla y darla a conocer a terceros ajenos al convenio, a menos que cuenten para ello con la autorización expresa, previa y escrita de parte propietaria y generadora de la información, sin perjuicio de la entrega que de ella se efectué a las empresas relacionadas a la Farmacia, esto es exclusivamente a CESFAR LTDA., a propósito de la orientación oncológica para los beneficiarios y a VISSION LTDA:, para efectos de administrar el programa informático en la aplicación de los beneficios objeto del presente instrumento.

Las partes acuerdan otorgar el carácter de esencial a la presente cláusula de modo que su incumpliendo faculta a las Isapres y a la Farmacia, para poner término inmediato al presente convenio".

Tal como es posible inferir, a raíz de dicho convenio, la Isapre Banmédica, trató de respaldar la transferencia de datos privados sensibles, relativos al diagnóstico clínico no solo de la señora Sara Castro, sino también de los demás afiliados, situación que no tiene razón de ser, debido a que la transmisión de datos con estas características se encuentran regulados por la ley, situación que de acuerdo a lo establecido por la Superintendencia de Salud en la resolución de mérito, *"no releva en absoluto a Isapre Banmédica, S.A. de su deber de cautela de los datos sensibles de sus beneficiarios establecido en la Ley No. 19.628."*

2) Recurso de Reposición.

En el recurso de reposición interpuesto el día 9 de abril de 2010, en contra de la Resolución Exenta No. 552, la Isapre Banmédica, S.A., fundó el mismo bajo los argumentos siguientes:

a) Existió una incongruencia entre el único cargo formulado por la Superintendencia en el procedimiento sancionatorio, consistente en una omisión por no arbitrar los mecanismos suficientes para cautelar el derecho a la privacidad de la información transmitida a la Farmacia Cruz Verde, en relación con la sanción impuesta consistente en una acción distinta, el haber comunicado datos sensibles en exceso e innecesarios para la entrega de medicamentos.

Cabe señalar que sobre este punto, la Superintendencia resolvió que dicha incongruencia era más bien aparente, toda vez que el cargo se fundó en el hecho que la Isapre no había arbitrado los mecanismos necesarios para cumplir con la obligación de cautelar el derecho a la privacidad de la información enviada a la farmacia, al incluir en la transmisión efectuada, datos sensibles relativo a los problema de salud GES de sus beneficiarios, adoptado de esa forma una conducta poco diligente, en cuanto daba cabida a una eventual violación del derecho a la privacidad de los afectados –por parte de la farmacia- en virtud de que la referida información NO ERA INDISPENSABLE PARA LA ENTREGA DE MEDICAMENTOS. Se evidencia por tanto, que no se actuó con rigurosidad al definir los mecanismos de transmisión de los datos de los beneficiarios.

"b) El cargo formulado se refirió a una situación general y la resolución recurrida sancionó una conducta específica."

Frente a este punto, la Superintendencia indicó que la sanción aplicada efectivamente tenía fundamento en una conducta genérica, no obstante haberse iniciado el procedimiento sancionatorio por una conducta específica referida por denuncia de la señora Castro.

"c) *La resolución emitida no analizó las pruebas que acreditarían la supuesta infracción, ni tampoco las presentadas por Banmédica, S.A."*

Complementando lo anterior, debido a que la resolución no señaló las pruebas referidas a la infracción al derecho de privacidad de la señora Castro en la supuesta comunicación en exceso, dado que sólo hizo referencia a una fiscalización realizada el 17 de abril de 2009 en la que no se nombró a la afiliada.

Asimismo, la Isapre arguyó que la resolución no tomó referencia alguna a la prueba documental y testimonial rendida para desvirtuar el supuesto de no haber arbitrado los

mecanismos para la cautelar la privacidad de las personas en la entrega de información, especialmente en cuanto al informe de Seguridad de Transmisión de Datos realizado por ENTEL, en el que se concluye que existen mecanismos que otorgan seguridad y la garantía adecuada para proteger la privacidad de la información transmitida.

Sin embargo, al respecto podemos determinar que la Isapre claramente confundió que los mecanismos a instalar eran sobre el tipo de transmisión de los datos enviados en línea mediante enlace dedicado a la Farmacia. Mientras que, por el contrario, los mecanismos o procedimientos se referían a no proporcionar información personal de sus afiliados. Esto demuestra una dificultad de lineamientos específicos que el encargado de manejar la base de datos personales debe tener presente, sin imprecisión alguna, aspecto relevante que la política pública sobre protección de datos personales debe prever e incorporar.

Por otra parte, cabe señalar que referente a la FALTA DE PONDERACIÓN DE LAS PRUEBAS VERTIDAS EN EL PROCESO para dictar la resolución impugnada, la Superintendencia aclaró que si bien la Isapre acreditó que la información se enviaba de forma encriptada a la farmacia, con la existencia de controles pertinentes para que terceros no violaran el proceso de transmisión, *"la prueba rendida por la Isapre no resultó suficiente para desvirtuar el incumplimiento de la obligación de cautelar el derecho a la privacidad de los beneficiarios, al no justificar que la remisión del dato sensible relativo al problema de salud que los afectaba, fuera necesario para la entrega del medicamento*".(subrayado es nuestro).

Lo anterior, nos llevaría a deducir que ocurrió no solo por la falta de educación, difusión, y conocimiento inequívoco sobre el derecho de protección de datos personales, sino también por la inexistencia de un órgano independiente, especialista en la materia, que promulgue y divulgue los aspectos necesarios tanto para los titulares de los datos como para los responsables de bases de datos y su manejo. Esto sería, en síntesis, un ente independiente y regulador de la ley.

d) La resolución recurrida sanciona una supuesta conducta "poco prudente", y no una infracción legal o reglamentaria específica y concreta, violando el principio de legalidad de los actos de la administración y de tipicidad respecto de la facultad sancionatoria.

Tal argumentación denota una clara y manifiesta necesidad de contar con una Ley que contenga un ente especialista y conocedor de la materia.

Al respecto, la Superintendencia de Salud, determinó que, "*en tal contexto, corresponde señalar que la sanción aplicada a Isapre Banmédica tiene efectivamente su fundamento en una conducta genérica, no obstante haberse original el proceso sancionatorio en una conducta específica referida a la señora Castro, quien efectuó una denuncia debido a que la dependiente de la farmacia señaló a viva voz su problema de salud, cuyo resultado fue informado a Isapre Banmédica a través del Oficio SS/N° 1319 de 5 de mayo de 2009."*

"e) Si la Autoridad reconoce la facultad de la Isapre para tratar datos sensibles en la determinación de un beneficio de salud, no puede luego sancionarla por haberla ejercido de una manera u otra, si no existe una normativa que regule la materia."

En este punto, se observa que si bien existe una ley en la materia, siendo la Ley 19.628, la misma carece de los componentes y mecanismos idóneos que la hagan prevalecer y ejecutar debidamente.

"f) La eventual "entrega de información e datos sensibles en exceso", no puede constituir una infracción al artículo 5 de la Ley 19.628, toda vez que esta norma sólo autoriza al responsable del registro o banco de datos a establecer un procedimiento automatizado de transmisión de datos y no se refiere a la mayor o menor extensión de los mismos."

"g) La información transmitida o disponible en línea es la estrictamente necesaria para otorgar un beneficio de salud y jamás se ha transmitido un diagnóstico clínico."

Al respecto, al analizar lo planteadose determina que el beneficio de salud es otorgado al beneficiario al momento de acogerse como paciente GES, sin embargo se estableció una interpretación errónea por parte de la Isapre Banmédica, S.A., al entender que la ejecución de dicho servicio, entiéndase la entrega de medicamentos, se refiere al otorgamiento de un beneficio de salud.

Finalmente, la Isapre Banmédica, S.A., solicitó al Intendente revisar la nomenclatura que utiliza la resolución recurrida, debiendo eliminarse toda referencia a "diagnóstico clínico". En ese sentido indicó que la información transmitida fue la relativa a los aspectos siguientes:

i. Individualización de la Isapre.
ii. Individualización del beneficiario a través de su nombre y RUT.
iii. Código asociado a una determinada canasta de medicamentos, que es la que corresponde según la cobertura GES a la patología que se trate.
iv. Número de solicitud GES.
v. Período asociado al beneficio.
vi. Prestador autorizado.

De igual forma reiteró que la información concerniente al problema de salud se entrega mediante código, no con palabras, de modo tal que la entrega de Banmédica a la Farmacia Cruz Verde es un simple número codificado sin incluir información adicional o ajena a la prestación de salud que se otorga al beneficiario.

Sin embargo, de acuerdo a la actividad de fiscalización efectuada por la Superintendencia de Salud, se verificó en la pantalla que utilizaban las dependientes de la Farmacia Cruz Verde, la asociación del diagnóstico clínico de la señora Sara Castro, diagnóstico que de conformidad a la ley, no tiene derecho a tener conocimiento la Farmacia.

Para concluir sobre este aspecto, se puede señalar que la Superintendencia determinó que *"se encuentra facultada para fiscalizar y sancionar a la Isapres que incurran en infracciones acreditadas por este Organismo, conforme al artículo 110 del DFL No. 1 de Salud, cuyo N° 4 establece la facultad de velar porque las instituciones fiscalizadas cumplan con las leyes y reglamentos que rigen y con las instrucciones que la Superintendencia emita".*

Debido a lo anterior las Isapres deben sujetar su actuar, entre otras, a las normas de la Ley No. 19.628 que establece la obligación de protección a la vida privada por parte de quienes están autorizados para transmitir datos personales y en especial respecto de quienes manejan datos sensibles, teniendo en consideración que los datos relativos a la salud de los individuos son sensibles y su insuficiente protección puede llevar a su uso no autorizado ó a su revelación a terceros.

De igual forma aunque no se cuente con un procedimiento definido para el tratamiento de datos sensibles, las instituciones deben ser diligentes en el manejo de los mismos, por lo que la entrega de información cuestionada de la Isapre a la farmacia no fue acertada.

Por otra parte señala que el artículo 5° de la Ley 19.628 dispone*: "el responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes".*

En base a lo anterior, es posible mencionar que el convenio suscrito contiene una cláusula de confidencialidad que debía ser cumplida por la Farmacia. Sin embargo, y tal como se señaló en la resolución recurrida, esta cláusula no releva a la Isapre Banmédica, S.A. de su deber de adoptar los mecanismos suficientes para cautelar los datos sensibles de los beneficiarios, obligación determinada por ley.

De igual forma la Superintendencia determinó que en razón de las diligencias efectuadas, *"se dictaron normas para que las isapres adoptaran los resguardos debido en relación con traspaso de información sensible de sus beneficiarios a establecimientos privados de venta, arriendo, distribución o entrega de artículos, insumos/o medicamentos de apoyo terapéutico".*

Dichas normas se comentarán más adelante, a efecto de determinar los resultados de las mismas.

Por lo que en este apartado se concluye, que la Superintendencia entró a pronunciarse sobre las obligaciones existentes entre las partes, Isapre y Farmacia, determinando que la farmacia no cumplió a cabalidad con las mismas. Al respecto, cabe la acotación que la Superintendencia debió ser más enfática en argumentar que dicha cláusula es contraria al orden público específicamente en cuanto a la transmisión de datos sensibles. La Isapre se valió de dicha cláusula para permitir la transmisión de los datos sensibles a la Farmacia Cruz Verde, actuación que durante el proceso ventilado en sede administrativa argumentó que fue no fue realizado de forma directa, sino que a través de códigos encriptados, que fueron descifrados para determinar un tipo de canasta de medicamentos a la que los beneficiarios tenían opción dentro de su cobertura de salud. Sin embargo, pudo constatarse que esto no fue así, debido a que la Farmacia poseía el diagnóstico específico de cada paciente afiliado.

Farmacia Cruz Verde.

El día 26 de mayo de 2009 emitió una declaración pública[24], manifestando:

"1. Solo recibimos de las Instituciones de Salud Previsional la información básica necesaria que permite a éstas otorgar, a través de Cruz Verde, los medicamentos e insumos farmacéuticos a sus afiliados y/o cargas de familia, exclusivamente cuanto receptores de los beneficios de salud contemplados en la Ley 19.966 sobre el Régimen General de Garantías en Salud y su normativa complementaria.

2. La información básica recepcionada por nosotros no contempla ningún otro dato o información que no sea la necesaria al objeto señalado, por lo cual en ningún caso comprende diagnósticos o fichas médicas de los afiliados de las respectivas instituciones de Salud Previsional.

[24] La declaración pública fue emitida en periódicos de mayor circulación nacional, siendo oportuno resaltar que a nuestro criterio, se debió a la connotación mediática y notoria del caso suscitado en razón de la denuncia de la señora Sara Castro, lo que permitió destapar "la punta del iceberg" relativo a la transferencia de datos personales sensibles.

Los medios de comunicación ejercieron un papel importante y de presión, sin embargo los resultados finales no han sido totalmente los esperados para la mejora actual de la política pública.

3. En Cruz Verde utilizamos esta información básica exclusivamente para dar cumplimiento a lo contemplado en la legislación vigente y conforme a los convenios suscritos con las Instituciones de Salud Previsional."

Sin embargo, el envío de datos no se refirió sólo a información básica, ya que también se remitieron datos sensibles, sin mediar el consentimiento de los titulares.

Adicionalmente, la Superintendencia de Salud en la resolución No. 163, sostuvo que la Farmacia (a nuestro criterio, no estando facultada por ley pero con la información sensible transmitida en sus bases) no tuvo el cuidado suficiente para el resguardo de los mismos, colocándolos de forma negligente a la vista de todas las dependientes de las sucursales.

En el convenio suscrito entre la Isapre Banmédica, S.A. y la Farmacia Cruz Verde -documento de que no se logró tener acceso[25] para el presente estudio, a pesar de las gestiones realizadas para ello-, las Isapres deben colocar restricciones sobre el envío de esta información. Asimismo, no es posible convenir de forma privada sobre aspectos que ya están específicamente regulados por ley.

La Farmacia Cruz Verde, recibió una fiscalización indirecta de la Superintendencia de Salud, debido a que funcionarios de dicha entidad se presentaron en una sucursal para verificar los registros de la pantalla, a efecto de constatar de que se había eliminado el diagnóstico clínico de los afiliados, según el oficio No. 1319 de fecha 5 de mayo de 2009.

Cabe señalar que éste es otro vacío existente en la legislación, ya que la Farmacia no está autorizada por el titular para el tratamiento de datos sensibles y no es posible ordenarle rectificar datos de su base como si fuera el encargado o responsable, debido a que ésta no debió tenerlos disponibles, por no estar facultada por ley.

Superintendencia de Salud.

<u>Análisis de las resoluciones emitidas en la fiscalización realizada.</u>

Mediante la resolución Exenta I.F. No. 163 de fecha 30 de marzo de 2010, provista por el Intendente de Fondos y Seguros Previsionales de Salud, la Superintendencia de Salud determinó lo siguiente:

La Superintendencia de Salud realizó el día 17 de abril de 2009 una fiscalización en una sucursal de la farmacia Cruz Verde, constatando que efectivamente en la pantalla de los equipos computacionales de los dependientes, figuraba el diagnóstico de los beneficiarios de Isapre Banamédica e Isapre Vida Tres, acogidos al Régimen de Garantías Explícitas en Salud.

[25] Según resolución Exenta SS/N° 2007 de fecha 27 de diciembre de 2011, emitida por la Superintendencia de Salud, acogiéndose a lo dispuesto en el inciso tercero del artículo 20 de la Ley No. 20.285, al encontrarse impedida de entregar los documentos "Convenio Farmacia Cruz Verde e Isapre Banmédica, S.A." y "Convenio de Colaboración Farmacia Cruz Verde e Isapre Vida Tres, S.A."

Con anterioridad se pidió a la Superintendencia toda información relacionada al caso de la señora Sara Castro, sin embargo de acuerdo a la resolución Exenta SS/No. 1805 de fecha 16 de noviembre de 2011, dicha entidad determinó que dada las características del expediente, y que el en su contenido se hace referencia constante a datos relacionados con el estado de salud y la vida privada de las señora Castro, no resulta posible entregar ni aún parcialmente la información requerida por la señora Barrera, resolviendo rechazar la solicitud de la información requerida por Tania Barrera Quintanilla, atendida la causal de secreto o reserva estipulada en el artículo 21 No. 2 de la Ley de Transparencia.

Por lo que posteriormente mediante ORD. SS/N 1319, de fecha 5 de mayo de 2009, se instruyó a Isapre Banmédica, S.A. y también a Isapre Vida Tres, S.A.[26], eliminar del acceso de las dependientes de la farmacia, toda información referida a datos sensibles de los beneficiarios, instrucción que Isapre Banmédica cumplió a cabalidad , según da cuenta el ORD. SS/N°2406, de fecha 10 de agosto de 2009, del Departamento de Control y Fiscalización de la Superintendencia de Salud.

Cabe destacar lo indicado en el oficio ORD SS/N 1319, el cual se cita a continuación.

"Los resultados de la fiscalización se encuentran contenidos en el informe que se adjunta, el que da cuenta de los convenios *entre esas Isapres Banmédica y VIDA TRES y Farmacia Cruz Verde y de los flujos de información entre ellas.*

Asimismo, se revisó en una sucursal de la Farmacia en convenio, la información disponible en las pantallas que individualizan los beneficios a los que puede acceder los beneficiarios al momento de requerir los medicamentos, determinándose que para el beneficio GES, se indica el código para el problema de salud y la descripción del problema, a modo de ejemplo, en el caso de la reclamante se visualiza la siguiente glosa: problema de salud XXXXX, tratamiento XXXXX.

Cabe hacer presente que, conforme con lo dispuesto en la letra g) del artículo 2 de la Ley No. 19.628 son datos sensibles "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" En ese orden de ideas, el artículo 7 establece que "Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo".

Por su parte, el artículo 11 es preciso al señalar que "El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

A mayor abundamiento, el artículo 23 establece que "La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal".

[26] Con la fiscalización efectuada por la Superintendencia de Salud, salió a relucir que la ISAPRE VIDA TRES, S.A., también había transferido datos de sus beneficiaros a la cadena de farmacias, siendo dicha práctica efectuada de forma constante, reiterada y sin control previo al caso de la señora Sara Castro. La Isapre Vida TRES, S.A. también fue multada, bajo el mismo único cargo formulado a la Isapre Banmédica, S.A. En base a lo anterior se multó con 50 U.F., mediante la Resolución Exenta I.F. No. 162 de fecha 30 de marzo de 2010, la cual fue recurrida por la Isapre Vida Tres, S.A, según recurso de reposición, resuelto por la Superintendencia de Salud en la Resolución Exenta I.F. 551 de fecha 16 de septiembre de 2010, en la que se acogió parcialmente el recurso interpuesto, dejándose sin efecto dicha multa.

La Isapre Vida Tres, S.A. interpuso en subsidio al recurso de reposición, un recurso jerárquico ante el Superintendente de Salud, el cual fue resuelto en la Resolución Exenta SS/N° 1481 de fecha 14 de octubre, en el que el Superintendente de Salud determinó rechazarlo.

En atención a lo expuesto, instruimos realizar las gestiones tendientes a la eliminación de todos los datos sensibles que estén a la vista de los dependientes de las Farmacias Cruz Verde en un plazo máximo de 3 días contados a partir de la fecha de notificación del presente Oficio, lo que posteriormente será monitoreado por este Organismo de Control.

Asimismo en virtud de lo anterior, las Isapres Banmédica y Vida Tres deberán arbitrar los mecanismos y procedimientos necesarios para el debido resguardo del cumplimiento de la Ley 19.628".

Posteriormente, bajo tal actuación verificada, la Superintendencia formuló un único cargo a la Isapre Banmédica, S.A., consistente en "No arbitrar mecanismos suficientes para cumplir con la obligación de cautelar el derecho a la privacidad de la información transmitida a la Farmacia, irregularidad que transgrede lo dispuesto en el artículo N°5 de la Ley 19.628 sobre Protección de Datos de Carácter Personal".

Finalmente como se había indicado con anterioridad, la Superintendencia de Salud resolvió multar a la ISAPRE Banmédica, S.A. con 100 Unidades de Fomento (UF) – multa que posteriormente fue modificada a 30 Unidades de Fomento por el recurso de reposición interpuesto en contra de la citada resolución. Dentro de las valoraciones que hizo dicha resolución y que se consideran pertinentes resaltar, se establecen las siguientes:

1. Aclaró que si bien la ley otorga una mayor protección a los datos sensibles, el artículo 10 de la Ley No. 19.628, autoriza expresamente a las Isapres a tratar datos sensibles de sus beneficiarios, desde que es necesario para la determinación u otorgamiento de los beneficios de salud que correspondan a los titulares de dichos datos.

Lo anterior fue establecido a partir de lo que prescriben los artículos 171, 173, 174, 184 y 189 del DFL No. 1 de Salud de 2005, en cuanto a que es giro privativo de las Isapres, con cargo a la cotización para salud, el financiamiento de prestaciones y beneficios de salud, previa suscripción de un contrato de salud previsional de plazo indefinido. Por lo que determinó que, *"De consecuencia, la facultad legal de Isapre Banmédica, S.A. para tratar datos sensibles de sus beneficiarios es indiscutida y en todo caso ha sido de pleno conocimiento de esta Intendencia."*

2. Tuvo a la vista el convenio suscrito entre la Isapre Banmédica, S.A. y la Farmacia Cruz Verde, de fecha 29 de junio de 2005, documento que revisó y analizó, lo que le permitió determinar las vinculaciones de ambas entidades referentes a un acuerdo privado respecto al tratamiento sobre la información de los beneficiarios de la Isapre.

En dicho análisis se destaca la cláusula novena relativa a la CONFIDENCIALIDAD, anteriormente transcrita en este estudio de caso, en la que se le brindó tal carácter a dicho convenio, "*en especial respecto de toda información que se han entregado recíprocamente en función de la celebración del mismo, por lo que ninguna de las partes podrá divulgar su contenido sin la autorización expresa de la otra parte."* En este punto, la cláusula regula la confidencialidad de la información entregada uno a otro contemplando la posibilidad de compartirla o divulgarla con terceras personas, sólo con autorización expresa y previa de la contraparte. Dicho pacto, es completamente atentatorio, ya que como se afirmó con anterioridad no es posible pactar en contra de lo indicado en la ley, y aunque específicamente no versan o no atañe sobre datos sensibles, las alegaciones y justificaciones hechas por la Isapre Banmédica, S.A. giraron en torno a lo dispuesto en el convenio.

Por otra parte, si bien, no fue posible tener acceso a dicho convenio para la revisión completa del mismo, algunos medios de comunicación expresaron en el momento de notoriedad pública que obtuvo el caso, que de acuerdo a cláusulas adicionales establecidas en dicho documento, con los datos de los beneficiarios de las Isapres que adquirían medicamento en las farmacias se formaron registros de consumo. Estos registros posteriormente se transferían, con fines comerciales y se establecían perfiles de consumo, Para el caso citamos una parte de la noticia encontrada en el período La Nación[27]:

"Los antecedentes obtenidos serán proporcionados al fiscal que investiga la colusión en el caso farmacias, con el objetivo de abrir una nueva arista en este caso.

Además del convenio, en el juicio que está en curso y que se vio el martes pasado en tribunales, se accedió a documentos donde figuran todas las compras que realizó XXXXX, desde pañuelos desechables hasta fármacos, lo que permite elaborar un completo perfil de la paciente.

Los denunciantes explicaron que las isapres y farmacia pueden establecer convenios para comprar y distribuir medicamentos del AUGE para optimizar el servicio a los clientes, pero lo que no pueden hacer es violar la privacidad de las personas.

"Cuando leí el documento me entero que el convenio no se circunscribe a AUGE, sino que también posibilita la emisión de informes sobre consumo", dijo la abogada. Lo anterior se establece en la letra K del documento, firmado el 29 de junio de 2005 y que obliga a la emisión mensual de reportes.

Al cierre de esta edición, por medio de un comunicado, ambas isapres y la farmacia aclararon que "ha convenido las estipulaciones estrictamente necesarias para otorgar debidamente los beneficios (...) y sólo se utilizan para efectos de cumplir con las exigencias de la Superintendencia de Salud".

Asimismo, notamos con relación a la información que recíprocamente se entreguen las Isapres y la Farmacia, que las partes determinaron que la misma será de propiedad de la parte que la genera, por lo que las Isapres, la Farmacia y sus dependientes o apoderados no podrán copiar o utilizar la información para fines distintos a los que expresamente se establecen en dicho instrumento.

En base a lo anterior, es posible indicar que existió un tratamiento inadecuado de la titularidad de los datos, debido a que las partes aducen en el convenio que la información es propiedad de quien la genera, obviando la particularidad que, si se refiere a datos personales y más si versa sobre datos sensibles tienen un tratamiento especial, debiendo contar indefectiblemente con el consentimiento del titular. Para el caso, la titularidad del diagnóstico clínico de un paciente afiliado al régimen GES, éste debe pertenecer al propio paciente, mientras que el acceso de la Isapre a este diagnóstico se explicaría únicamente para que dicha institución determine u otorgue de beneficios de salud, especialmente en la entrega de medicamentos, conforme al principio de finalidad. La Isapre no es la titular de dichos datos y, con mayor razón, por considerarse un dato sensible el cual debe procurase un mayor resguardo y protección.

[27] Fuente: http://www.lanacion.cl/acusan-a-isapres-y-farmacia-de-trafico-de-informacion/noticias/2009-09-16/230322.html

Por otra parte, la resolución en referencia analizó lo dispuesto en el "Anexo C - Operatividad" del Convenio, el cual contempla el procedimiento para la adquisición y entrega de medicamentos el cual sólo requiere la entrega de un bono emitido por la Isapre y la presentación de la cédula de identidad del beneficiario, determinando la Superintendencia que el haber comunicado el diagnóstico clínico de la señora Castro Pérez la cadena de farmacias Cruz Verde constituyó un incumplimiento al deber de reserva de los datos sensibles, proporcionando información innecesaria para el cumplimiento de la entrega del medicamento.

3. Justificó de cierta forma la necesidad de suscripción de un convenio entre las Isapres y las farmacias para el cumplimiento de la entrega de medicamentos, ya que de conformidad con el artículo 123 del Código Sanitario la venta al público de productos farmacéuticos para uso humano solo puede hacerse a través de las farmacias, por ende las Isapres se encuentran legalmente impedidas de cumplir directamente la entrega de los medicamentos.

4. Estableció que, "*la transmisión de ciertos datos personales de los beneficiarios de Banmédica S.A., es imprescindible para el cumplimiento del Régimen GES, de manera que la información que deba remitirse a la farmacia, debe ser estrictamente necesaria para permitir la entrega del medicamento, quedando obligada legalmente la Isapre a resguardar y cautelar la reserva de la restante información de sus beneficiaros*".

En ese sentido, *"la remisión del diagnóstico clínico que por esencia es un dato sensible, no es una información que la Isapre Banmédica, S.A., debió haber comunicado a la farmacia, pues la obligación de ésta última, es sólo verificar en la entrega de los medicamentos la identificación del beneficiario designado o a quien lo represente con su cédula de identidad.",* conforme a lo pactado por las partes en la letra n) de la cláusula tercera del convenio.

Sobre las anteriores argumentaciones, se plantea la idea que, si la Superintendencia determinó que este tipo de documentos debe mediar entre los prestadores de servicios para el efectivo cumplimiento del régimen de salud, y en la resolución de mérito entró primeramente analizar lo pactado por las partes del convenio, para determinar el no cumplimiento a cabalidad de lo estipulado por el mismo, Dado que esto no fue así, cabe preguntarse entonces ¿Porqué la Superintendencia no determinó –desde un inicio- establecer un mecanismo de revisión o de control previo de los mismos en todo caso, específicamente a las áreas que por legislación dichas entidades deben acatar? esto se menciona ya que al analizar la resolución de mérito, se observa que la Superintendencia revisó lo pactado en el convenio.

5. Dicha resolución destaca que la *"circunstancia que por convenio se haya estableció el deber de confidencialidad de la información que recíprocamente se entregarían las partes, no releva en absoluto a la Isapre Banmédica, S.A. de su deber de cautela de los datos sensibles de sus beneficiarios, deber establecido en la Ley 19.628."*

Al respecto, determinamos que, tanto en la elaboración como en la ejecución del contrato de salud previsional que suscriben las Isapres, están deben observar las normas de cumplimiento de las obligaciones que se establece la legislación adicional vinculada a sus actividades, fortaleciendo la argumentación que hasta hoy se ha venido manejando.

Teniendo todos estos elementos de juicio a la vista, el Intendente concluyó que debió restringirse al mínimo necesario la comunicación de datos sensibles, transmitiéndose solo aquellos estrictamente imprescindibles para el suministro del medicamento prescrito.

Cabe señalar que la Superintendencia primeramente hizo un análisis de lo establecido en el Convenio. Dicho convenio estableció la confidencialidad entre las partes sobre los datos a transmitirse por las mismas. La transmisión de datos sensibles, por tanto, sobrepasa este acuerdo.

Por otra parte, en la ejecución de dicho convenio para la entrega de los medicamentos, se estableció que sólo se requerirá la entrega del bono emitido por la Isapre y la presentación de la cedula de identidad del beneficiario (ó la presentación de una receta médica cuando son medicamentos controlados), situación claramente obviada por las entidades vinculadas.

Finalmente, se concluye que lo ahí estipulado no inhibió a la Isapre de su obligación de protección de los datos de sus beneficiarios, traspasando información innecesaria para el cumplimiento de su deber como proveedora del servicio, situación que es de suma gravedad, más aún cuando versa sobre datos sensibles y que corresponden no solo a la denunciante, sino también a un grupo extenso de beneficiarios de dos Isapres.

Ahora bien, como se mencionó con anterioridad, contra dicha resolución, la Isapre Banmédica interpuso el día 9 de abril de 2010 un recurso de reposición, el cual fue tramitado y resuelto según la Resolución Exenta No. 552 de fecha 16 de septiembre de 2010, emitido por el mismo Intendente de Fondos y Seguros Previsionales de Salud.

Dicho proveído determinó: *"ACOGER PARCIALMENTE el recurso interpuesto por la Isapre Banmédica, S.A., rebajando la multa impuesta ascendente a 100 UF, a una multa de 30 UF, en consideración a los fundamentos expuestos en el considerando 10 precedente".*

Es importante destacar que al momento de adoptar dicha resolución, la señora Castro estaba ventilando un Recurso de Protección ante la Corte de Apelación de Santiago, por vulneración a lo dispuesto en el artículo 19 No. 4 y no. 1 de la Constitución Política, del cual se desarrollará más adelante.

Ahora bien, la resolución de la Superintendencia de Salud, en cuanto al recurso de reposición adoptó básicamente lo siguiente:

"1) Tal como expresa la recurrente, a la época de la fiscalización no había un procedimiento regulado que indicara expresamente cómo debía hacerse la transmisión de información por parte de las Isapres a terceros que otorgan prestaciones a los beneficiarios de esas instituciones y, no obstante que se ha estimado que la Isapre Banmédica proporcionó datos innecesarios para entrega de los medicamentos, esta Intendencia no puede desconocer que la responsabilidad principal en la situación que afectó a la señora Castro, recae en la farmacia.

Cabe tener presente que a propósito de la situación en análisis, se dictaron normas para que las Isapres adoptaran los resguardos debidos en relación con el traspaso de información sensible de sus beneficiarios a establecimientos privados de venta, arriendo, distribución o entrega de artículos, insumos y/o medicamentos de apoyo terapéutico.

2) (...) respecto a la falta de tipificación de las faltas administrativas, este Intendente ha de tener en consideración que no se ha vulnerado en la especie una norma específica en relación con la cautela de la privacidad de los datos sensibles de los afiliados a la Isapre Banmédica, sino más bien, dicha institución ha incurrido en una conducta poco diligente, que no atentaba por sí misma contra esa privacidad, sino que constituía un riesgo frente a la

utilización que pudiera hacer de la información, un tercero que también estaba obligado a cautelar dichos intereses."

Sobre este punto, permite generar confusión y controversia a la vez, ya que la Superintendencia se contradice, dado que el tercero que indica (Farmacia Cruz Verde) no es quien está obligado a cautelar dichos intereses, sino más bien este tercero nunca debió tener acceso a la información del diagnóstico proporcionado por la Isapre. Por lo tanto, la vinculación de la Farmacia en la cadena de participación no contrarresta o disminuye en todo caso la violación al resguardo que la Isapre debía tener para con los datos de sus afiliados.

Por otra parte, se indica que la Isapre no había vulnerado la cautela de la privacidad de los datos sensibles, sino más bien había incurrido en conducta poco diligente, conducta que si bien no atentó contra la privacidad, si constituyó un riesgo por la utilización derivada de hacerse con la información En este sentido cabría preguntarse ¿Dónde queda la vulneración que tuvo la señora Sara Castro? Si por la queja de dicha administrada fue que se inició el proceso relativo a la fiscalización hecha a las Isapres por dicha circunstancia. La recurrente indicó cómo la situación ocurrida afectó su salud, así como también las posibles repercusiones en el ámbito social y familiar. Indudablemente, la situación no fue sólo un riesgo posible, fue una situación que efectivamente atentó contra la privacidad de la recurrente y la prueba fehaciente de ello fueron las múltiples denuncias de la señora Castro, hechas en las distintas sedes a las que los procedimientos habilitados le permitieron acceder.

3) De acuerdo con la instrucción hecha en el Oficio No. 1319, la Superintendencia ordenó realizar gestiones para la eliminación de todos los datos sensibles que estuvieran a la vista de los dependientes de la Farmacia. Asimismo la Superintendencia determinó que la Isapre Banmédica, S.A. dio cumplimiento oportuno a dicha instrucción, la cual fue acreditada en el Oficio No. 1430.

Es preciso indicar que dicha instrucción fue girada a la Isapre Banmédica, S.A. para su cumplimiento con la Farmacia. Sin embargo, debe considerarse que la misma no fue suficiente, constituyendo una eliminación de la vulneración hecha; la orden de la Superintendencia debió ser enfática en cuanto a no transferir, bajo forma alguna, el diagnóstico clínico de los beneficiarios de la Isapre a la Farmacia.

Asimismo, el planteamiento de la Superintendencia es insuficiente, lo que podría deberse a que la institución considera tener mayor vinculación y fuerza respecto de aquellas fiscalizaciones relativas a garantizar los mecanismos y finalidad del sistema GES, en vez de aquellos derechos adicionales existentes, pero no "primordiales" o "básicos". Sin embargo, esto representa el problema de la política pública de la Protección de Datos existente, y la necesidad de tener un organismo propio e independiente y con la fuerza legal para fiscalizar y dictar las sanciones correspondientes a estas vulneraciones, con el caso descrito ha quedado sumamente claro que no está funcionando el sistema tal como se encuentra regulado.

4) No se demostró *"perjuicios respecto a otros beneficiarios de la Isapre Banmédica, S.A. distintos de la denunciante, con motivo de la conducta objetada."*

En definitiva la Superintendencia de Salud no es la Institución facultada para deducir este tipo de responsabilidad ya que según los principios de la Protección de Datos no es necesario establecer que se produzca un daño, si no evitarlo, una vez producido el daño, la Institución competente es la Corte mediante el Recurso de Protección.

Valoraciones Adicionales respecto a la Resolución.

Por otra parte es necesario mencionar las valoraciones adicionales hechas por la Superintendencia de Salud como por la Isapre en dicha resolución.

La Isapre postuló que, si bien la Superintendencia reconoce la facultad de la Isapre para tratar datos sensibles en la determinación de un beneficio de salud, no puede posteriormente sancionarla por haber ejercido de una manera u otra, si no existe una normativa que regule la materia.

Al respecto la Superintendencia indicó que, en la comunicación hecha el 10 de junio de 2009 enviada a la señora Castro, se informó sobre la evaluación de la pertinencia y procedencia de perfeccionar la regulación administrativa vigente en la materia (protección de datos), lo que reafirma que no existía una infracción específica que imputar a esa Isapre.

En este punto se puede apreciar que la Superintendencia de salud no es la institución facultada para deducir este tipo de responsabilidad. Según los principios vistos de la Protección de Datos no es necesario establecer que se produzca un daño, sino más bien evitarlo. En caso que se produjese un daño, la institución competente es la Corte mediante el Recurso de Protección.

Nos preguntamos entonces ¿Qué pasó con dicha regulación administrativa? ¿Existe a la fecha?

Efectivamente, la Superintendencia realizó una modificación a su regulación administrativa en cuanto al tratamiento de Datos Personales, sin embargo, esto es sólo lo adoptado por la Superintendencia de Salud, significa un avance pero es un avance aislado suscitado por el caso ocurrido, por lo que también nos preguntamos ¿Qué sucedió con respecto de la política pública de protección de datos?

Tal como se indicó con anterioridad, cuando el caso de la señora Castro ocurrió, también se verificó dicha conducta con la Isapre Vida Tres, S.A. En ese entonces, la Superintendencia de Salud tenía en vigencia la Circular IF/No. 51 de fecha 22 de agosto de 2007, la cual *"IMPARTE INSTRUCCIONES RESPECTO AL PROCEDIMIENTO QUE DEBERÁN ADOPTAR LOS SEGUROS PREVISIONALES DE SALUD FRENTE A REQUERIMIENTOS DE DATOS SENSIBLES DE SUS COTIZANTES Y BENEFICIARIOS."*

Posteriormente dicha circular fue complementada con la circular IF/No. 104 de fecha 31 de agosto de 2009, la cual "*INCORPORA INSTRUCCIONES SOBRE ENTREGA DE INFORMACIÓN SENSIBLE DE BENEFICIARIOS Y BENEFICIARIAS DE ISAPRES Y FONASA A ESTABLECIMIENTOS PRIVADOS DE VENTA, ARRIENDO, DISTRIBUCIÓN O ENTREGA DE ARTICULOS, INSUMOS Y/O MEDICAMENTOS DE APOYO TERAPEUTICO*."

Con la emisión de dicha circular principalmente se aclaró la tesis manejada desde un inicio en este estudio de caso: La Farmacia como prestador institucional de servicios médicos no debe recibir por parte de la ISAPRE información sensible, aduciendo que es para cumplir con prestaciones determinadas en el régimen de salud.

Para el caso, el documento en mención (circular IF/No. 104), señala en el punto relativo a los antecedentes lo siguiente:

"2. La Circular IF N° 71, de 27 de junio de 2008, modificó las instrucciones impartidas por esta Intendencia de Fondos para el envío de información de las isapres a la Superintendencia de Salud, sobre las redes de prestadores de salud[28].

El Anexo N° 4 de la mencionada instrucción, reemplazando el Subanexo N° 4 de la Circular IF N° 25, de 2006, incorpora en el grupo de los "Prestadores Institucionales" con quienes las isapres pueden celebrar convenios, en la categoría de "Establecimientos privados de artículos, insumos y/o medicamentos de apoyo terapéutico", entre otros a los Centros de Órtesis, Centros de Terapia Respiratoria, Farmacias y Ópticas.

Cabe señalar que es a los prestadores mencionados en el párrafo anterior (Farmacias entre otras) a quienes los aseguradores remiten o entregan información sobre sus beneficarios y beneficiarias, para permitir el acceso de éstos a los beneficios legales y contractuales que forman parte de los respectivos convenios , en tanto que los demás prestadores, generalmente generan o reciben directamente de los pacientes información que tiene el carácter de datos sensibles, especialmente diagnósticos y estados de salud físicos o psíquicos, por lo que no necesitarían su transmisión desde las ISAPRES para estar en conocimiento de éstos."

Ahora bien respecto a las adiciones establecidas, dicha circular baso en cuatro aspectos:

"1. Transmisión segura de información."

Donde indica que, *"La información relativa a los beneficiarios y beneficiarias de los seguros de salud y que deba ser entregada a los establecimientos privados de venta, arriendo, distribución o entrega de artículos, insumos y/o medicamentos de apoyo terapéutico (tales como centros de órtesis, centros de terapia respiratoria, farmacias, ópticas, entre otros) en virtud de los convenios que hubiesen suscrito o que en el futuro suscriban, para el otorgamiento de los beneficios de salud legales y contractuales, deberá transmitirse mediante un mecanismo que asegure la protección adecuada de la misma, evitando, en cuanto sea posible, el acceso del prestador a antecedentes de la persona beneficiaria que tengan el carácter de datos sensibles, a la luz de la definición contenida en la letra g) del artículo 2° de la Ley N° 19.628."*

Resulta notorio que la instrucción no parte de una obligación puntual y determinante, sino más bien de una solicitud para que sea considerada *"tratando de evitar en cuanto sea posible".*

Lo anterior podría obedecer, particularmente al hecho, como se mencionó con anterioridad, que la Superintendencia de Salud tiene como facultad primaria asegurar las prestaciones de salud, las cuales deben ser brindadas por parte de todas las entidades involucradas, respetando, entonces, los demás derechos existentes. Sin embargo, esto se traduce en una dificultad por cuanto al balance de derechos, salud y protección de datos.

"2. Mecanismos de protección y actualización de la información.

Las isapres y el Fonasa adoptarán los mecanismos que permitan resguardar la totalidad de la información y, en particular, aquélla que contenga datos sensibles, de manera que los prestadores con quienes han suscrito o suscriban convenios para el otorgamiento de los

[28] Las instrucciones en cuestión, Circular IF N° 25, 11.7.2006 y Circular IF N° 37, 20.3.2007, están referidas a la información que deben mantener actualizada las isapres, ante la Superintendencia, respecto a los prestadores con quienes han celebrado convenios para brindar atenciones de salud (GES, CAEC, modalidad cerrada o preferente de los planes de salud y beneficios mínimos del artículo 194 del DFL N° 1).

beneficios de que se trate, sólo accedan a la información mínima e indispensable que permita entregar dichos beneficios.

Además, adoptarán los resguardos conducentes a que la información de que dispongan los prestadores mencionados sea fidedigna y lo más actualizada posible, a objeto de que los beneficiarios vean satisfecho el acceso a los beneficios que les correspondan."

Con este fundamento, se cumple con los principios de resguardo de la información, exactitud de los datos y vigencia de los datos.

"3. Cláusula Contractual."

Asimismo dicha circular incorporó la obligación de información a la Superintendencia de Salud por parte de las Isapres y de Fonasa, sobre los mecanismos que adopten o hubiesen adoptado para cumplir dichas instrucciones.

Con esto surgió nuevamente la interrogantes antes planteada, ¿Porqué la Superintendencia no entró a establecer un mecanismo previo de revisión de los convenios suscritos?.

Descripción de diligencias indicadas en documentación adicional emitida durante la solución de los reclamos[29] **de la señora Sara Castro.**

Mediante nota SS/No. 1430 de fecha 15 de mayo de 2009, la Superintendencia informó a la Isapre Banmédica S.A., que el día 12 de mayo de 2009 fiscalizó una sucursal de Farmacias Cruz Verde con el objeto de verificar el cumplimiento de las instrucciones impartidas en el Oficio en referencia, en conformidad con la normativa que regula la materia.

Como resultado de dicha actividad la Superintendencia determinó que "*esa entidad dio cumplimiento en cuanto a la eliminación de la glosa descriptiva de la patología GES".*

Advertimos que la Superintendencia de Salud tiene como limitante el no tener facultades amplias y suficientes para fiscalización de farmacias, por lo que únicamente pudo pronunciarse en cuanto a la actuación hecha por la Isapre.

Posteriormente, a través de la nota SS/N° 1626 de fecha mayo de 2009, la Superintendencia informó a la señora Sara Castro sobre las acciones adoptadas por dicho organismo fiscalizador en relación con el traspaso de información desde la Isapre Banmédica S.A. a la Farmacia Cruz Verde. En dicho documento consta que: fue emitido de tal forma a solicitud de la señora Sánchez ya que las respuestas habían sido enviadas a través de correos electrónicos sin cumplir con formalidad alguna en la misma.

La Superintendencia informó cronológicamente el proceso de fiscalización realizado a la Isapre Banmédica S.A., respecto del convenio celebrado con las Farmacias Cruz Verde, en relación con la denuncia presentada por la misma el 13 de abril de 2009.

[29] Tal como se mencionó con anterioridad, para esta investigación, no se obtuvo acceso al expediente de reclamo hecho en la Superintendencia de Salud por la señora Sara Castro. Sin embargo, se obtuvieron indicios sobre algunas diligencias y alegaciones vertidas a partir del expediente del recurso de protección interpuesto por la reclamante, identificado bajo el Rol No. 6523-2009.

El 17 de abril de 2009, la Superintendencia procedió a fiscalizar, entre otras, a la Isapre Banmédica S.A., y, a través de ésta, inspeccionaron en terreno una sucursal de la Farmacias Cruz Verde constatándose la efectividad de la denuncia.

El día 5 de mayo de 2009 (ORD. SS/N 1319, de fecha 5 de mayo de 2009) se instruyó a la Isapre Banmédica, S.A., que realizara las gestiones tendientes a la eliminación de todos los datos sensibles que estuvieran a la vista de los dependientes de las Farmacias Cruz Verde, hecho que, posteriormente, sería monitoreado por el organismo de control.

Es así que, con fecha 12 de mayo de 2009, se verificó en terreno el cumplimiento de lo instruido. Para tal efecto, se realizaron simulaciones de venta de medicamentos a personas beneficiarias que hacen uso de las GES verificándose lo siguiente*: "en la pantalla a la que tiene acceso los vendedores fue eliminada la glosa descriptiva de la patología GES."* Esta información es recogida en el oficio SSS/No. 4430 de fecha 15 de mayo de 2009.

En ese sentido, la Superintendencia indicó que con dichas gestiones espera haber dado respuesta a la solicitud de la señora Castro e informó que respecto al reclamo N° 9272 ingresado con fecha 13 de mayo, se encontraba en etapa de análisis.

La respuesta a este segundo reclamo, identificado con el No. 9272, versó en los siguientes aspectos:

Comunicó que tal como había informado a la reclamante en el Oficio Ordinario SS/N° 1626 de mayo de 2009 y mediante correos electrónicos enviados por el Jefe del Sub departamento de Atención al Usuario de la Superintendencia de Salud, el día 17 de abril de 2009, se efectuó una fiscalización extraordinaria a las distintas Isapres abiertas, "*con la finalidad de recabar información sobre los contratos vigentes con farmacias, con el objeto de conocer el flujo de información entre las Isapres y éstas para el otorgamiento de beneficios, especialmente en lo que versa sobre la existencia de traspaso de información que pudiera revestir el carácter de sensible según lo dispuesto en la Ley No. 19.628. Así, mediante una inspección en terreno a una sucursal de la Farmacia Cruz Verde, se pudo constatar que efectivamente, los encargados de venta de medicamentos tenían a la vista la información relativa al problema de salud de los beneficiarios GES de las Isapres Banmédica, S.A. y Vida Tres, S.A.*

A raíz de ello, el 5 de mayo de 2009, instruyó a la Isapre que realizara las gestiones tendientes para eliminar todos los datos sensibles que estuvieran a la vista de los dependientes de las Farmacias Cruz Verde, medidas que fueron monitoreadas por este Organismo de Control, verificándose que el 12 de mayo del año en curso, mediante simulaciones de ventas de medicamentos a personas acogidas a la GES, -dentro de las cuales se encontraba la señora Castro- *que en la pantalla a la que tienen acceso los vendedores fue eliminada la glosa descriptiva de la patología GES.* Si bien esta información se borró de la pantalla, ¿Cómo se podría verificar que la farmacia ya no tiene la base de datos?

Al respecto, una opción es que podría establecerse de forma tal como se encuentra regulado en la Ley de datos personales de Perú, donde entidades públicas e instituciones privadas, tienen la carga de la prueba para comprobar el cumplimiento de las obligaciones de la Ley y su reglamento. Asimismo, hace falta la emisión de un Reglamento que determine estos aspectos.

En este contexto, cabe hacer presente que la regla general en esta materia es la prohibición expresa para el tratamiento de datos sensibles, dentro de los que se encuentra la información relacionada con el estado de salud de las personas. Sin embargo, las Isapres cuentan con una

facultad excepcional consagrada en la propia ley para realizar un tratamiento de datos sensible cuando estos sean necesarios para la determinación u otorgamiento de beneficios de salud que corresponda a sus titulares. Para lo cual, la Superintendencia se pronunció sobre la materia de Datos Personales.

Ahora bien, en el tratamiento de los datos antes señalados, la Isapre debe actuar con la debida diligencia a fin de no ocasionar daños, como los alegados; dado que en caso de verificarse una falta de diligencia o causar una negligencia en el tratamiento de los datos sensibles, ésta puede ser responsable civilmente –recibiendo la sanción administrativa consecuentemente- por la indemnización de los perjuicios que hubiere ocasionado en su actuar.

Es por ello, y atendido que es deber de la Superintendencia de Salud velar por que las Instituciones de Salud Previsional y el Fondo Nacional de Salud cumplan con la legislación vigente en sus actuaciones, y en el otorgamiento de los beneficios a que por ley o por contrato se encuentran obligados, que junto con la fiscalización extraordinaria citada en lo precedente, se está evaluando también la pertinencia y procedencia de perfeccionar la regulación administrativa vigente en esta materia.

Circular IF/N° 51 de fecha 22 de agosto de 2007 y su modificación posterior.

Dicho documento IMPARTE INSTRUCCIONES RESPECTO AL PROCEDIMIENTO QUE DEBERAN ADOPTAR LAS ISAPRES FRENTE A REQUERIMIENTOS DE DATOS SENSIBLES DE SUS COTIZANTES Y BENEFICIARIOS.

La finalidad de este texto es uniformar el procedimiento que deberán adoptar frente a solicitudes de comunicación, cesión, transferencia, trasmisión o cualquier tipo de operación que derive en el proceso o conocimiento, por parte de terceros, a los datos sensibles de sus beneficiarios y/o ex – beneficiarios, el mismo es el que se encontraba vigente en el momento de surgir el caso de la señora Sara Castro y que posteriormente fue ampliado por la circular No. IF No. 104 de fecha 31 de agosto de 2009.

Cabe señalar que de acuerdo con lo establecido en el artículo 10 de la Ley No. 19.628, las Isapres y Fonasa, poseen legítima facultad para el tratamiento de datos sensibles relativos al estado o condición de salud de sus cotizantes y beneficiarios.

Por su parte, los artículos 12 y 13 de la Ley No. 19.628 confieren al titular de los datos, el derecho a exigir a quien sea responsable de los mismos, información sobre datos relativos a su persona, así como la modificación, cancelación o bloqueo de la información[30].

De esta forma, y en conformidad con este Instructivo, es posible establecer que las Isapres deben tener la obligación de revisar y fiscalizar los convenios suscritos entre ellas y las cadenas de farmacias. Dicha circular regula los requerimientos formulados entre Seguros Previsionales de Salud, y los requerimientos formulados por terceros[31].

[30] Ello fue lo que se hizo en sede administrativa, se canceló los datos de los afiliados a la Isapre con cobertura GES. Lo que implicó el fundamento de la resolución de la Suprema Corte. Sin embargo, constituyó una transgresión, ya que se trasladaron datos sensibles sin consentimiento del titular sin que hayan sido necesarios para el otorgamiento de salud.

[31] Según la circular, el concepto "tercero" comprende a todos quienes no sean la institución aseguradora de salud y cotizante y/o beneficiario que ha celebrado un determinado contrato de salud, en el caso de la Isapres. Para los efectos de estas instrucciones, si bien las Isapres y el Fonasa tienen el carácter de terceros en las relaciones jurídicas en que no son parte, tendrán tratamiento especial referido en el mismo bajo tal calidad.

Se establece, además y como condición, que Fonasa o la Isapre cuando sean requeridos por un tercero para comunicar, ceder, transferir, transmitir u otro tipo de operación que derive en el tratamiento de datos sensibles de sus beneficiarios y/o ex beneficiarios, deberán abstenerse de acceder a dicha solicitud, cualquiera sea la causa invocada como fundamento de la petición, sólo en el caso de que el titular de los datos consienta expresamente en ello, y autorice que se proporcione la información.[32]

La primera condición sería, por tanto, que el dato sea requerido por el tercero, situación que en el caso de la señora Castro no ocurrió, ya que los datos fueron enviados por acuerdo entre la Isapre y el tercero, violentándose claramente el Instructivo y la Ley 19.628. Asimismo, y como segunda condición, se necesita que el titular brinde el consentimiento.

Dicho consentimiento deberá ser otorgado por el titular de los datos sensibles o por su representante legal, a FONASA o a la Isapre, por escrito, en términos claros y explícitos, precisando los datos que el asegurador podrá entregar o informar y con plena individualización del beneficio y/o ex-beneficiario cuando corresponda.

Posteriormente y a raíz del caso suscitado por la señora Sara Castro, el Instructivo en mención fue modificado de la forma siguiente:

CIRCULAR	FECHA	CONTENIDO
Circular IF No.51	22/08/2007	Imparte instrucciones respecto al procedimiento que deberán adoptar los Seguros Previsionales de Salud frente a requerimientos de datos sensibles de sus cotizantes y beneficiarios.
Circular IF No. 68	06/06/2008	Imparte instrucciones sobre el procedimiento que deberán adoptar los seguros frente a requerimientos de datos sensibles de sus cotizantes y beneficiarios.
Circular IF No. 104	31/08/2009	Incorpora instrucciones sobre entrega de información sensible de beneficiarios y beneficiarias de Isapre y Fonasa a establecimientos privados de venta, arriendo, distribución o entrega de medicamentos de apoyo terapéutico.

Fuente: Adaptación de la Superintendencia de Salud.

4.3. Sede Judicial.

Señora Sara Castro.

El día 8 de mayo de 2009, con base al artículo 20 de la Constitución Política de Chile, la señora Castro Pérez interpuso el Recurso de Protección contra los representantes de la Isapre Banmédica, S.A. y de Farmacias Cruz Verde, S.A.

En el mismo solicitó la eliminación de toda comunicación escrita, digital o de cualquier otra especie entre Isapre Banamédica, S.A. y Farmacia Cruz Verde, S.A. o a cualquier otro tercero, respecto a la información de la recurrente sobre el "beneficio de las Garantías Explicitas de

[32] Derechos no solo es para afiliados sino también para los ex beneficiarios.

Salud –GES- y su diagnóstico clínico de Depresión Severa Mayor, así como de la disposición de dicha información de las dependientes de la referida farmacia.

Lo anterior, fue argumentado por la recurrente en base a que la información se encuentra en manos de terceros sin mediar consentimiento expreso, lo que constituyó un acto ilegal y arbitrario, que le priva del derecho a la vida privada y honra e integridad psíquica.

La señora Castro solicitó a la Corte que realizara como diligencia el requerimiento del Convenio suscrito entre la Isapre Banamédica, S.A. y la Farmacia Cruz Verde. Asimismo, indicó que aunque siguió cotizando en la Isapre, en el mismo mes de marzo de 2007 que se afilió, abandonó el tratamiento de las Garantías Explicitas de Salud (GES), la cual finalizó en marzo de 2008, fecha en que la Isapre debió haber eliminado toda la información GES de su persona.

Arguyó que la reserva de sus antecedentes de salud incluidos los diagnósticos médicos fue violada por la acción de la Isapre al entregarlo a la farmacia, no habiéndole concedido permiso alguno para entregarlos a terceros.

De igual forma los dependientes de la farmacia al ingresar su RUT conocían su historial clínico, lo cual se dio cuenta en abril de 2009, dos años después que no utilizó el GES y un año después de haber vencido el mismo. En base a lo anterior, la señora Sara Castro solicitó principalmente a la Corte, que:

a) Ordene a la Isapre Banmédica, S.A. el cese de la entrega de la información a la Farmacia Cruz verde sobre su persona por no tener ya la calidad de beneficiaria GES.

Y que se le requiriera a Isapre Banmédica, S.A. la copia del convenio, contrato o instrumento jurídico en virtud del cual se remitió el diagnóstico médico de su persona a la Farmacia. Asimismo copia y fecha de envío de los antecedentes de la recurrente.

b) Ordene a la Farmacia Cruz Verde la eliminación del registro informático de sus terminales de sucursales de toda referencia de que la recurrente fue paciente GES.

Requerirle a la misma para que se remita la copia íntegra de todas las compras de remedios efectuados por la recurrente bajo su RUT desde el 8 de marzo de 2007 hasta mayo de 2009, indicando los productos y precios.

c) Requerirle a la Superintendencia de Salud, que informe sobre la Reglamentación que rige a las Isapres sobre la entrega de datos de sus afiliados a terceros en el cumplimiento de las prestaciones o beneficios GES, y sobre qué datos de los afiliados no se pueden entregar y la razón.

Asimismo solicitó que se tomaran todas aquellas providencias necesarias que considerara convenientes para el restablecimiento del imperio del derecho y de su debida protección.

Posteriormente, el día 8 de julio de 2009, la señora Sara Castro indicó que la Isapre no entregó ante la Sala la copia del convenio, contrato o instrumento jurídico en virtud del cual se remitió el diagnóstico médico de la recurrente a la Farmacia Cruz Verde. De igual forma, adujo que no se entregó copia y fecha del envío de los antecedentes de la recurrente a la farmacia.

Isapre Banmédica.

Solicitó el rechazo del recurso de protección, basados en los siguientes argumentos:

1. En cuanto a que la situación de hecho a la que se refiere el mismo se encuentra resuelta en la sede administrativa, ante las gestiones realizadas por la Superintendencia de Salud.

Por la misma naturaleza del recurso de protección el cual se encuentra encaminado a resguardar y proteger el legítimo disfrute de algunos de los derecho y garantías reconocidos a todas las personas en el artículo 19 de la Constitución de la República, solicitó que previo a entrar al fondo de la cuestión planteada en el procedimiento invocados, se tuviera en cuenta que la medida en cuestión, se refiere a una situación de hecho que se encuentra concluida, dejando de tener sentido el recurso.

De igual forma argumentó que la Superintendencia tiene atribuciones de fiscalización respecto de las Isapres pero no respecto de las Farmacias, y es de ahí que el hecho que se den instrucciones o se hagan comentarios a la Isapre no puede ser entendido como una atribución o afirmación de responsabilidad, sino que es consecuencia de que ella es la única a quien el órgano fiscalizador puede dirigir tales instrucciones o comentarios[33].

Indicó que la situación fue concluida remitiéndose afirmar que el reconocimiento hecho por la Superintendencia en el oficio SS/No.1430 de fecha 15 de mayo de 2009 es la mejor demostración. Asimismo rechazó que haya incurrido en acción u omisión arbitraria o ilegal alguna que afecte o haya podido afectar el legítimo ejercicio de los derechos constitucionalmente garantizados de la recurrente.

Que según lo indicado, y aun cuando pudiera estimarse que en el pasado se incurrió en una acción u omisión que afectó legítimamente los derechos de la recurrente -cosa que igual rechaza categóricamente-, se expresa que dicha situación ya se encuentra concluida a juicio incluso del ente público encargado de fiscalizar el cumplimiento de la ley por parte de todas las Isapres.

No existe base jurídica suficiente para continuar con la tramitación del recurso, puesto que ya no existe la privación, perturbación o amenaza que se pretende terminar, combatir o evitar -aún no se había resuelto sobre la sanción, únicamente sobre la fiscalización y cumplimiento de lo ordenado.

2. Isapre Banmédica, S.A., no ha incurrido en acción u omisión arbitraria o ilegal alguna que afecte o haya podido afectar el legítimo ejercicio de los derechos constitucionalmente garantizados de la recurrente.

Que a diferencia de lo que parece entender la recurrente en el sentido que su representada traslado información sensible de sus afiliados a una cadena de Farmacias, lo cierto es que la Isapre se limitó a *"cumplir con lo establecido en la legislación vigente, respetando en todo momento las normas vigentes relativas al cuidado de los datos personales"* [34]

[33] A nuestra opinión, si bien la Superintendencia de Salud no puede fiscalizar a las Farmacias, cuando se verse sobre aspectos de datos sensibles de personas afiliadas a las Isapres, si puede emprender las medidas de verificación y protección necesarias, incluso contra aquellos terceros involucrados.

[34] Estamos ante una política pública deficiente que carece de controles apropiados, así como de conocimiento certero de los participantes de los diversos sectores.

Lo anterior lo afirma basado en el inciso 1 del artículo 205 del Decreto don Fuerza de Ley No. 1 de 2005, del Ministerio de Salud, donde indica que las Isapres están *"(...) obligadas a otorgar a los cotizantes y a sus beneficiarios las GES relativas a acceso, claridad, protección financiera y oportunidad contempladas en el Régimen General de Garantías de Salud, de conformidad a lo dispuesto en la Ley que establece dicho Régimen*[35]*".*

La Ley a que se alude en la norma antes citadas es la No. 19.966, la que establece en su artículo 11 que *"Las GES serán elaboradas por el Ministerio de Salud, de conformidad con el procedimiento establecido en esta ley y en el reglamento, y deberán ser aprobadas por decreto supremo de dicho Ministerio suscrito, además por el Ministro de Hacienda".*

En ese sentido la forma en que las Isapres dan cumplimiento a la obligación de otorgar a sus afiliados la cobertura GES se encuentran regulados en la normativa vigente, así se tiene que el inciso 2° del mencionado artículo 205 del Decreto con Fuerza de Ley No. 1 de 2005 del Ministerio de Salud, señala que *"los procedimientos y mecanismos para el otorgamiento de las garantías deben sujetarse al reglamento y serán sometidos por las instituciones Salud Previsional al conocimiento y aprobación de la Superintendencia".*

Para el efecto señalado, la Isapre Banmédica, S.A., manifestó que la norma básica en relación a la GES es el Decreto No. 44 de 2007 el Ministerio de Salud, en el que establece detalladamente las distintas patologías que quedan incluidas y las coberturas que en cada caso corresponden, en consecuencia, es ahí donde se encuentra detallada la cobertura que, en cada caso, corresponde otorgar por las Isapres a sus afiliados, en la medida que se encuentren afectados por una de esas patologías y decidan optar por la cobertura GES.

Asimismo dicha la Isapre recurrida hizo una relación de cómo funciona y opera la cobertura GES la que por Ley está obligada a cumplir, básicamente indicando que:

La Cobertura GES incluye remedios o medicamentos, esto se traduce en el financiamiento por parte de la respectiva Isapre en cuanto a una parte del precio de los remedios o medicamentos que corresponde al tratamiento de la patología de que se trata, estos a su vez reciben habitualmente la denominación de Canasta de Medicamentos.

Dicha canasta varía según la patología de que se trate, de igual forma dependiendo de dicha patología varía el porcentaje del valor de los respectivos medicamentos que debe cubrir la Isapre (cobertura financiera).

Lo anterior implica en la práctica que cuando un afiliado de una Isapre solicita la Cobertura GES, dicha institución queda obligada a cubrir parte del precio de determinados medicamentos, es decir aquellos que están incluidos en la respectiva canasta de medicamentos.

De acuerdo al inciso 1 del artículo 173 del ya mencionado Decreto con fuerza de Ley No. 1 de 2005 del Ministerio de Salud en relación con el inciso 1° del artículo 123 del Código Sanitario, la venta al público de los productos farmacéuticos para uso humano sólo podrá hacerse en las farmacias, lo que implica que las Isapres no pueden entregar directamente a sus afiliados los medicamentos que corresponden a la cobertura GES, por lo que se concurre a la celebración de convenios con farmacias de manera que sean estas las que entreguen los

[35] Si bien es cierto esta es la principla obligación de las Isapres las actividades de las mismas no se puede apartar de obligaciones adicionales establecidas en legislaciones adicionales.

medicamentos a los afiliados con el consecutivo descuento que corresponde asumir a la Isapre[36].

Para el funcionamiento de dicho sistema resulta indispensable que la Isapre entregue alguna información a la cadena de farmacias respectiva pues de lo contrario, sería imposible hacer operativo el beneficio. En ese sentido la Isapre Banmédica, S.A., hace llegar a la cadena de farmacias como información fundamentalmente la individualización del beneficio y la indicación de los medicamentos que cubre el beneficio. Asimismo, dicha Isapre enfatizó que no se entregan antecedentes respecto a un diagnóstico específico, ni menos aún datos propios de la ficha clínica del respectivo paciente.

De igual forma la canasta de medicamentos se entrega bajo un código de manera que no queda abierta de manera amplia a cualquier persona.

Además adujo, que dicho mecanismo también fue reconocido por la Cadena de Farmacias según declaración pública emitida por la misma el 26 de mayo de 2009 y que la funcionalidad del sistema cumple con los tres supuestos de validación que contempla el artículo 10 de la Ley No. 19.628, es decir:

1) Los datos que se entregaron a la cadena de farmacias eran los dispensables para hacer operativo un beneficio establecido en la legislación.

2) Los datos se entregaron como consecuencia de una solicitud por parte de los respectivos afiliados para la obtención de un beneficio específico.

3) El objetivo de la entrega de los datos era precisamente para el otorgamiento de un beneficio de salud al titular de los datos, el cual es la cobertura GES respecto de la canasta de medicamentos relativa a la patología específica.[37]

La Isapre Banmédica, S.A., afirmó que con dichas consideraciones no puede dejarse de lado que una persona con algún grado de conocimiento como las dependientes de las farmacias pueden asociar los medicamos que se trata con la patología a cuya cobertura corresponden, situación que escapa del control de las Isapres.

Por otro lado, la sociedad recurrente expresó que existe una cierta responsabilidad de la Isapre en que los datos entregados a la Cadena de Farmacias, y que estos hayan permanecido en los registros de esta institución, aún después de expirada la vigencia del beneficio de la cobertura GES[38]. En el caso de ser tal situación efectiva, ello queda fuera de la competencia, atribuciones y obligaciones de la Isapre.

3. No se ha producido una afectación de los derechos constitucionales de la señora Sánchez, consagrados en los No. 4 y 1 de la Constitución Política que sea imputable a la Isapre.

---

[36] Ya es conocido que las Isapres deben realizar convenios con farmacias para la entrega de medicamentos, ¿Por qué los mismos no son revisados y aprobados por la Superintendencia de Salud? Si estamos hablando de una extensión del beneficio que de igual forma debe ser protegido.

[37] El otorgamiento del beneficio de salud no se configura o no nace aquí, el beneficio se otorga cuando el interesado acude a la Isapre a reportar la condición y el deseo de cobertura GES y paga la cuota correspondiente. La entrega de medicamentos solo constituye una derivación o ejecución del beneficio ya otorgado.

[38] Dicha afirmación es verdadera en virtud del principio de finalidad. El primer principio violentado fue que no existió el consentimiento del titular ya que no era un dato necesario para otorgamiento de beneficio de salud pues este ya había sido otorgado como tal, siendo la entrega de medicamentos una ejecución O COBERTURA EFECTIVA de dicho beneficio. Posteriormente se violentó muchos principios adicionales.

Farmacia Cruz Verde.

1. La Farmacia Cruz Verde S.A. alegó, en primer lugar, que el recurso era improcedente por falta de oportunidad en su presentación, dada la regularizaron de los registros asociados a la recurrente. Explica también que, *a la fecha,* no existen normas constitucionales que sean vulneradas. Por último, recuerda la visita de la Superintendencia cuando constató este hecho con una fiscalización en terreno, comprobando que en los locales de la farmacia, no se encuentra ninguna información relacionada a la recurrente en la calidad de paciente GES.

2. Asimismo, alegó que el recurso era improcedente, dada la inexistencia de vulneración de garantías constitucionales, reiterando argumentos ya vertidos por la señora Castro, y agregando que, dependiendo de la enfermedad, la Isapre cubre una determinada cantidad de medicamentos, los cuales son parte de las prestaciones que estas entidades de salud deben otorgar, en cumplimiento de las prestaciones GES y, en este contexto, las Isapres realizan determinados convenios con farmacias, informándole a éstas que un determinado afiliado posee cobertura GES, lo que no se relaciona con el diagnóstico médico o ficha clínica, pues sólo sirve para que la farmacia tenga conocimiento del stock de medicamentos que están incluidos en esta cobertura.

3. Asimismo, anexó un cuadro que contiene un listado de medicamentos adquiridos por la señora Castro, conteniendo el número de RUT, fecha y hora, así como la descripción del medicamento.

Al respecto, cabe destacar, que a pesar de haber negado rotundamente la vulneración de los derechos de la señora Castro, la Farmacia indicó que la situación fue resuelta con anterioridad, a raíz de las gestiones hechas en la instancia administrativa con la intervención de la Superintendencia de Salud, institución que conoció del reclamo y que, de acuerdo con las atribuciones disciplinarias y de control sobre la Isapre Banmédica S.A., ordenó a ésta finalizar la transferencia de cualquier información sensible a la farmacia, a lo cual y tal como consta, Banmédica S.A. dio estricto cumplimiento. Por lo tanto puede desprenderse que efectivamente en un momento determinado, si existió una vulneración a los datos sensibles de la señora Sara Castro.

Superintendencia de Salud.

El día 4 de agosto de 2009 este organismo rindió el informe requerido por la Corte, el cual contuvo esencialmente lo siguiente:

I. Reclamo administrativo tramitado por esa Superintendencia.

Reclamo de fecha 15 de abril de 2009 con fecha de ingreso 7200-2009.

Indicó que debido a que dicho reclamo no fue primeramente atendido en la Isapre, se derivó a la misma en cumplimiento del artículo 127 inciso primero del DFL N° 1 de 2005 de Salud.

Asimismo, realizó la narración de los hechos, informando que constató que en la información desplegada en pantalla de una sucursal de la Farmacia Cruz Verde S.A, figuraban los diagnósticos GES de los beneficiarios de la aseguradora. En consecuencia, y de acuerdo con las facultades concedidas por el artículo 110 del citado Decreto con fuerza de ley, se instruyó a la Isapre Banmédica, S.A., mediante Oficio SS/N° 1319 de 5 de mayo de 2009, que

eliminara la información indebida de los registros de ventas de medicamentos GES, constándose en terreno el cumplimiento de lo ordenado con fecha 12 del mismo mes y año.

Finalmente, el procedimiento administrativo iniciado por el reclamo de la señora Castro concluyó con la emisión del oficio IF/N° 4443 de 10 de junio de 2009.

La Superintendencia indicó en dicho oficio, que se informó a la reclamante que las Isapres están autorizadas por ley[39] para efectuar el tratamiento de datos sensibles de sus afiliados, dado que se trata del otorgamiento de beneficios de salud -excepción contemplada en la Ley No. 19.628 sobre Protección de Datos Personales- lo que en ningún caso puede ocasionar perjuicios a los beneficiarios de dichas instituciones. En la especie, se indicó, el registro de la patología GES fue eliminado y que, por tanto, la Superintendencia estimó debidamente atendido el reclamo de la señora Castro.

II. Regulación del tratamiento de datos sensibles por parte de las ISAPRES.

1. CONVENIOS PARA OTORGAR LAS PRESTACIONES GES.

En este apartado la Superintendencia de Salud, invocó los preceptos jurídicos por los cuales las ISAPRES tienen la facultad de tratar datos sensibles de sus beneficiarios, citando principalmente lo siguiente: *"De la normas transcritas se desprende que, por un aparte, las Isapres están obligadas a otorgar a sus beneficiarios las coberturas amparadas en las GES, y, por otra, que los respectivos pacientes deben atenderse en los prestadores de salud con los cuales aquéllas hayan suscrito un convenio al efecto, puesto que la Ley de Isapres prohíbe expresamente a tales entidades otorgar directamente prestaciones de salud.".*

Al respecto, es de hacer notar que dicha facultad nunca fue recurrida o puesta en duda. En ese sentido, es posible determinar que la vulneración no se refirió al tratamiento de los datos sensibles por parte de la Isapre, sino a la transmisión de dichos datos a terceros, por no tener autorización la Isapre para el traslado, aun y cuando mediare un convenio.

Posiblemente, aquí podríamos decir que es cuando entran en pugna dos derechos, debido a que la Superintendencia de Salud tiene la competencia única y exclusiva, para que las prestaciones de salud sean efectivamente brindadas y otorgadas; sin embargo, las mismas deben realizarse, con los mecanismos adecuados que cumplan y protejan los derechos derivados de dicha prestaciones de salud. De allí, la necesidad indefectible de contar con un órgano especializado en la materia.

En ese sentido, recalcamos que si bien los convenios son necesarios para la prestación de las GES, la Superintendencia, tiene la obligación de revisar dichos instrumentos en virtud de lo dispuesto en el artículo 110 del DFL No. 1 del Ministerio de Salud en concordancia con la Ley No. 19.628.

2. CALIDAD DE PRESTADORES DE SALUD DE LAS FARMACIAS.

Una de estas prestaciones cubiertas por la GES es, precisamente, la correspondiente a los medicamentos asociados a determinadas patologías, tal como lo establece el artículo 2° del DS No. 44 de 2007 de Salud, que contiene el listado de patologías garantizadas por la GES.

[39] A criterio de quien realizó este Estudio de Caso, este punto nunca se cuestionó, por lo que no es un tema a justificar.

De tal modo, la propia normativa vigente expresa que los medicamentos garantizados están considerados como prestaciones en sí mismos[40], por lo que, sólo las farmacias pueden otorgar tales "prestaciones GES" (según lo indica el código Sanitario y el Reglamento de Farmacias), para efectos de este beneficio legal, también se debe considerar a dichas instituciones como prestadores de la Red Cerrada de las Isapres[41].

3. TRATAMIENTO DE DATOS SENSIBLES EN EL ÁMBITO DE LA SALUD.

En este punto se argumentó que, se ha establecido que las Isapres deben otorgar sus prestaciones a través de convenios por expresa disposición legal (y por la prohibición de su giro exclusivo), y que, a su vez, entre los prestadores en convenio se encuentran las farmacias (instituciones que también tienen un giro exclusivo, en su caso, la venta de fármacos), sólo cabe concluir que a estos establecimientos les resulta plenamente aplicable lo regulado en el artículo 10 de la Ley No. 19.628 sobre Protección de Datos Personales, en cuanto *"No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que corresponda a sus titulares".*

Concluyó que las farmacias, en el contexto de los beneficios de las GES, y dada su calidad de prestadores de salud para otorgar medicamentos garantizados, se encuentran facultadas para efectuar tratamiento de datos sensibles de los beneficiarios de aquellas Isapres con las cuales hayan suscrito los convenios que exige la ley para determinar la Red Cerrada de Atención. Lo anterior cobra mayor sentido por el hecho de que estas garantías legales requieren de ciertos requisitos taxativos para ser invocadas, lo que forzosamente se debe comprobar en la respectiva farmacia al momento de requerírsele una prestación garantizada, esto es, la venta de medicamentos incluidos en el listado especifico de una patología GES.

Corte de Apelaciones de Santiago.

El tribunal intermedio solicitó informe a la Superintendencia de Salud, por el recurso de autos. En la misma resolución suspendió el decreto que ordenó traer los autos en relación. Admitió de forma extemporánea la evacuación de la audiencia otorgada a la Farmacia Cruz Verde. Se emitieron los alegatos verbales correspondientes.

Finalmente, dictó sentencia el día 2 de noviembre de 2009, determinando lo siguiente:

1. Que para la procedencia del recurso de protección, se requiere la concurrencia de los siguientes requisitos:

a) Que se compruebe la existencia de la acción reprochada.
b) Que se establezca la ilegalidad o arbitrariedad de esa acción.
c) Que de la misma, se siga un directo e inmediato atentado contra una o más de las garantías constitucionales invocadas, protegidas por esa vía, y
d) Que dicha Corte esté en situación material y jurídica, de brindar la protección pedida

2. Que debido a lo anterior, atendiendo a la naturaleza y fines cautelares de una acción de esta clase, para que ella pueda prosperar es indispensable que exista una situación de hecho ilegitima que ocasiones afectación a una de las garantías constitucionales protegibles por esta

[40] Esto contradice la teoría que esta investigación ha venido sustentando.
[41] El beneficio legal es acogerse al régimen GES, la entrega de medicamentos vendría a ser una ejecución de dicha prestación. Por lo que, si se considera la entrega de medicamentos, como un beneficio legal, entonces, si podría trasladárseles los datos sensibles. Quien lleva adelante esta investigación no comparte dicho criterio.

vía, de modo que esta Corte pueda restablecer el imperio del derecho y otorga la debida protección al afectado.

A contrario sensu, el recurso resulta improcedente si la situación fáctica que lo motiva no existe o si ha cesado[42].

3. Que en el presente caso, de lo expuesto por las partes, lo informado por la Superintendencia de Salud y documentos acompañados, en especial, el expediente sobre el reclamo administrativo No. 7.200-2009, resulta que la actual recurrente accionó administrativamente, ante esa autoridad con fecha 15 de abril de 2009, ejerciendo el derecho que le confiere el artículo 127 del D.F.L. No. 1 de 2005 de Salud, procedimiento en el cual se ordenó a la Isapre Banmédica, S.A., la eliminación de los registros de ventas de medicamentos GES, reclamado por la actora, poniéndose término a la transferencia de toda información sensible hacia la farmacia recurrida, habiéndose constatado en terreno por esa Superintendencia el cumplimiento de lo resuelto.

De lo anterior, se sigue que los hechos alegados por la actora, en los que se funda su acción, han estado bajo la tutela del derecho durante la tramitación del presente recurso, y que dicho procedimiento ha culminado, adoptándose por parte de la autoridad requerida, las medidas convenientes en resguardo de sus derechos.

4. Que atendiendo a lo antes indicado, habiéndose decidido y resuelto las medidas correspondientes para regularizar la situación de la recurrente, en particular, lo que atañe al registro de datos confidenciales relacionado con ella, resulta innegable que no existe actualmente providencia urgente alguna, que pueda esta Corte resolver en protección de la actora en esta sede, por cuanto, habiendo cesado el hecho que motivó la presente acción, la misma ha perdido oportunidad.

5. Que en consecuencia, y por los motivos señalados, debe concluirse que dicho recurso no puede prosperar, por no concurrir en la especie los fundamentos que lo hacen procedente; y en razón de ello, se omitirá por ser improcedente, el análisis de las restantes alegaciones de las partes[43].

Finalmente, la Corte Suprema rechazó por extemporáneo la tramitación del Recurso de Protección de Garantías Constitucionales.

[42] Este es un problema de la política existente. De acuerdo con la revisión del derecho comparado realizado con anterioridad, podemos determinar qué: existen tres escenarios de protección posibles a todo administrado en relación con la protección de datos, creando para ellos las instancias y mecanismos acordes y necesarios, siendo: 1. La creación de disposiciones que garantizan un nivel de protección elevado para los datos personales tratados por las instituciones y los organismos respectivos. Esto es el deber ser, la idónea operatividad y tratamiento. 2. La Creación de una instancia de vigilancia independiente encargada de controlar la aplicación de dichas disposiciones. En ese sentido, será la encargada de aplicar las acciones correspondientes, en cumplimiento de la ley respectiva y de acuerdo con las políticas y programas creados para tal finalidad. 3. La creación o acceso de un recurso judicial idóneo, adecuado y delimitado en cuanto a la protección y tiempo.

La Comunidad Europa, al respecto ha indicado que: las legislaciones nacionales, deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos, no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

[43] No entro en análisis del fondo del asunto y rechazó su tramitación por extemporáneo.

4.4. Apelación.

Señora Sara Castro.

El día 7 de noviembre de 2009, la señora Sara Castro interpuso recurso de apelación de la sentencia emitida por la Corte de Apelaciones de Santiago, descrita con anterioridad. Argumentó que el recurso si cumple con los requisitos necesarios para su procedencia, puesto que:

A. Se encuentra debidamente comprobado en autos, con el mérito de la denuncia y de los informes de los recurridos que, efectivamente, ***existe la acción reprochada,*** esto es, la existencia del registro en las base de datos de la Farmacia Cruz Verde sobre los datos sensibles de su persona obtenidos con infracción de ley, diagnóstico de depresión severa y ser paciente de GES, sin tener la calidad de beneficiario GES desde el 9 de marzo de 2008[44].

B. Se encuentra establecido que la acción reprochada es ilegal, por cuanto el registro de datos sensibles de la recurrente no estaban amparados por la ley del AUGE[45], ya que no era beneficiaria de GES, ni tampoco los recurridos tenían el consentimiento del titular para mantener en su base de datos, los datos sensibles ya indicados, infringiendo el artículo No. 2 letra g) y 10 de la ley 19.628.

C. Que de esta acción reprochable e ilegal, se siguió un directo e inmediato atentado contra las garantías constitucionales establecidas en el artículo 19 No 4 y 1° de la Constitución Política del Estado.

D. Que la I. Corte de Apelaciones de Santiago, estando en situación material y jurídica de brindar protección a la recurrente, no lo hizo, debiendo por ende presentar dicho recurso para enmendar el agravio[46].

E. La recurrente adujo que lo ordenado por la Superintendencia de Salud a la Isapre, no corresponde a lo reclamado por ella en el recurso de protección invocado, el cual consiste en i) El restablecimiento en el imperio del derecho y ordenar que se deje sin efecto los actos[47] Isapre Banmédica, S.A. y Farmacia Cruz Verde que posibilitaron la entrega de datos sensibles, como el diagnóstico médico, a los empleados de la Farmacia Cruz Verde, ii) El cese del hecho que la recurrente es beneficiaria GES desde el 9 de marzo de 2008[48], y iii) Ordenarse la eliminación del registro informático de sus terminales de mesones y de las bases

[44] Es ilegal por no existir consentimiento expreso de la titular. El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

[45] En caso que no opera mi interpretación sobre el hecho, en cuanto a que la entrega de medicamentos, por parte de las farmacias, no constituye por sí mismo el otorgamiento de un beneficio de salud, (ya que este ya fue otorgado por la isapre, y la entrega de medicamento es parte del servicio de cobertura), es posible establecer que la titular, ya no estaba afiliada a dicha cobertura y por lo tanto, era un dato que había caducado y por el artículo 6 debía ser eliminado.

[46] Ello debido a que la Corte indicó que según lo accionado en sede administrativa, se puso término de toda transferencia de información sensible a la farmacia recurrida, por lo que no existió en el momento de tramitación del recurso providencia alguna que la I. Corte pudiera resolver en protección de la recurrente.

[47] Los actos se constituyen a través de los Convenios. Sobre esto, no se pronunció la Superintendencia en la tramitación del reclamo. (Posible cambio en la modificación de la circular.).

[48] Sobre esto tampoco existió pronunciamiento, sólo se eliminó la glosa de la pantalla que aparece en las sucursales de la farmacia. Creemos que, aunque se trata de un dato caduco, tendría que haber sido eliminado por la ISAPRE y guardar en sus registros sólo como archivo.

de datos de toda referencia a que la recurrente es paciente GES y el diagnóstico médico en todas sus sucursales[49].

F. Con el informe de la Superintendencia quedó acreditado que: la acción administrativa sólo se dirigió contra la Isapre Banmédica y no se acreditó la medida de eliminación de los *"registros de ventas de medicamentos GES"* en que se funda la sentencia en alzada, y no también hacia la Farmacia Cruz Verde[50].

Por lo que la señora Castro, solicitó:

1. La revocación del fallo en alzada en todas sus partes, dando lugar al recurso de protección y restablecer el imperio del derecho ordenando:

a) Para la Isapre Banmédica y a la Farmacia Cruz Verde, la eliminación en las bases de datos institucionales todos los datos personales, y datos sensibles, de la recurrente, obtenidos de forma ilegal y sin autorización de la actora, declarándose expresamente que desde el 9 de marzo de 2008 no es beneficiara GES.

Ello, debido a que a la fecha no se ha acreditado en auto la eliminación de dichos registros, para así dejar sin efecto todos los actos arbitrarios e ilegales de las recurridas.

b) Oficiando, a quien corresponda, para que fiscalicen el cumplimiento de esta resolución por el desamparo, desprotección y vulneración de la vida privada que afecta a la recurrente ante el poder económico de la sociedades anónimas, y la falta de acceso a las bases de datos donde sus datos personales y datos sensibles, diagnóstico médico están registrados y aún permanecen sin ser paciente GES[51].

Por lo que solicitó la tramitación del recurso previa vista de la causa, en atención a la importancia y materia del asunto y por la conmoción pública que los hechos del recurso causaron a la opinión pública.

Farmacia Cruz Verde.

El día 25 de noviembre de 2009**,** solicitó que la apelación deducida por la recurrente, fuera resuelta previa vista de la causa, atendiendo a la complejidad[52] técnica de las materias ventiladas en el recurso de protección y la connotación pública[53] generada por el caso.

Isapre Banmédica.

Se hizo presente en el proceso el día 27 de noviembre de 2009.

---

[49] En teoría, se solventó con el reclamo administrativo, pero suponemos que ella quería cubrir un mayor espectro, ya que se desconocía si la cadena de farmacia tenía estos datos, posiblemente lo quería hacer a nivel general. Esto genera un grave inconveniente puesto que no se sabe hasta dónde llego la transferencia de sus datos. La Superintendencia debió pronunciarse al respecto y la Corte también.

[50] Este es otro problema de la ley. Pero consideramos que si existe violación por parte de la misma, en virtud del tratamiento de datos sensibles cuando no estaba facultada por ley para hacerlo. En caso de que si esté facultada es la eliminación del registro por haber caducado. Para lo cual preguntamos: ¿Quién la sanciona? Este es el inconveniente, al no existir un órgano competente sobre la materia.

[51] Debió invocar hacer uso del derecho consagrado en el artículo 12 de la Ley. Sin embargo, la totalidad de la eliminación opera para la farmacia, por no ser autorizada por ley ni por la titular para tratar datos sensibles. De acuerdo con el artículo 15, inciso final, la Isapre no puede eliminar que tuvo la cobertura GES, pero si debe rectificar que la cobertura ya finalizó, indicando que la señora no tiene cobertura desde el 9 de marzo de 2008.

[52] Necesidad de órgano especializado.

[53] Los medios de comunicación fueron un actor de peso relevante.

Tercera Sala de Suprema Corte.

El día 21 de diciembre de 2009, confirmó sin argumentos adicionales la sentencia apelada.

Cabe señalar, por último, La señora Castro, solicitó la devolución de documentos en custodia en dicha instancia. Otra situación que se podría solventar con una política pública adecuada, evitando la burocratización que genera el avocarse a instancias judiciales.

5. Comentarios, Conclusiones y Recomendaciones finales respecto al caso.

En el desarrollo de cada etapa del caso visto, se han hecho diversas observaciones, comentarios, así como conclusiones y recomendaciones, no obstante ello, se considera oportuno traer a considerar puntualmente algunos aspectos adicionales.

1. A la señora Sara Castro le fueron transgredidos principios básicos inherentes a un dato personal, tales como el traslado de la información sin mediar autorización y sin guardar los mecanismos de traslado adecuados, falta de consentimiento del titular, el plazo de la información, modificación y eliminación de los registros.

2. Existen diversos vacios en la legislación, en el caso antes señalado se verificó que debido a que la Farmacia no está autorizada por el titular para el tratamiento de datos sensibles, no fue posible por parte de la Superintendencia de Salud, ordenarle rectificar datos de su base, quedando sujetada a requerírselo únicamente a la Isapre.

3. La Superintendencia de Salud, determinó que el convenio suscrito entre la Isapre y la Farmacia se encontraba emitido en orden, y que el problema fue que el mismo no se cumplió tal como fue constituido.

   Sin embargo, a nuestro criterio la cláusula de confidencialidad trata los datos como si los mismos fuesen propiedad de la Isapre, no mediando distinción alguna, cuando en realidad la titularidad de los mismos es de las personas naturales afiliadas debido a su característica peculiar de datos sensibles. En ese sentido, si la Superintendencia está de acuerdo con la emisión de dichos tipos de acuerdos, debería en todo caso efectuar revisiones previas a los mismos para su adopción, así como fiscalización de su cumplimiento.

   Con lo anterior recaemos nuevamente en la situación de la necesidad de una política pública que entregue el tratamiento de este tema a un organismo independiente, especialista en la materia, que cautele los principios establecidos en la legislación pertinente.

3. Como se planteó con anterioridad, las Isapres deben sujetar su actuar, entre otras, a las normas de la Ley No. 19.628 que establece la obligación de protección a la vida privada por parte de quienes están autorizados para transmitir datos personales y en especial respecto de quienes manejan datos sensibles, teniendo en consideración que los datos relativos a la salud de los individuos son sensibles y su insuficiente protección puede llevar a su uso no autorizado ó a su revelación a terceros.

4. Los hechos alegados por la actora, en los que fundó la acción recurrida en sede administrativa y la primera fase de la sede judicial, no se encontraron bajo la tutela del derecho durante la tramitación. Los mismos fueron efectivamente resguardados hasta

que la Superintendencia de Salud realizó la fiscalización respectiva y ordenó la rectificación de la base de datos.

En ese sentido, el resultado del recurso de protección invocado, conllevaba como Sala al haberse corregido la situación por parte de la Superintendencia de Salud.

Siendo posible concluir que dicho recurso reparó los perjuicios que sufrió la señora Sara Castro por el tratamiento ilícito de sus datos, tal como las directrices antes analizadas lo indican, siendo por lo tanto insuficiente en su aplicación efectiva.

5. La señora Sara Castro, en su calidad de profesional del derecho conocía las instancias adecuadas para recurrir, sin embargo, nos preguntamos ¿qué sucede con el grupo de ciudadanos que carece de la información respectiva?

   Si bien se tienen mecanismos para proteger los datos personales a través de la emisión de la normativa actual, se advierte que los mismos no accionan de la forma correcta, de igual forma no existe una política pública específica que permita a los afectados conocer de las garantías y de las instancias idóneas para evitar y corregir dicha vulneración.

6. El otorgamiento del beneficio de salud no se configura con la entrega de medicamentos, el beneficio se otorga cuando el interesado acude a la Isapre a reportar la condición y el deseo de cobertura GES. La entrega de medicamentos solo constituye una derivación o ejecución del beneficio ya otorgado, en ese sentido tanto la Isapre, la farmacia como al Superintendencia emitieron una interpretación distinta a la planteada.

7. El caso ocurrido fue ventilado debido a la denuncia interpuesta por Sara Castro, sin embargo, con dicha acción se determinó no solamente la vulneración de resguardo los datos de la señora Castro sino de todos los afiliados tanto de la Isapre Banmédica como Vida Tres, resultando paradójico el hecho que la se impuso una multa que luego fue disminuida.

8. Finalmente podemos indicar que las ilegalidades cometidas se resumen en:

Ley 19.628	Infracción de la ISAPRE	Infracción Farmacia Cruz verde
Artículo 6	La no eliminación por haber caducado). No necesitaba requerimiento del titular. (eliminación de datos personales?)	
Artículo 7	Confidencialidad de los mismos datos.	
Artículo 9 inciso 2	Exactos y actualizados y responder con veracidad a la situación real del titular.	
Artículo 10		La Farmacia no está facultada por ley para tratar datos sensibles.
Artículo 11	No guardó la debida diligencia.	

6. Conclusiones y recomendaciones generales.

1. La protección de la privacidad y el tratamiento de la información personal requieren de una coordinación por parte de las empresas privadas y el Estado, con la finalidad de

ofrecer al ciudadano una adecuada protección a su intimidad, y a la vez, la promoción del comercio tanto a nivel nacional como internacional.

2. Chile fue de los primeros países de Latinoamérica en aprobar una ley de protección a la privacidad, la cual contiene varios principios fundamentales sobre protección de datos personales, sin embargo debido al ritmo vertiginoso y evolutivo de la sociedad, el comercio; así como la realidad actual del país, dicha legislación demanda una reforma profunda, lo que conlleva de forma implícita la creación de un ente con autoridad de supervisión y control de los principios fortalecidos como el principio de la finalidad del dato. Esta sugerencia se encuentra en concordancia con los requerimientos de la OCDE.

3. Ha quedado evidenciado que sin dicho órgano fiscalizador independiente, la Ley podrá adolecer de una efectiva ejecución. Por lo que debe asimismo incorporarse un régimen de sanciones adecuadas, equiparables entre la conducta efectuada y la sanción económica. Existen, por ejemplo, una moción parlamentaria que buscan endurecer las penas a quienes hagan un mal uso de los ficheros de datos personales.

4. La Ley actual no específica sobre la transferencia internacional de datos, lo que permite concluir que dicha actividad se encuentra permitida, siempre y cuando se cumplan las disposiciones generales establecidas en la misma, no obstante ello, es recomendable que la reforma delimite sobre este punto a efecto de tener reglas claras y precisas que contribuyan al flujo del comercio internacional.

5. Se ha observado que si bien las modificaciones a las Ley 19.268 no están avanzando, se han promulgado leyes complementarias que regulen el tratamiento de los datos personales, previniendo que bases de datos de usuarios sean vendidas o intercambiadas entre empresas. Actualmente las bases de datos son un bien intercambiable entre empresas, entregando información personal de una empresa a otra, sin el permiso de quien es dueño de esa información.

6. Se ha visto que la experiencia europea posee una adecuada regulación en el tema de protección de datos personal, la cual marca la tendencia a nivel mundial, habiendo redactado una serie de informes que contienen valiosas aportaciones para su estudio. Sin embargo en el capítulo II del presente estudio, se advirtió cinco áreas que coinciden en la mayoría de directrices y lineamientos internacionales sobre el tratamiento de datos personales, por lo que se recomienda su análisis y adopción.

7. Es necesaria la adopción de una política pública integral, que facilite la implementación de la legislación adecuada, los recursos suficientes para su aplicación, la promulgación de campañas publicitarias que hagan del conocimiento a la población en relación con los derechos que poseen, así como las instancias donde pueden recurrir.

8. La adopción de un organismo técnico especializado en la materia permitirá facilitar al ciudadano vulnerado la ejercitación efectiva de la figura del habeas data legal.

9. Se recomienda dar trámite expedito al estudio y análisis de las propuestas de reforma de Ley existentes, es decir un cambio legislativo urgente, que permita determinar la necesidad de no adoptar copias de otros países sino más bien buscar un modelo integral acorde a la protección de los principios necesarios de la protección de los datos personales, como la adopción de un ente de control independiente.

7. Referencias Bibliográficas.

ALTER, Steven. 1999. *A General Yet Useful Theory of Information Systems.* Communications of the Association for Information Systems. Volume 1, article 13. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.196.2706&rep=rep1&type=pdf> (Consultado Diciembre 2011).

APONTE NÚÑEZ, Emercio José. 2007. *La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano*. Revista de derecho privado. Número 12-13. Consultado en línea <http://dialnet.unirioja.es/servlet/articulo?codigo=3252388> (Consultado Agosto 2011).

ARRIETA, CORTÉS, Raúl. *Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile*. Expansiva. Marzo 2011. Consultado en línea <http://www.expansiva.cl/media/publicaciones/libros/pdf/12.pdf> (Consultado Junio 2011).

Banco Mundial. ¿Qué es la globalización? Grupo de políticas económicas y Grupo de economía para el desarrollo. Abril 2000, PREM. Consultado en línea <http://www.bancomundial.org/temas/globalizacion/cuestiones1.htm> (Consultado Junio 2011).

BECERRA PALOMINO. Carlos Enrique. *Derecho a la Intimidad e Informática*. En Revista del Colegio de Notarios de Lima Nº 3.-Lima, 1992-93.

BOLOGNA, J. y WALSH, A. M. 1997. *The Accountant´s Handbook of Information Technology*, John Wiley and Sons. Pp. 1.

Chile y la Protección de Datos Personales ¿Están en crisis nuestros derechos fundamentales? Serie Políticas Públicas. Ediciones Universidad Diego de Portales. 2009. Consultado en línea <http://www.expansiva.cl/media/publicaciones/libros/pdf/7.pdf> (Consultado Junio 2011).

CASTELLS, Manuel. *La nueva frontera del desarrollo: el modelo informacional.* Conferencias Presidenciales de Humanidades, Santiago de Chile. 2005.

La era de la Información. Economía, Sociedad y Cultura. Quinta edición. Siglo XXI, México, D.F., 1999.

La privacidad en Internet. Consultado en línea <http://www.uoc.edu/web/cat/articles/castells/m_castells10.html> (Agosto 2011).

DANIELS, John L. y DANIELS, N.C. 1993. *Global visión.* New York. McGraw-Hill, Inc.

DÁVARA RODRÍGUEZ, Miguel Ángel. 2004. *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC).* Davara & Davara, Asesores Jurídicos y Fundación Vodafone. Madrid, España. Pp.3.

GARAY, Luis Jorge. Colombia: estructura industrial e internacional 1967-1996. El concepto de Competitividad. Consultado en línea: <http://www.banrepcultural.org/blaavirtual/economia/industrilatina/246.htm> (Consultado Agosto 2011).

GARRIDO IGLESIS, Romina. 2013. El Habeas Data y la ley de protección de datos en Chile. Serie Bibliotecología y Gestión de Información N° 83, Junio, 2013. <http://eprints.rclis.org/19755/1/Serie%20N%C2%B0%2083%20Romina%20Garrido.pdf> (Consultado Octubre 2013).

HERNÁNDEZ MUÑOZ, Ana Karina; PALACIOS HENRÍQUEZ, Juan Andrés. 2008. Tesis: *El dato sensible. Su tratamiento en Chile y en el derecho comparado.* Facultad de Derecho. Universidad de Chile.

HUICHALAF ROA, Pedro. Artículo denominado *Sobre las modificaciones a la Ley N°19.628 de "datos personales" chilena*, publicado en la página web del Observatorio Iberoamericano de Protección de Datos. http://oiprodat.com/2013/11/13/sobre-las-modificaciones-a-la-ley-no19-628-de-datos-personales-chilena (Consultado Diciembre 2013).

MATUS, Jessica. Ponencia para Seminario Regional de Protección de datos. Transferencias Internacionales a Países con niveles adecuados y no adecuados de Protección, aspectos prácticos. Montevideo, 2010.

MATUS ARENAS, Jessica y MONTECINOS GARCÍA, Alejandro. 2006. *La cesión de datos personales*. Santiago 2006. Editorial Lexis Nexis.

OCAMPO, José Antonio. *Los paradigmas del desarrollo en la historia Latinoamericana,* pág. 19-58. Hacia la Revisión de los paradigmas del desarrollo en América Latina. CEPAL 2008.

PIACENZA, Diego Fabio. 2008. *El derecho a la intimidad y los medios de comunicación.* AR: Revista de Derecho Informático, ISSN-e 1681-5726, No. 133,2009 <http://dialnet.unirioja.es/servlet/articulo?codigo=3292313. (Consultado Marzo 2011).

RICO CARRILLO, Mariliana. 2007. *Derecho de las nuevas tecnologías*. Buenos Aires, Ediciones La Rocca.

SOLIS LIMA, Antonio Pozo. 2007. Mapeo de actores sociales. <http://intranet.catie.ac.cr/intranet/posgrado/SA508/1_Los%20actores%20de%20un%20territorio/3%20Mapeo%20de%20actores%20sociales.pdf> (Consultado Octubre 2011).

SORIA, Carlos. La información de lo público, lo privado y lo íntimo. Consultado en línea <http://www.cuentayrazon.org/revista/pdf/044/Num044_004.pdf> (Consultado Agosto 2011).

VÁSQUEZ, Aldo. 1998. *Conflicto entre Intimidad y Libertad de Información: La experiencia europea*. Editorial Universidad San Martín de Porres, Facultad de Ciencias de la Comunicación.

WARREN, S. D. Y BRANDEIS, L.D. 1890. *The right to privacy*, en Harvard Law Review, 1890. Vol. IV, Nº 5, págs. 194 y siguientes. RIVERA, J. C., *Derecho a la Intimidad*, L.L., T. 1980-D-912.

Material Normativo consultado.

- Declaración Universal de los Derechos Humanos

- Ley 19.628 Sobre la Protección de la Vida Privada y su Reglamento, publicada en Diario Oficial el 18 de Agosto de 1999.

- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Informes de la Unión Europea.

    1. COM (2007) 87, firmado en 7 de marzo de 2007.
    2. COM (2003) 265, con fecha 15 de mayo 2003.
    3. Directiva 2002/56/CE, de fecha 12 de julio de 2002.
    4. Decisión de la Comisión con número 2004/915/CE, 27 de diciembre de 2004.
    5. Decisión 2001/497/CE, con fecha 15 de junio de 200.
    6. Reglamento 45/2001/CE que fue firmado en diciembre de 2000.

- Acuerdo de Puerto Seguro

- Ley No. 19.733. Sobre Libertades de Opinión e Información y Ejercicio del Periodismo, publicada en Diario Oficial el 4 de Junio de 2001

- La Ley 20.285, denominada Ley de Transparencia, publicada en Diario Oficial el 20 de Agosto de 2008.

- D.F.L. Nº 3 del Ministerio de Salud.

- Ley 20.575, Ley titulada "Establece el Principio de Finalidad en el Tratamiento de Datos Personales", también conocida como Ley DICOM, publicada en Diario Oficial el 17 de Febrero de 2012.

- Directrices de las Naciones Unidas para la regulación de los archivos de datos personales informatizados. Adoptadas mediante resolución 45/95 de la Asamblea General, del 14 de diciembre de 1990.

- Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.

- Ley Estatuaria No. 1266 de 2008 de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

- Pacto de San José de Costa Rica

- Declaración Universal de los Derechos Humanos

- Constitución Política de la República de Chile

- Reglamento del Registro de bancos de datos personales, contenido en el Decreto No. 779 del Ministerio de Justicia.

- Acuerdo de Asociación Económica, Concertación Política y Cooperación firmado entre Chile y la Comunidad Europea

- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Redactadas el 23 de septiembre de 1980.

- Circular IF No. 51 emitida por la Superintendencia de Salud de fecha 22 de agosto de 207.

- Circular IF No. 68, emitida por la Superintendencia de Salud, de fecha 6 de junio de 2008.

- Circular IF No. 104, emitida por la Superintendencia de Salud de fecha 31 de agosto de 2009.
- Decreto don Fuerza de Ley No. 1 de 2005, del Ministerio de Salud.

- Decreto No. 44 de 2007 del Ministerio de Salud

Procesos, Sentencias y Resoluciones Consultadas.

- Resolución Exenta I.F. No. 163 de fecha 30 de mayo de 2010. Emitida por la Superintendencia de Salud.

- Resolución Exenta I.F. No. 552 de fecha 16 de septiembre de 2010. Emitida por la Superintendencia de Salud.

- Resolución Exenta SS/No. 1480 de fecha 14 de octubre de 2010. Emitida por la Superintendencia de Salud.

- Sentencia definitiva de fecha tres de marzo de dos mil cuatro, emitida por la Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador, en el proceso de Amparo con referencia 118-2002.

- Recurso de Protección con Rol No. 6523-2009, interpuesto en la Corte de Apelaciones de Santiago.

Portales WEB consultados.

- Biblioteca del Congreso Nacional de Chile
  http://www.bcn.cl/

- Superintendencia de Salud.
  http://www.supersalud.gob.cl/portal/w3-channel.html

- Isapre.
  http://isapre.cl/

Noticias consultadas.

http://www.latercera.com/contenido/895_146299_9.shtml

http://www.cooperativa.cl/noticias/pais/salud/isapre/asociacion-de-isapres-defendio-entrega-de-informacion-de-enfermedades-a-farmacias/2009-05-26/075741.html

http://m.df.cl/isapres-relacion-con-farmacias-se-da-para-cumplir-con-el-auge/prontus_df/2009-05-27/102800.html

http://www.elciudadano.cl/2009/05/26/8287/isapres-estarian-vendiendo-informacion-sobre-las-enfermedades-de-sus-afiliados-a-las-farmacias/

http://economia.terra.cl/noticias/noticia.aspx?idNoticia=200905261057_INV_78098854

http://radio.uchile.cl/noticias/87158/

http://www.cambio21.cl/cambio21/site/artic/20130510/pags/20130510134016.html

http://www.lanacion.cl/acusan-a-isapres-y-farmacia-de-trafico-de-informacion/noticias/2009-09-16/230322.html

8. Anexos.

Anexo 1. Cuadro que contiene las últimas reformas aprobadas relativas a la Protección de datos personales, indicado en la página

No.	Norma	Fecha Promulgación	Fecha Publicación	Organismo	Título	Parte	Acción	Tipo Modificación	Parte Modificada
1	LEY 20575	14-FEB-2012	17-FEB-2012	MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO; SUBSECRETARÍA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO	ESTABLECE EL PRINCIPIO DE FINALIDAD EN EL TRATAMIENTO DE DATOS PERSONALES	Artículo 7	MODIFICA	MODIFICAR	Artículo 17
2	LEY 20521	05-JUL-2011	23-JUL-2011	MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO; SUBSECRETARÍA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO	MODIFICA LA LEY Nº 19.628, SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA GARANTIZAR QUE LA INFORMACIÓN ENTREGADA A TRAVÉS DE PREDICTORES DE RIESGO SEA EXACTA, ACTUALIZADA Y VERAZ	Artículo UNICO	MODIFICA	MODIFICAR	Artículo 9
3	LEY 20463	15-OCT-2010	25-OCT-2010	MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO; SUBSECRETARÍA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO	MODIFICA LEY Nº 19.628, SUSPENDIENDO POR EL PLAZO QUE INDICA LA INFORMACIÓN COMERCIAL DE LAS PERSONAS CESANTES	Artículo UNICO	MODIFICA	MODIFICAR	Artículo 17
4	LEY 19812	11-JUN-2002	13-JUN-2002	MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA	MODIFICA LA LEY Nº 19.628, SOBRE PROTECCION DE LA VIDA PRIVADA	Artículo 2	MODIFICA		Artículo 16
	LEY 19812	11-JUN-2002	13-JUN-2002	MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA	MODIFICA LA LEY Nº 19.628, SOBRE PROTECCION DE LA VIDA PRIVADA	Artículo 2	MODIFICA		Artículo 17
	LEY 19812	11-JUN-2002	13-JUN-2002	MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA	MODIFICA LA LEY Nº 19.628, SOBRE PROTECCION DE LA VIDA PRIVADA	Artículo 2	MODIFICA		Artículo 18

Fuente: Biblioteca del Congreso Nacional de Chile.

www.bcn.cl - Biblioteca del Congreso Nacional de Chile

Anexo 2. Entrevista señor diputado Pedro Araya.

Señor diputado, ¿Por qué se hizo un apartado especial para modificar la ley de DICOM y no se trabajó en modificar la Ley sobre Protección de Datos personales?

Lo primero que hay que decir es que Chile tiene una legislación muy antigua en materia de datos personales. Tenemos, por tanto, una legislación que es bastante débil para proteger los datos, y responde, más bien, a una realidad económica del país de los años setenta, ochenta; Entonces, esta legislación no se condice con lo que está pasando en el Chile actual. El tema de la Ley de DICOM respondió básicamente a la necesidad de avanzar, a lo menos, en uno de los temas que más preocupaban a los ciudadanos. Había ciudadanos que por distintos motivos caían en DICOM y esto se les volvía una verdadera traba, dado que muchas empresas estaban pidiendo a gente que postulaba a un trabajo traer el DICOM. Esta fue la razón. Además, entendemos que la nueva Ley de protección de Datos Personales será una ley con una discusión más larga, porque hay que abarcar una serie de temas. Nuestra idea, por tanto, darle una señal a la ciudadanía, de que íbamos a protegerla, impidiendo que las empresas discriminaran a los ciudadanos que postularan a los trabajos a causa del DICOM.

Muchas veces la ciudadanía hace una interpretación errónea y se sobre-endeuda. No sé si el congreso ha previsto eso y está ideando algún tipo de propuesta a la ley en general, para poder educar a la gente respecto a la ley.

Básicamente los temas de educación son de competencia del gobierno no del parlamento. Nosotros lo que hacemos es la parte legislativa, todo lo que tenga que ver con la parte educacional lo realiza principalmente el gobierno. El Congreso, dentro de las actividades que realiza, también puede hacer campañas de difusión, seminarios, explicaciones a la gente. Con respecto al otro tema, efectivamente aquí existe un problema de sobre-endeudamiento, porque la gente no es que malinterprete, sino es que se han acostumbrado un poco a sobre-endeudarse. Los chilenos verán que la ley del DICOM, en algún minuto, les favorecerá, en el sentido en que no les aparecerán las deudas consolidadas que tenían. En líneas generales, mi impresión es que la tasa de endeudamiento que tienen muchos chilenos se mantendrá o se hubiera mantenido con o sin la aplicación de esta ley.

La Ley de regulación del DICOM establece diversos tipos de principios de protección de datos personales. Y, sobre todo, lo que se trató de modificar fue el principio de finalidad. También se establece acerca de los Medios probatorios que es responsabilidad de que quienes son responsables de esta base de datos el probar ante un juez, que cumplieron con los principios correspondientes a la ley de Protección de Datos Personales.

Sí, el gran problema que hay en Chile y, que seguimos teniendo, es que no ha habido una definición clara y precisa *de cuál es la protección de datos y para qué son los datos*. Entonces lo que había ocurrido antes de la Ley de DICOM, es que teníamos un verdadero trafico por parte de empresas de bases datos de ciudadanos. Estas bases de datos que se fueron construyendo en el tiempo y que fueron creadas por establecimientos comerciales, bancos, cadenas del Retail, particulares. El problema es que estas bases de datos se vendían o se transaban entre estas empresas, afectando, obviamente, a una persona x que veía como sus antecedentes económicos o financieros eran conocidos por instituciones que no tenían por qué saberlo. Por ejemplo, alguna empresa antes de contratar trabajadores tenía conocimiento del estado financiero de una persona. Entonces, lo que se buscó con la Ley del DICOM fue justamente establecer la finalidad del dato. Segundo, nosotros tenemos una legislación civil y procesal civil que es muy antigua, nuestro código del procedimiento civil es del año 1900. Por tanto, la carga de la prueba era distinta, y básicamente se hacía inviable o muy difícil para

aquella persona que quería iniciar un juicio una demanda contra estas empresas que administraban bases de datos, poder presentar medios probatorios, dado lo limitado que son estos dentro de nuestro Código de Procedimiento Civil. La Ley justamente lo que buscó fue invertir la carga de la prueba para darle una mayor facilidad al ciudadano que se veía afectado por estas malas prácticas de alguna empresa.

Al Invertir lo de la carga de la prueba, entonces prácticamente el mecanismo de los medios probatorios estaría cambiando.

Claro, los estarían cambiando los medios probatorios, o sea más que cambiando, habrá una mayor facilidad en los medios probatorios.

Y en este caso, señor Vicepresidente, se necesitaría cuna capacitación adicional para los jueces que ven este tipo de materia. Tendría que ser responsabilidad, entonces, del órgano judicial de realizar este tipo de capacitaciones.

Lo que pasa es que el órgano judicial posee la Academia Judicial y todos los jueces, una vez al año, tienen que postular o hacen al menos un curso de perfeccionamiento de distintas materias como sectorización de legislación, nuevos procedimientos, entre otros. Entonces, mi impresión es que la propia judicatura dictará los cursos especializados en estas materias. Por lo demás, a mi me ha tocado ver que la Academia Judicial o el órgano jurisdiccional organiza cursos de perfeccionamiento respecto a leyes especiales, respecto a modificaciones importantes que ha habido. Por tanto, no es de extrañar que, sino en el transcurso de este año o en el próximo, vamos a tener dentro de los cursos a los que van a poder postular los jueces para perfeccionarse lo que diga relación con la Ley de Dicom. Amén de los seminarios particulares que organizan universidades u otras instituciones.

Acerca del proyecto que presentó de la modificación de la Ley 19628, que presentó el gobierno, se estableció en el boletín del mensaje del presidente donde decía cuales son las modificaciones que va a tener este tipo de ley; ¿ustedes ya prevén que tipo de inconvenientes políticos existirían al aprobar este tipo de proyecto?. Porque es un cambio muy fuerte el que se estaría haciendo a la ley. Por lo que he revisado, en este tiempo, se han presentado alrededor de más o menos setenta reformas a la Ley de Datos Personales, y éste es un cambio radical.

Todo proyecto de ley tiene complicaciones, porque uno nunca sabe que es lo puede pasar mientras se realiza la discusión. Ahora yo creo que éste es un proyecto que, si bien es cierto, hay bastante consenso en que hay que avanzar en lo que es protección de datos, también es cierto que se necesita modernizar la legislación, yo no estoy en condiciones de prever cuales van a ser los principales puntos de discusión. O sea, mi impresión es que efectivamente la principal discusión será qué es lo que pasa con las bases de datos históricas que están en poder de muchas tiendas y bancos.

Hay una denuncia contra Equifax, dado que está vendiendo su base de datos.

Se está aprovechando de vender información que tiene. Entonces justamente, yo creo que el principal foco de conflicto será ese. Porque obviamente habrá un lobby bastante fuerte sobre todo del comercio, del retail, de la banca de mantener este privilegio que tienen hoy día con las bases históricas.

Hay otro proyecto que se ha presentado por el diputado Nino Baltolu, que busca incrementar un tipo de sanciones, como ocurre con la legislación japonesa que busca

proveer una sanción más fuerte a todos aquellos que tengan o no una bases de datos personales y que cumplan con la finalidad o el tratamiento del mismo. Es algo más específico que la ley 19628. No sé si existe viabilidad para poder aprobar ese tipo de sanciones, me imagino que por lo mismo que está pasando con EquiFax, podrían darle una mayor promoción a esta reforma.

O sea, existe en la actualidad una mayor sensibilidad qen el congreso respecto a lo que está pasando con los abusos de algunas empresas que mantienen bases de datos. Obviamente puede generar que haya un mayor apoyo, porque el gran problema que tenemos en Chile es que muchas veces, y dado lo desactualizado de la legislación, a las empresas les sale más barato infringir la ley que cumplirla, porque generalmente estas conductas se sancionan con multas que son irrisorias respecto a las utilidades que tienen las empresas. Entonces, mi impresión es que dado de que aquí hay como un consenso de que hay que modificarlo, puede que este proyecto genere un apoyo transversal que le permita ser luego ley.

No sé, señor diputado, si recuerda un caso donde una isapre trasladaba información de sus usuarios a una cadena de farmacias. Esto explotó debido a que una afectada puso una denuncia en la Superintendencia de salud y posteriormente un recurso de protección en la corte. El problema en este caso fue que la isapre y la cadena de farmacia, firmaron un contrato, donde ellos podían trasladar ese tipo de información. Y, desafortunadamente, en este tipo de contratos, la Superintendencia no está obligada a revisarlos porque se escapa un poco al ámbito privado, y explican que no se puede tener ningún tipo de intervención. Hasta qué punto podemos establecer un límite de hasta dónde puede llegar la esfera privada de la esfera pública en este tipo de casos de protección de datos.

Es que…A ver el principio básico en Chile es que el organismo público actúan dentro de los límites que fija la constitución y la legislación. Si la superintendencia, no tiene facultades para fiscalizar, obviamente que no lo hará, así como tampoco podrá hacerlo ningún organismo, porque ese es el principio básico constitucional en Chile. Entonces en esa lógica…Claro, obviamente si uno mira y además a eso, uno le suma que nuestra ley de protección de datos son bastante débiles, obviamente las cadenas de farmacia, y en este caso, la isapre utilizaron los forados que tiene la legislación, para hacer algo que es éticamente reprochable, pero que legalmente no está prohibido; bueno y como nos encontramos entonces en derecho privado, y en derecho privado tú puedes hacer todo lo que expresamente no esté prohibido por la ley, entonces obviamente ahí, hay un reproche ético o moral que uno puede hacer. Buena parte de las modificaciones a la legislación se están dando por estos casos que han ido ocurriendo. Porque con ellos se burla el espíritu de la ley, pero como la ley expresamente no lo prohibió, lo pueden hacer. Y por eso es importante avanzar en la modernización de nuestra nueva protección de datos personales. Porque, si uno la observa, nuestra protección de datos personales es muy débil, porque además, ésta tiene otros factores: cuando la sociedad chilena era otra, cuando la actividad económica en el país era distinta, cuando nuestra conectividad a internet era mínima respecto a lo que tenemos hoy día por ejemplo; o la capacidad de intercambiar información. Entonces ese es uno de los temas de porque hay que ir rápidamente legislando en esto.

Claro, más ahora como miembros de la OCDE.

Claro, es uno de nuestros requerimientos, justamente ese uno de nuestros temas a resolver…
Yo creo, lo que pasa es que nosotros tenemos problemas serios, porque, además nunca como país dimensionamos la necesidad de proteger datos, y ese fue el gran problema

No se colocó como en los puntos de agenda, de irlo reforzando, modificando, y acoplando a la tecnología y a la sociedad.

Porque generalmente se pensó en la protección, más que de datos, de ciertos grados de información de la persona. Pero después te das cuenta que tenemos un mundo que cambió en menos de diez años, y que ahora los datos son un bien absolutamente transable y muy apetecido en el Mercado. Y en eso nos fuimos quedando un poco atrás. De hecho, si uno mira lo que ido pasando en los últimos veinte años, se ha dictado mucha legislación parche para ir protegiendo datos, por ejemplo, la ley del DICOM, respecto, por ejemplo, de los temas sanitarios, del de las fichas médicas. Entonces no hubo una mirada global del tema, hasta que las autoridades se dieron cuenta de que efectivamente aquí tiene que venir una regulación global. Porque, además, hoy en día, el nivel de intercambio de información, y la rapidez con que tú puedes cambiar la información no es la misma que hace diez o quince años atrás, entonces por eso se ha hecho necesario poder ir avanzando en estos temas. Y aquí hay que ir directamente a la finalidad del dato. Porque cuando uno legisla tiene que hacerlo pensando en la gran mayoría del país; pero, obviamente, siempre habrán excepciones a la regla, entonces lo que hay que tratar de buscar aquella norma, o aquel fin que pueda efectivamente fijar los lineamientos para todo el país. Y en esa línea, creo que el tema de la finalidad del dato va a ser lo más concreto y lo mejor. Y eso, además, tiene que ir de la mano, aparejado también con modificaciones a otros cuerpos normativos: Código sanitario, el mismo código civil, el código del trabajo, respecto de como esta ley se integre con las otras normas que son bastante más antiguas y que no están en carpeta que van a ser modificadas.

Podría decirse, entonces, que la finalidad del dato, es lo más importante de resguardar:
La finalidad del dato es lo más importante de resguardar.

Muchísimas gracias Señor Diputado.

Anexo 3. Noticias de la prensa.

Fuente:

http://www.lanacion.cl/acusan-a-isapres-y-farmacia-de-trafico-de-informacion/noticias/2009-09-16/230322.html

Acusan a isapres y farmacia de tráfico de información
Jueves 17 de septiembre de 2009

El diputado Gabriel Silber (DC) denunció ayer la existencia de un convenio entre Farmacia Cruz Verde y las isapres Banmédica y Vida Tres, que violaría la ley sobre protección de datos de carácter personal, ya que permite que estas empresas compartan y trafiquen información sobre todas las compras que realiza un usuario e incluso sus diagnósticos médicos.

El parlamentario exhibió el contrato, al cual se pudo acceder gracias al recurso de protección que interpuso en mayo la abogada XXXXX, quien se percató que el dependiente conocía su patología AUGE.

"Ésta puede ser la punta del iceberg de la cual nosotros creemos ha sido la política de la industria farmacéutica a la hora de traficar y comerciar con información privilegiada de los consumidores", señaló.

FISCAL DE COLUSIÓN

Los antecedentes obtenidos serán proporcionados al fiscal que investiga la colusión en el caso farmacias, con el objetivo de abrir una nueva arista en este caso.

Además del convenio, en el juicio que está en curso y que se vio el martes pasado en tribunales, se accedió a documentos donde figuran todas las compras que realizó Sánchez, desde pañuelos desechables hasta fármacos, lo que permite elaborar un completo perfil de la paciente.

Los denunciantes explicaron que las isapres y farmacia pueden establecer convenios para comprar y distribuir medicamentos del AUGE para optimizar el servicio a los clientes, pero lo que no pueden hacer es violar la privacidad de las personas.

"Cuando leí el documento me entero que el convenio no se circunscribe a AUGE, sino que también posibilita la emisión de informes sobre consumo", dijo la abogada. Lo anterior se establece en la letra K del documento, firmado el 29 de junio de 2005 y que obliga a la emisión mensual de reportes.

Al cierre de esta edición, por medio de un comunicado, ambas isapres y la farmacia aclararon que "ha convenido las estipulaciones estrictamente necesarias para otorgar debidamente los beneficios (…) y sólo se utilizan para efectos de cumplir con las exigencias de la Superintendencia de Salud".

Fuente:
http://economia.terra.cl/noticias/noticia.aspx?idNoticia=200905261057_INV_78098854

Isapres hacen sus descargos en polémica por intercambio de información con farmacias
26 de Mayo de 2009
Por Sergio Jara Roman

SANTIAGO, mayo 26.- El director ejecutivo de la Asociación de Isapres, **Rafael Caviedes**, descartó que el presunto intercambio de información entre farmacias e isapres fuera un tráfico de datos personales de pacientes, tras la denuncia suscitada por una abogada que pudo comprobar cómo los datos de su enfermedad, y que conocía su isapre Banmédica, figuraban en una base de datos de un local de Farmacias Cruz Verde.

Ante este caso, la Superintendencia de Salud salió a confirmar que Banmédica y la isapre Vida Tres son investigadas, sin descartar sanciones, mientras el diputado PS Fulvio Rossi aseguró que la cadena Salcobrand también recibe información confidencial de parte de las instituciones privadas de salud.

Al respecto, Caviedes dijo que las Isapres se ven obligadas a distribuir sus medicamentos AUGE a través de las farmacias, por lo que resguardar el secreto de diagnóstico es muy difícil.

En entrevista con **Terra.cl**, Rafael Caviedes habla sobre el nuevo caso que pone en tela de juicio al sector privado de la salud.

¿Las asociación de Isapres cómo evalúa este intercambio de información entre isapre y farmacia?
Las Isapres por el AUGE adquirieron el compromiso legal de entregar los medicamentos que corresponden a las 56 patologías AUGE de sus afiliados. Por otra parte, el Código Sanitario establece que exclusivamente las farmacias pueden distribuir medicamentos en Chile y los hospitales públicos a través de su consultorio obviamente.

Por lo tanto, las Isapres no tienen otro mecanismo para entregar los medicamentos del AUGE para cumplir con la ley, que no sea haciendo convenio con las farmacias. En consecuencia, eso es lo que motiva a esta vinculación que existe entre las Isapres y las farmacias, una vinculación obligada por ley para poder cumplir con el AUGE. Ahora, es evidente que hay que mejorar los mecanismos de información que existen para que esto sea lo más confidencial y se proteja de la mejor forma posible a los pacientes. Yo estoy pero absolutamente de acuerdo en la necesidad de entregar la mayor protección posible a los pacientes.

Por ejemplo, ¿a través de códigos en vez de nombres de enfermedades?
Claro, pero de todas maneras hay que tener presente que si al paciente X le corresponde entrega una fluoxetina o un medicamento de esa naturaleza, es evidente que ese paciente tiene depresión y si al otro paciente le corresponde entregar la triterapia para el Sida, es evidente que ese señor es un enfermo de Sida. Entonces, está bien, se le entrega el código, este paciente tiene la enfermedad del código 56, pero si se le está entregando la triterapia del Sida van a saber igual.

¿Cómo se hace esto de forma más privada?
Bueno, eso es bien difícil.

Se armó todo un revuelo a partir de esto...
Bueno, fue bien lamentable la situación, y por eso mismo yo creo que hay que tomar mejores providencias para cautelar la privacidad del diagnóstico de los pacientes.

¿Es una práctica generalizada de las Isapres con las farmacias?
Yo no tengo idea como estarán operando las Isapres, yo lo que digo es cuál es la obligación que tienen las Isapres, cual es la obligación que le entregó la ley a las Isapres para entregar estos medicamentos y por qué razón las Isapres tiene que operar a través de las farmacias.

¿Ustedes como asociación de Isapres se juntarán con el gobierno para ver qué curso seguirá este tema?
No. Aquí hay una ley que regula la entrega de medicamentos del AUGE lo cual se hace a través de las farmacias de Chile. Las farmacias de acuerdo al Código Sanitario, son las entidades autorizadas por ley para distribuir fármacos.

Sí, pero el problema no es ese. El problema es que se están entregando los datos personales, la información de los consumidores.
Las Isapres están obligadas a dar medicamentos a los pacientes AUGE según su diagnóstico. Entonces, hay que establecer la mejor vinculación posible entre farmacia e isapre para tratar de cuartelar la privacidad del paciente, no obstante, le insisto, eso es difícil por cuanto la isapre tiene que entregar los medicamentos establecidos en el protocolo para cada diagnóstico, y esos medicamentos indican claramente aunque nadie lo quiera, cuál es el diagnóstico que tiene ese paciente.

En el debate sobre este caso se habla sobre tráfico de información o datos personales entregados por la isapre a la farmacia y que pueden ser utilizados para otros fines comerciales... ¿qué le parece eso?
No tengo idea en realidad, me sorprendí mucho del titular de *La Tercera*. Quizás hubo un tratamiento poco cauteloso o criterioso de parte del dependiente de la farmacia (en el caso expuesto por la prensa).

¿Considera que el caso de colusión de las farmacias salpica a este tipo de cosas?
Seguramente, pero las Isapres tienen la obligación de entregar los medicamentos AUGE a las farmacias y los medicamentos, necesariamente tienen un cartel con el diagnóstico. Cualquier persona, hasta nosotros que somos civiles y no médicos, sabemos perfectamente que una triterapia corresponde a un Sida, cuáles son los nombres para los medicamentos del cáncer, la depresión y con mayor razón lo sabe una persona que trabaja en una farmacia. Es complejo el manejo de la información. Mientras las isapres tengan que operar por las farmacias de acuerdo a lo que establece el código sanitario, va a ser así.

¿Tendrán que idear un sistema de códigos complejo entonces?
Lo que hay que hacer es no referirse al diagnóstico para cautelar la mayor privacidad posible.

Fuente:
http://m.df.cl/isapres-relacion-con-farmacias-se-da-para-cumplir-con-el-auge/prontus_df/2009-05-27/102800.html

Isapres: relación con farmacias se da para cumplir con el Auge
Miércoles 27 de mayo de 2009

El director ejecutivo de las Isapres, Rafael Caviedes explicó que si se prohíbe esta vinculación, "el Auge se acaba".

El director ejecutivo de las Isapres, Rafael Caviedes, reiteró hoy que la vinculación que se da entre las farmacias y las Isapres se da para cumplir con los protocolos del plan Auge y que estos datos se usan exclusivamente dentro de este contexto.

"Lamentablemente no se explicó en forma oportuna que esta relación se hace por la obligación que tienen las isapres de entregar los medicamentos Auge. Esa explicación no se ha dado de forma oportuna, la gente no la entendió así, tampoco el Gobierno. Es absolutamente necesario que exista esta vinculación. Desde el momento en que a las isapres se les prohíba ejercer esta vinculación, el Auge se acaba", explicó Caviedes a Radio Agricultura.

"Lo mismo sucede con los hospitales. Llegaríamos a una locura y un absurdo donde no se podría mover ninguna información, tiene que haber una cierta cordura y operatividad del sistema para que el Auge funcione", agregó el ejecutivo.

Caviedes sostuvo que "tendría que haber una caja secreta y entregar los medicamentos con unos guantes negros, una cosa así, cosa absurda. Los medicamentos hay que entregarlos y lo hace un dependiente de la farmacia, alguien perfectamente identificado. Al final de la línea siempre se va a dar esto", señaló.

El director ejecutivo aseguró que "la ley obliga a las Isapres a entregar el Auge. El Código Sanitario dice que sólo pueden entregar medicamentos ambulatorios las farmacias. Las Isapres tienen giro único y no pueden tener farmacias. Teniendo esto en consideración, se entiende que las Isapres para poder cumplir con el Auge tienen que establecer convenios con las farmacias para entregar medicamentos ambulatorios", precisó Caviedes.

El tema se da luego de conocerse la entrega de información de las fichas clínicas de los cotizantes de ciertas Isapres a una de las grandes cadenas farmacéuticas, lo que abrió un debate para el Ministerio de Salud, que ayer confirmó su intención de presentar acciones legales en contra de quienes resulten responsables del traspaso de datos confidenciales.

Fuente:
http://www.cooperativa.cl/noticias/pais/salud/isapre/asociacion-de-isapres-defendio-entrega-de-informacion-de-enfermedades-a-farmacias/2009-05-26/075741.html

Asociación de Isapres defendió entrega de información de enfermedades a farmacias.
26 de mayo de 2009

Descartó que haya traspaso de historiales médicos.

Señaló que por ley es necesario para otorgar medicamentos de las patologías cubiertas por el AUGE.

El director ejecutivo de la Asociación de Isapres, Rafael Caviedes, defendió la entrega de información de enfermedades a las farmacias, ya que señaló que, por ley, están obligadas en los casos de las patologías cubiertas por el AUGE, descartando el traspaso de historiales médicos.

Caviedes declaró a El Diario de Cooperativa que las isapres por ley están obligadas a entregar el AUGE y que éste contempla otorgar medicamentos ambulatorios, por lo que las entidades deben hacer convenios con las farmacias para que éstas puedan ofrecérselos a los pacientes.

"Nunca ninguna isapre ha entregado los historiales médicos, pero si una persona que tiene diabetes por ejemplo, la isapre le tiene que informar a la farmacia que a esa persona hay que entregarle determinados medicamentos", afirmó.

La polémica se desató luego de que la abogada XXXXX denunciara que todos los locales de la cadena de la Farmacia Cruz Verde conocían su enfermedad por lo que la Superintendencia de Salud comenzó una investigación a las Isapres Banmédica y Vida Tres.

Caviedes reforzó que "no hay ninguna situación irregular en la entrega de información de la Isapre a la farmacia para la entrega de medicamentos AUGE porque esa información es necesaria que la farmacia la tenga".

Sin embargo, señaló que "lo que no se puede permitir es que se vocee el diagnóstico en las farmacias, que se diga en altavoz y que se vulnere la lógica de confidencialidad que existe en determinado diagnóstico".

"Yo le puedo asegurar que aquí no hay traspaso de historiales médicos, lo que pasó en este caso en particular es que el dependiente voceó" los medicamentos que necesitaba la paciente, afirmó.

Fuente: http://radio.uchile.cl/2010/10/15/la-huella-digital-el-otro-costo-de-los-bonos-de-isapre

No hay salud

La huella digital, el otro "costo" de los bonos de Isapre
Rodrigo Alarcón López
15 de octubre de 2010.

Un usuario se niega a usar la huella digital para atenderse y obtiene una particular respuesta, al margen de la ley sobre datos personales, que lo obliga a comprar sus bonos en una sola sucursal. "Es como un castigo", dice, mientras sigue esperando para atenderse. Abogados y organizaciones de usuarios explican por qué la isapre no cumple como debería.

Justo cuando se cumplían ocho meses de su primer reclamo, el pasado martes 12 de octubre, el ingeniero Jaime Baeza insistió con una nueva solicitud ante la Superintendencia de Salud que se arrastra desde inicios de año.

Entonces pidió dos cosas a la Isapre Consalud: no ser obligado a firmar un contrato, a través de la huella digital, con el servicio I-Med al momento de comprar un bono para obtener una atención de salud; y conocer qué datos son almacenados a través del dispositivo, para qué son utilizados y, especialmente, aclarar la "posible comunicación a terceros" que figura en ese contrato.

Ante la solicitud, Consalud accedió a eliminar la información de Jaime Baeza desde la base de datos de I-med, obligándolo a concurrir a una sola sucursal para comprar sus bonos sin usar la huella y sólo su carnet de identidad. La empresa recalcó además que los datos no se pondrán a disposición de terceros, pese a que el contrato que se firma al usar el dispositivo digital estimula la eventual transmisión de esa información.

La Superintendencia acogió el allanamiento de la empresa y dio un plazo de tres días al ingeniero para presentar sus observaciones. Sin embargo, la carta que lo informaba llegó a su casa días después, por lo que el caso quedó resuelto sin que éste obtuviera lo que buscaba.

A meses de ocurrido lo anterior, Baeza explica que "estoy todavía en una situación stand-by, esperando que la Superintendencia me dé una respuesta respecto a mi petición del 19 de abril, que fue dilatada, para que resuelvan o traten de conseguir la información de la isapre. Lo que persigo es que me digan: 'usted puede atenderse en cualquier parte y comprar el bono presentando el carnet de identidad'. Eso debería ser el resultado final, para todos, no sólo para mí. Y que la empresa I-Med diga lo que sabe".

Según dice el usuario, el objetivo es que "se publique cuáles son los datos que ellos almacenan, porque eso va a decir por qué los almacenan, obvio. Si ellos lo que necesitan es validar tu identidad por la huella, como cuando vas a cobrar un cheque al banco, en que toman mi huella, la contrastan y listo. Si es así, por qué no lo aplican en la isapre también. Entonces aquí hay algo que están ocultando y me gustaría que se supiera. Y si quiero que mis datos estén ahí para ahorrarme tiempo sea una elección completamente libre e informada".

Un asunto social
No es primera vez que un particular cuestiona el uso que las instituciones de salud hacen de sus datos. Cuando se conoció el caso de Baeza, la abogada XXXXX participó de la denuncia presentada ante la Superintendencia de Salud por el diputado Gabriel Silber (DC). La jurista

ya había denunciado, años atrás, que las isapres Banmédica y Vida Tres compartían su información con la cadena de farmacias Cruz Verde.

Respecto al caso de Jaime Baeza, el coordinador de la Organización de Consumidores y Usuarios, Alejandro Pujá, enfatiza que la ley 19.628 "garantiza a los consumidores, a los titulares de los datos, el derecho a saber el uso que se va a dar a la información. Y también a la seguridad de que ese dato no va a ser mal utilizado. Por lo tanto, los ciudadanos no están indefensos". Es decir, la petición del usuario está avalada por la ley, tal como él mismo lo recalca en una de las cartas que envió a la isapre.

Aunque Pujá es claro en que la organización no tiene denuncias sobre mal uso de las huellas dactilares, "la aprehensión que tenemos es que esa huella no esté correctamente almacenada, se pueda filtrar o ser mal utilizada".

El reclamo ante Consalud y la Superintendencia tuvo un costo para Jaime Baeza, porque no puede acceder a los servicios de salud como cualquier otro usuario. "Me sacaron de I-Med, pero con el perjuicio de que me obligan a comprar bonos en un solo punto, cosa que me coarta. En caso de que me quiera atender en otro punto, tendría que comprar un bono solo ahí. Es como un castigo", explica.

Según el abogado y ex presidente de la Corporación de Afiliados y Usuarios de Isapres, Pedro Barría, el usuario tiene "pleno derecho" a no querer usar el sistema de huella digital y "exigirle a la isapre que le habilite un sistema, porque no puede dejar de venderle bonos. No puede decir que los bonos se venden sólo con la huella, por lo tanto, a usted no le vendo más mientras no acepte utilizar la huella".

Asimismo, el abogado especializado en denuncias contra las instituciones privadas de salud enfatiza que el usuario no puede ser obligado, como en el caso de Baeza, a comprar sus bonos en un único centro de atención: "No podrían imponerle eso. Hace cinco años no existía este sistema (de huella digital), la persona iba a comprar bonos y lo hacía en cualquier sucursal de la isapre. Deberían habilitar un sistema para que él pudiera comprar bonos en cualquier sucursal, no tendrían por qué imponerle una. Por ejemplo, ¿qué pasa si él viaja a Concepción? ¿Tiene que venir a comprar el bono a Santiago? Es absurdo. El problema lo tiene la isapre y ésta tendrá que ver cómo lo resuelve", explica.

Barría aclara que si eso significara un perjuicio económico para la empresa, "ésta verá cómo lo resuelve, él no tiene por qué hacerse cargo. Es un afiliado, necesita servicios de la isapre y ésta no se los puede condicionar a una sucursal o a que acepte usar la huella".

Baeza considera que el conflicto "es un asunto personal y social", porque el mal uso de la información personal podría ser usado con carácter discriminatorio también con otras personas: "El manejo de información cuesta plata y estas empresas lucran con eso, no creo que el tema sea la huella nada más", dice.

Mientras, continúa esperando una respuesta de su isapre que no sean "puras evasivas" y le dé una solución de fondo, y el resto de los usuarios se ven forzados a entregar su huella digital para acceder a una atención en salud. "Desde esa fecha yo no he vuelto a atenderme, porque quiero tener la claridad de cómo funciona el asunto y tener respuestas para hacer uso de mi plan de salud". Tendrá que armarse de paciencia.