**Universidad de Chile**
Facultad de Derecho
Departamento de Derecho Procesal
Centro de Estudios en Derecho Informático

# TRATAMIENTO DE DATOS SENSIBLES EN LA ACTIVIDAD DE INTELIGENCIA Y DE PERSECUCIÓN PENAL. EL CASO DEL INFORMANTE.

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

Cristian Andrés Campos Meza

Patricio Andrés Moreno Oviedo

Profesor guía: Alex Pessó Stoulman

Santiago, Chile

2014

Quiero expresar un profundo agradecimiento a mi familia, tanto la actual como la futura, por el arduo trabajo que ha significado el apoyarme durante esta investigación, especialmente a Daniela, sin cuyo amor, paciencia y aliento, esta empresa jamás hubiese llegado a un buen puerto.

-Cristian

A mi familia, por su apoyo constante.

-Patricio

## TABLA DE CONTENIDOS

## RESUMEN

Los autores buscan establecer la procedencia del tratamiento de datos personales sensibles por parte de los organismos de inteligencia y de persecución penal. A partir del análisis de los artículos 10º y 20° de la Ley 19 628 y de la legislación comparada, particularmente la argentina y española, se establece que éstos sólo pueden ser utilizados legítimamente cuando se cuenta con norma expresa en tal sentido, lo que determinará una búsqueda de dicha autorización en las respectivas legislaciones sectoriales. Se abordarán, al mismo tiempo, las diversas posturas doctrinarias, tanto aquellas que dicen encontrar autorizaciones genéricas, como aquellas que abogan por el principio de especificidad de la ley. Se sugerirá establecer una ley que autorice sólo bajo ciertos presupuestos acotados y específicos el tratamiento de datos sensibles en materia de seguridad nacional. Con respecto a la institución del informante, como método de investigación, se analizan las implicancias que acarrea su uso, tanto en materia de persecución penal como de inteligencia, con motivo del respeto de la intimidad de los investigados.

# INTRODUCCIÓN

Describamos a una persona: sexo masculino, un metro y setenta centímetros de estatura, ojos negros, cien kilos de peso. O bien podría ser una mujer: ojos azules, cabello castaño, esbelta complexión. Pero, ¿quiénes son estas personas?, ¿Qué podemos decir de ellas?, aparte de aventurar algún riesgo cardiovascular en uno o cierta ventaja para conseguir trabajo en otra, no podemos decir mayor cosa. La personas no estamos limitados a nuestro ente físico, la identidad se configura mediante la suma de pequeñas partes de información, cada una de las cuales aporta elementos definitorios que determinan quienes somos. No es lo mismo decir que nuestro hombre del ejemplo es un conductor de bus que decir que es un levantador de pesas; o decir que nuestra mujer tiene veinte años que decir que tiene sesenta. Nuestra percepción cambia con la simple adición de un dato.

Si la construcción de la identidad de un individuo a través de pedazos de información nos otorga una imagen suficientemente clara de lo que una persona es (o no es), esta imagen no es completa. Existen parcelas de información íntima, pequeñas islas sustraídas del conocimiento externo,

reservadas exclusivamente al propio individuo y su círculo cercano. Parecieran, en la suma, ser aspectos apenas decorativos en la identidad, pero condimentan cada una de las partes del ser, otorgando ese grano de arena que nos convierte en seres únicos e irrepetibles. Tradicionalmente estos antecedentes se denominan datos sensibles. Sensibles, porque son fuertemente susceptibles a estímulos externos no autorizados y principalmente porque alimentan el motor emocional que guía todas las acciones; las opiniones políticas, creencias religiosas, convicciones filosóficas o morales motivan el proceder de las personas en un determinado sentido; las acciones inmorales cometidas, las orientaciones sexuales minoritarias, el origen racial o estados de salud físicos o psíquicos se convierten en desventajas competitivas cuando son conocidas por personas con poder de decisión y que no comulgan o comparten con estos elementos característicos, que pueden devengar en discriminaciones arbitrarias. Por lo tanto, esta información se convierte en un capital valiosísimo que es necesario proteger. La Ley intenta encargarse de eso.

El hombre y la mujer son seres sociales y como tales se verán en la necesidad de compartir ciertas cantidades de información personal con la finalidad de generar confianza para así obtener determinados beneficios. Muchas veces será a través de actuaciones positivas; así, deberán aportar información referente a su capacidad económica y a su comportamiento comercial si quieren acceder a un crédito financiero; o entregar antecedentes sobre la cualificación profesional para obtener un trabajo; otras veces deberán tolerar la invasión al propio espacio, como la realización de exámenes físicos para obtener un diagnóstico médico, pero en todos estos casos el hombre o la mujer consienten en esta exposición, pues consideran que el beneficio lo justifica. Si descontamos esta tendencia actual de exponer voluntaria y públicamente la vida privada y sus matices a cambio de una remuneración económica y una fugaz fama, ningún beneficio justifica transar la información íntima. Nadie podría tampoco, como contraparte, éticamente requerirla. El problema radica, como usualmente ocurre, cuando la protección celosa de la vida privada afecta directa o indirectamente derechos o libertades de otras personas o intereses generales de mayor valor.

Seguridad nacional y orden público son bienes jurídicos esenciales para la vida en sociedad. Se dice que sólo un mínimo de seguridad garantiza el ejercicio de las libertades, mientras la mantención del orden público asegura que dichas libertades se ejerzan en paz. ¿Qué hacer cuando la protección de la vida íntima de las personas afecta la integridad de estos bienes jurídicos? Ya que el Estado es garante de ambos, ¿puede legítimamente irrumpir en la esfera privada de los ciudadanos para adquirir antecedentes sensibles de los mismos?, ¿puede hacer esto aun sin su consentimiento?, es más, ¿puede hacerlo sin su conocimiento?

Cierta tendencia concibe la mutación de las conductas privadas en públicas cuando su trascendencia social permite tal modificación. Así, las preferencias sexuales de una persona imputada o víctima adquieren relevancia tratándose de delitos contra la sexualidad; las creencias religiosas o convicciones filosóficas de sospechosos pasan a ser importantes tratándose de labores preventivas o investigativas de acciones terroristas.

¿Significa esto que la sola invocación de criterios generales como seguridad nacional u orden público justifican una intromisión activa del Estado en la esfera más íntima de las personas?

Nuestra labor es determinar si los organismos públicos, especialmente aquellos de persecución penal y de inteligencia pueden tratar datos personales sensibles, y de ser afirmativa la respuesta, en qué condiciones. Estableceremos un desarrollo del derecho que justifica la protección de datos, para determinar si el derecho a la intimidad se basta a sí mismo o si la construcción reciente del derecho a la autodeterminación informativa como manifestación positiva del primero, le permite una existencia independiente constituido como derecho de tercera generación; a continuación avanzaremos sobre los bienes jurídicos en cuestión: la seguridad nacional y el orden público, para luego centrarnos en los órganos públicos encargados de su protección.

Para determinar claramente si la actividad estatal permite establecer excepciones a la protección reforzada de los datos sensibles, analizaremos el sistema jurídico nacional de protección de datos, desde la propia Constitución, pasando por la Ley N° 19 628 de protección a la vida privada, hasta las leyes propias de los órganos en estudio. Revisaremos también la existencia de reglamentos o normas internas y si éstos pueden considerarse vinculantes como desarrollo de un derecho fundamental.

No pretendemos cuestionar la completa actividad de tratamiento de datos personales. Inteligencia o persecución penal sin información pierden el sentido; mientras la primera busca asesorar al poder ejecutivo en la toma de decisiones con el mayor fundamento posible, o anticiparse a hechos potencialmente gravosos que atenten contra la seguridad nacional interna o externa; la segunda busca alcanzar la verdad judicial, sea que esta implique la declaración de la culpabilidad del imputado o su inocencia, para lo que necesitará contar con todos los antecedentes necesarios y pertinentes para tal objeto. La información para ambas, es esencial.

El punto discutido radica en el hecho de si esta autorización legal de la que gozan los órganos públicos para tratar datos personales en general se extiende a su vez al tratamiento de datos sensibles; o si por el contrario, cada vez que quieran enfrentarse a esa actividad necesitan la existencia de una ley que legitime dicha acción, en cuyo caso estableceremos si esa norma existe y si es así, cuál es su alcance.

Todo el desarrollo de esta investigación está diseñado para converger finalmente en una figura bastante particular contemplada en la legislación chilena e inmersa directamente en el ámbito del tratamiento de los datos personales de estas dos áreas de la actividad estatal. Nos referimos, en efecto, al informante.

Tradicionalmente la inteligencia, como actividad de investigación, siempre estuvo ligada al potencial humano. Previo al surgimiento de las

tecnologías de la información, toda esta actividad giraba en torno a un núcleo esencial, integrado por la capacidad de agentes de recopilar antecedentes necesarios para los objetivos planteados. Posteriormente, ya en la segunda mitad del siglo XX, el desarrollo exponencial de las tecnologías de la información viene a desplazar del centro mismo de la actividad a los recursos de inteligencia humana, para resurgir finalmente en el último tiempo al revaluarse el potencial ilimitado del contacto interpersonal como fuente directa de información. Es en este contexto en el que se desarrolla la actividad del informante, figura que plantea numerosas interrogantes tanto respecto a los elementos que la integran como a sus implicaciones y consecuencias en el ámbito del respeto a los derechos y garantías fundamentales.

El Estado, que por una parte debe en su actuar respetar todos los derechos y garantías asegurados por la Constitución, por la otra se erige como garante de la seguridad nacional y el orden público. La conjugación de estos deberes debe efectuarse sin afectar los derechos en su esencia y en

caso de considerar que un derecho prima sobre el otro, deberá ser legítimamente justificado, sin atención a criterios arbitrarios y en cualquier caso por disposición de la voluntad soberana, única facultada para limitar los derechos fundamentales atendiendo a criterios de determinación y especificidad; sólo un adecuado balance entre unos y otros, permite en definitiva, un ejercicio socialmente rentable de ambos.

No basta, sin embargo, un armónico régimen de tratamiento de datos, si los métodos de investigación utilizados para acceder a la información destruyen solapadamente dicha protección. No basta que la actividad estatal pueda tratar datos sensibles sólo en circunstancias calificadas si en esos casos, los métodos utilizados afectan más derechos de los que pretenden proteger. El costo que implica la delación debe estar socialmente justificado. La línea que separa la prevención de un atentado inminente a la seguridad nacional de una simple caza de brujas, es muy fina.

# CAPÍTULO I. DE LA PROTECCIÓN DE DATOS Y LA SEGURIDAD NACIONAL

## 1.1. Nociones históricas del derecho a la intimidad

Durante la edad clásica, no existió consideración especial por la vida privada de las personas: la expresión de la libertad de éstas, sólo se establecía en razón de su participación en la vida pública. La primera aproximación a la intimidad se realiza durante la Edad Media, siendo Santo Tomás uno de los pioneros en esbozar un núcleo íntimo de la persona, la que podría determinarlo, mediante un libre ejercicio de su voluntad.[1] Con el desarrollo de las ciudades mercantiles de Europa, y el nacimiento de una clase burguesa, la intimidad se desarrolla como una expresión más propia del individualismo que comenzaba a configurar este sector de la sociedad.[2]

Con el desarrollo de la filosofía liberal (principalmente pensadores como Hobbes y Locke) se comienza a erigir la esfera privada como una

[1] "la intimidad, [...] es una categoría del orden operativo, concretamente de la personalidad" […] De modo que no se admite que la persona es intimidad, sino que tiene intimidad, pues "sólo en un ser infinito, cuya operación se identifica con su propio ser, [...] su intimidad sería la persona" CRUZ CRUZ, Juan, 1999, El éxtasis de la intimidad. Ontología del amor humano en Tomás de Aquino, citado en SELLÉS, Juan, 2000, Sobre el éxtasis de la intimidad. Anuario Filosófico (33): 907-917, p. 908.

[2] BEJAR, Helena, 1990, El ámbito íntimo, privacidad, individualismo y modernidad, Madrid, España, p. 147 citada en HERNANDEZ, Ana y PALACIOS, Juan, 2008, El dato sensible: su Tratamiento en Chile y en el Derecho Comparado, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, p. 7

extensión de la autonomía y la libertad de las personas, circunscrita ésta a un ámbito distinto e independiente de aquel en que se desarrolla la vida en sociedad. Sin embargo, las grandes revoluciones del siglo XVIII –la norteamericana y la francesa– no establecieron en catálogos separados reivindicaciones respecto de la vida privada y la intimidad.

Tradicionalmente suele establecerse la obra de Samuel Warren y Louis Brandeis como punto de partida de la intimidad como derecho, publicada en la *Harvard Law Review* como "*The Right to Privacy*" de 1890.[3] Frente a la intromisión de la prensa en la vida privada de las personas, Warren y Brandeis configuran el "*right to be left alone"* es decir el derecho a estar solo, un espacio reservado de la intrusión de los medios de comunicación, los que premunidos de la poderosa herramienta gráfica que le otorgaba la naciente técnica fotográfica, transmiten en una simple imagen, más que cualquier combinación de palabras[4]. Ahora, pese a su

[3] HERNANDEZ y PALACIOS, Ob. Cit., p. 10
[4] ANGUITA, Pedro, 2007, La Protección de Datos Personales y el Derecho a la Vida Privada. Régimen Jurídico, Jurisprudencia y Derecho Comparado, Santiago, Editorial Jurídica de Chile, p. 17

utilidad inicial para la doctrina moderna, esta concepción primitiva de intimidad ya ha sido superada.[5]

La recepción en los cuerpos normativos de este derecho se inicia con la Declaración Universal de Derechos Humanos de 1948 en cuanto proscribe las injerencias arbitrarias en la vida privada de las personas[6], lo que establece el punto de partida para su recolección en las legislaciones nacionales. En nuestro país, pese a que desde el Reglamento Constitucional Provisorio de 1812 se recoge en forma limitada la intención de protección de la vida privada[7] (circunscrita al resguardo de una concepción más bien clásica de ésta, vinculada al derecho de propiedad y de la inviolabilidad de la correspondencia), es desde la dictación de la Carta Fundamental de 1980 que ésta se eleva a rango constitucional.[8]

[5] Vid. MURILLO, Pablo y PIÑAR, José, 2009, El Derecho a la Autodeterminación Informativa, Madrid, Editorial Fundación Coloquio Jurídico Europeo, p. 83.

[6] Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. ORGANIZACIÓN DE LAS NACIONES UNIDAS. Asamblea General. 1948, Declaración Universal de los Derechos Humanos. 10 de diciembre de 1948.

[7] ANGUITA, Ob. Cit., p. 109

[8] CHILE. Ministerio Secretaría General de la Presidencia, 2005, Decreto 100, fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. 17 de septiembre de 2005. Art. 19º Nº 4. "La Constitución asegura a todas las personas: … 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia;"

Ahora, la determinación de lo que es íntimo y de lo que no, se ha entendido por la doctrina de diversas maneras. Mientras la disciplina alemana ha optado por una construcción flexible llamada "teoría de las esferas", mediante la cual el ámbito de acción de una persona puede entenderse como circunferencias concéntricas, correspondiendo su núcleo a lo secreto, su periferia a la individualidad y ocupando la intimidad la posición intermedia[9]; otros sectores de la doctrina, entendiendo las diversas dificultades en la apreciación en concreto acerca de qué merece el calificativo de íntimo, y la insuficiencia de la propia teoría de las esferas, han recurrido a criterios auxiliares esbozando al respecto tres concepciones: la geográfica, la subjetiva y la objetiva[10]. Sin embargo, todas estas

[9] CERDA, Alberto, 2003, Autodeterminación Informativa y Leyes sobre Protección de Datos, Revista Chilena de Derecho Informático (3): 47 – 75, p. 49.

[10] Siguiendo a Cerda, para la primera de ellas, debe atenderse únicamente a un criterio geográfico: en efecto, merecen la protección aquellos espacios sobre los cuales la persona tiene un efectivo control, como el hogar, y junto con ello, su correspondencia. Para una visión subjetiva, la calidad de la persona tiene la primacía: distinguir entre privados y funcionarios o personajes públicos, entre otros; los segundos, por la relevancia pública de sus vidas, no pueden verse amparados por la intimidad. Finalmente, la concepción objetiva, se hace cargo del interés público de las conductas puestas en escrutinio, y de los bienes que satisfacen para ser merecedoras de la protección de la ley.
La primera de estas carece de la profundidad suficiente para erigirse como una efectiva barrera de la intromisión pública, siendo catalogada de extremadamente restrictiva y vaciando de valor el concepto de intimidad. La dificultad de la segunda radica en la desigualdad vivida entre unos y otros, contrario a los sentidos de igualdad jurídica, proponiendo una dualidad de estatutos entre unos y otros. La tercera de estas busca indagar en las conductas mismas, buscando criterios

construcciones son insuficientes para fundamentar la protección de los datos personales, pues se basan en una faceta negativa de control de los antecedentes que pueden ser conocidos; sencillamente delimitan el alcance permitido de las intromisiones. En consecuencia, en este punto, el derecho a la intimidad se caracterizaba por constituir un simple derecho de tutela y salvaguarda del individuo frente a intromisiones externas que lo protege en tanto decide aislarse.[11]

1.2. Desafíos del derecho a la intimidad frente a las nuevas tecnologías.

Con el desarrollo de la informática, el procesamiento y la comunicación de datos, existieron (y aún existen) quienes temen que dichos avances puedan acarrear el riesgo de vulneración de derechos fundamentales, al iluminar parcelas anteriormente resguardadas de la intromisión de terceros[12]. Considerando que la protección de datos

como la "trascendencia" para que una actividad originariamente como privada mute en una pública. Ibíd., p.50.

[11] HERRÁN, Ana Isabel, 2002, El derecho a la intimidad en la nueva ley orgánica de protección de datos personales, Madrid, Editorial Dykinson. p. 62.

[12] Vid. CASTILLO, Cinta, 2001, Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información, Derecho y Conocimiento (1): 35-48., p. 38.

personales frente al tratamiento automatizado implica el reconocimiento de un ámbito activo que permita a la persona controlar sus propios antecedentes, tanto en cuanto quién, cómo o por cuánto tiempo realiza esta actividad, la doctrina no ha sido pacífica en la determinación de cuál es el bien jurídico protegido; mientras un sector ha precisado que basta una reformulación del concepto clásico de intimidad, otorgándole una faz positiva de control[13]; el otro, ha resaltado que estamos en presencia de un nuevo derecho, basado en la intimidad, pero autónomo e independiente de éste, denominado "autodeterminación informativa" o "libertad informática".[14]

El reconocimiento de este nuevo derecho como fundamento y origen de la protección de los datos surge de la Sentencia del Tribunal Constitucional Alemán, del 15 de diciembre de 1983, la que señalaba que "la autodeterminación individual presupone –también bajo las condiciones de la moderna tecnología para el procesamiento de información– que a los individuos se les dé libertad para decidir sobre qué actividades emprender y

[13] CERDA, Alberto, 2012, Legislación sobre protección de las personas frente al tratamiento de datos personales, documento inédito, Centro de Estudios en Derecho Informático, Universidad de Chile, p. 7.
[14] Ibíd. p. 8.

cuáles omitir, incluyendo la posibilidad de comportarse efectivamente de conformidad con esa decisión"[15]. Comienza así una nueva visión de la protección de datos personales, ya no centrada en la intimidad o en la vida privada, sino que en el derecho del individuo de determinar libremente cuáles serán los antecedentes que compartirá en la sociedad. En la sentencia en comento, se invalidó la Ley de Censo del año 1982 del país germano, no sólo por la excesiva cantidad de preguntas que ésta contenía (160), sino que, teniendo en cuenta el gran avance de la informática, y el tratamiento automatizado de los datos obtenidos, la relación de muchas de estas preguntas, cada una de ellas de por sí inocuas, pueden arrojar luces sobre un área de la intimidad de las personas, no tenido en cuenta por éstas al momento de entregar los datos primigenios.

Para Herrán, este derecho a la autodeterminación informativa ofrece tutela a las personas respecto a sus datos personales ante una eventual utilización abusiva de los mismos mediante la informática u otro tratamiento automatizado, extendiéndose el ámbito de protección no sólo a

[15] SCHWABE, Jürgen, 2009, Jurisprudencia del Tribunal Constitucional Federal Alemán, Editorial Fundación Konrad Adenauer, México D.F., p. 96.

los denominados datos sensibles, sino también a aquellos que sin pertenecer a la esfera más próxima del individuo son susceptibles de dañar su imagen o el ejercicio de sus derechos.[16]

La determinación final del derecho que fundamenta el sistema de protección de datos no puede dirimirse sin establecer claramente qué en definitiva es lo que entendemos por intimidad. La dialéctica entre las posturas señaladas anteriormente, tanto aquellas que abogan por el derecho a la intimidad como aquellas que erigen a la autodeterminación informativa como una nueva garantía, ha resultado, más allá de una definición clara, en el otorgamiento a la primera de una faz positiva de control de la que hasta el momento carecía. Si restringimos el alcance de esta intimidad a la esfera de lo secreto, lo reservado, lo íntimo; su nueva faceta positiva de control sólo se extendería a dichos ámbitos. No obstante, nuestro sistema de protección de datos intenta, al menos en principio, otorgar a los titulares una facultad de control respecto de toda la información relativa a ellos, en cuanto

[16] HERRÁN, Ob. Cit., p. 59.

personas naturales identificadas o identificables, y no se agota en el ámbito de lo estrictamente íntimo. [17]

Pensamos, en consecuencia, que nuestra normativa de protección de datos germina de la consolidación de la autodeterminación informativa[18] como derecho autónomo e independiente, pues justifica cabalmente el control de las personas respecto de todos los datos relativos a ellas, siendo irrelevante para el efecto, su inocuidad. Lo novedoso de esta estructura es que parte de un supuesto consistente en el desarrollo de la facultad de control de los titulares de los datos. Como señalan Hernández y Palacios, si bien dichas facultades se encuentran contenidas en los derechos de información, modificación, cancelación o bloqueo de la Ley de Protección

[17] Para Jijena, la existencia del Hábeas Data o Derecho de Acceso configuran la consagración del principio de autodeterminación informativa. Vid. JIJENA, Renato, 2001, La Ley Chilena de Protección de Datos Personales, una Visión Crítica desde el punto de vista de los intereses protegidos, Cuadernos de extensión jurídica (5): 85 - 111. p. 89.

[18] No obsta a lo anterior, el hecho que durante la tramitación de la misma, el legislador tuvo en consideración dicha figura, pero decidió descartarla en razón de que "[…] si bien la afirmación de este nuevo derecho ha sido seguida de cerca por los italianos y los españoles -y parte de nuestra doctrina, como los profesores de Derecho Constitucional señores Humberto Nogueira y Francisco Zúñiga-, no es pacífica en la propia Alemania. Parte de la doctrina señala el riesgo de incurrir en una consideración patrimonialista del nuevo derecho en caso de seguirse esta corriente, en razón a que induce a pensar que las personas ostentan un derecho de propiedad sobre sus datos." BIBLIOTECA DEL CONGRESO NACIONAL. 1999. Historia de la ley 19.628 Protección de la vida privada [en línea] < http://goo.gl/7duzyd > [consulta: 15 junio 2013]. p. 264.

de Datos, adoptar como punto de partida la autodeterminación informativa no implica dejar de lado la protección de los datos, sino que enfocarla en la persona en sí misma, como el titular de aquellos.[19] Aún más, el propio Consejo para la Transparencia[20], órgano encargado por ley de velar por el cumplimiento de la norma de protección de datos, establece en sus recomendaciones a los órganos de la Administración del Estado que la finalidad de la Ley 19 628 es asegurar a todas las personas el derecho a la autodeterminación informativa. Por tanto, el camino para su consagración definitiva está suficientemente allanado.[21]

[19] HERNÁNDEZ y PALACIOS, Ob. Cit., p. 57.

[20] "CONSIDERANDO: 1. Que la protección de datos personales, amparada en nuestra legislación en la Ley N° 19.628, tiene por finalidad asegurar a las personas un espacio de control sobre su identidad y de libre manifestación de su personalidad, lo que presupone, en las condiciones modernas de elaboración y gestión de la información, la protección contra la recogida, el almacenamiento, la utilización y la transmisión ilimitados de los datos concernientes a su persona, es decir, el derecho a la autodeterminación informativa". CONSEJO PARA LA TRANSPARENCIA, 2011, Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado, Diario Oficial, Santiago, Chile, 14 de septiembre, C – I, P. 10.

[21] En tanto derecho proyectado, el proyecto de ley que modifica la Ley N°19 628, boletín 8143-03, no contempla en su mensaje original referencia alguna a esta construcción, lo que no obsta a que, durante su tramitación, haya sido el mismo Consejo para la Transparencia, en el primer Informe de la Comisión de Economía, Fomento y Desarrollo a la Cámara de Diputados, el que estimó que "[…] para mejorar el la iniciativa es necesario: 1.- Fortalecer los derechos de los titulares de datos personales, reconociendo la autodeterminación informativa y el principio del consentimiento como elementos rectores de todo tratamiento; 2.- Subir la categoría de la protección de datos a la de un derecho fundamental que asegure a las personas el respeto, el control y la libre manifestación de su personalidad y la autodeterminación informativa; […]" REPÚBLICA DE CHILE. CÁMARA DE DIPUTADOS, 2013, Legislatura 361°. Sesión 75°, en martes 1 de octubre de 2013, [en línea] Valparaíso, Chile, p. 125 < http://www.camara.cl/pdf.aspx?prmID=10234%20&prmTIPO=TEXTOSESION> [consulta: 19 de diciembre de 2013].

## 1.3. Protección de los datos sensibles.

No obstante, toda resolución anterior sobre el derecho que fundamenta esencialmente la normativa de protección de datos en general, merece una revisión desde cero al momento de enfrentar el análisis del tratamiento de los datos sensibles. Veremos que este tipo de información predica una protección reforzada, y así lo ha manifestado la doctrina moderna y el a su vez naciente desarrollo legislativo comparado, por lo que no puede entenderse como una simple parte integrante de un sistema genérico de tutela. Mientras la autodeterminación informativa gana enteros asegurando una protección amplia de todo tipo de información personal, pierde la especificidad y atención que el dato sensible requiere. A su vez, no presenta una consagración expresa como derecho fundamental, como sí

ocurre en otros países[22], por lo que su reconocimiento como tal siempre encontrará detractores.[23]

Así, un sistema de protección de datos coherente con un refuerzo de la tutela de los datos sensibles necesita un fundamento fuerte que permita justificar esta situación, fundamento que no puede encontrarse en la autodeterminación informativa, pues al no constituir el desarrollo de un derecho fundamental[24], la limitación legal del tratamiento de estos datos pierde fuerza, ya que puede ser circunvalada a través de normas permisivas de mayor valor jerárquico o incluso por vías interpretativas.

[22] Es el caso, por ejemplo, de España, que reconoce en el artículo 18.4 de su Constitución la limitación al uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, y en su artículo 10 el derecho a la dignidad de las personas. De ambos preceptos deriva este derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. En desarrollo de esta garantía se aprobó la LOPD del año 1999.

[23] No obstante, para Nogueira, la ausencia de reconocimiento expreso constitucional no es óbice para afirmar que un derecho no goza del carácter de fundamental, puesto que de acuerdo a la concepción de los derechos implícitos, los derechos esenciales "pueden deducirse de valores, principios, fines y razones históricas que alimentan el derecho positivo constitucional e internacional. NOGUEIRA, Humberto, 2005, Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales [en línea] Revista Ius et Praxis, Vol. 11(2) < http://www.scielo.cl/scielo.php?pid=S0718-00122005000200002&script=sci_arttext> [fecha de consulta: 10 de diciembre 2013].

[24] Vid. HERNANDEZ y PALACIOS, ob. cit., p. 69. Esta situación, sin embargo, está resuelta en otras legislaciones, como la española o la uruguaya, que expresamente otorgan a la autodeterminación informativa, el carácter de derecho fundamental. Vid. ESPAÑA, 1978, Constitución española. Artículo 18.4. y URUGUAY, 1967, Constitución de la República. Artículo 72

Vimos que el derecho a la intimidad terminó reforzado con los años adquiriendo una faceta positiva de control anteriormente ignorada y es esta nueva concepción de intimidad la que aludimos ahora como fundamento de la protección específica de los datos sensibles, pues tiene éxito donde la autodeterminación informativa falla.

En primer lugar, el dato sensible se vincula directamente a aquella información íntima o privada de las personas, por tanto es una manifestación propia del derecho a la intimidad, en tanto adquieren materialidad como antecedentes procesables, aspectos propios de la personalidad o característicos de un estilo de vida, que por definición las personas pretenden mantener alejados del conocimiento público; hay por tanto una primera identificación a nivel conceptual[25]. En segundo lugar, si

[25] Existen, sin embargo, autores que cuestionan esta identificación conceptual aludiendo al hecho que los datos íntimos no serán siempre, a su vez, datos sensibles, pues la intimidad es una noción subjetiva y por tanto, no puede determinarse objetiva y genéricamente a través de la legislación. Vid. HERRÁN, Ob. Cit., p. 53. No obstante, nuestro concepto de dato sensible, como veremos, es una simple mención enunciativa que no pretende abarcar todas las hipótesis, pues en definitiva la sensibilidad del dato radicará en su relación a aspectos de la intimidad como potenciales generadores de discriminaciones arbitrarias en su titular. Herrán sustenta esta opinión aludiendo al caso en que muchas veces, el origen racial o ciertas enfermedades de señas visibles, serán circunstancias evidentes que traspasarían el ámbito de lo íntimo pues estaría en constante comunicación al público, pero que no pierden la característica de sensible. Pensamos, no obstante, que dicha argumentación sujeta la determinación de la intimidad a un control que

el carácter de derecho fundamental de la autodeterminación informativa es discutido; dichas dudas se disipan al remitirnos al derecho a la intimidad o vida privada de las personas, derecho de consagración específica y literal en nuestra Carta Fundamental. Finalmente y consecuencia de lo anterior, esta idea culmina la envoltura protectora de los antecedentes íntimos, pues al remitir la protección del dato sensible a la manifestación de un derecho fundamental, sólo la ley puede legítimamente desarrollarlo, por lo que cualquier excepción al control del titular deberá encontrar un sustento legislativo expreso, no pudiendo encontrarse una autorización de estas características por vías interpretativas.

### 1.4. Seguridad Nacional y Orden Público.

La seguridad nacional es un bien jurídico vinculado íntimamente a la defensa nacional[26], se erige como una condición, esencialmente dinámica, cuya determinación dependerá de una ecuación que conjugue los objetivos del Estado y los intereses nacionales con los riesgos, amenazas y obstáculos

---

escapa al ámbito del sujeto, pues simplemente no puede evitar esta situación. Pero, en una sociedad donde la personalidad del sujeto también se manifiesta virtualmente, dichas características no pierden el carácter de íntimas, sólo porque no puedan ocultarse del escrutinio público.

[26] CHILE. Constitución Política. Ob. Cit., art. 101

que eventualmente puedan afectarlos en un momento determinado.[27] Comprende, en aras de asegurarla, un cúmulo de acciones destinadas a preservar la seguridad tanto interna como externa del Estado, que se originan en una de política de defensa que engloba una serie de recursos, partiendo de la más esencial estructura orgánica, que permita, junto a un respaldo financiero y legislativo, su desarrollo coherente.[28] Una adecuada política de defensa nacional permite cautelar la seguridad externa del Estado, y un Estado libre de intervenciones foráneas y prevenido ante cualquier tipo de amenaza extraterritorial puede, en propiedad, permitirse asegurar y resguardar la faz interna del concepto de seguridad.

Es en este sentido que la seguridad nacional entronca con el concepto de orden público, bien jurídico de expresión difusa que, sin embargo, en todas sus formulaciones ronda las ideas de tranquilidad, seguridad, salud y moralidad públicas. Como tal, permite la combinación armónica de las instituciones del Estado, la legislación vigente, el respeto cabal a las normas morales, sociales y económicas y principalmente a los derechos y garantías

[27] MINISTERIO DE DEFENSA DE CHILE. 2010. Libro de la Defensa Nacional. p. 108. [ en línea ] <http://www.defensa.cl/> [ fecha de consulta 25 de septiembre de 2013]
[28] Ibíd., p. 109.

fundamentales, todo esto en aras de promover el bien común de la sociedad.[29]

El Estado, como garante y protector por mandato constitucional de la seguridad nacional y el orden público[30] [31], tiene a su haber una serie de recursos disponibles para esta tarea, desde el ejercicio de la diplomacia y la política exterior combinadas con la función de defensa -esta última desplegada en forma operativa por las Fuerzas Armadas- que garantizan conjuntamente la seguridad externa; hasta la administración de justicia y la acción de las Fuerzas de Orden y Seguridad, vinculadas directamente al resguardo de la seguridad interna. Para este fin, y buscando asegurar el tránsito de nuestro país hacia el desarrollo, se requiere de parte de sus organismos la capacidad de prever y analizar escenarios futuros, para determinar el mejor curso de acción por parte de las autoridades, que se traducirá en políticas públicas tendientes a asegurar los intereses y la seguridad ya referida. En aquellas situaciones, el proceso de toma de decisiones debe enmarcarse en un contexto de análisis adecuado de la

[29] PFEFFER URQUIAGA, Emilio, 1993, Constitución Política de la República de Chile, 1980. Repertorio de legislación y jurisprudencia chilenas., Editorial Jurídica de Chile. pp. 129-130.
[30] Constitución Política, Ob. Cit., art. 1° inc. 4° y 5°
[31] Ibíd., Art. 5°.

información obtenida. Es este proceso el que, tradicionalmente, se conoce como inteligencia.

Siguiendo en esta materia a Vera[32], coincidimos en que la inteligencia no se agota en la acepción gramatical[33]; en efecto, dentro de las múltiples facetas que integra el concepto en estudio podemos encontrarnos con la inteligencia como conocimiento, como organización y finalmente como actividad. Dentro del primer concepto, podemos caracterizarla como información obtenida por los más diversos mecanismos, la que es procesada mediante un método racional, utilizando en este caso la definición gramatical de inteligencia en línea con lo establecido en el artículo 2° letra a) de la ley 19 974 que dispone que la inteligencia es "el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones". [34] Para el segundo concepto, es decir, inteligencia como organización, se refiere a

[32] VERA LAMA, Rodrigo, 2008, Sistema de Inteligencia del Estado a la luz del Derecho, Santiago, Librotecnia, p. 15.
[33] "Inteligencia", entre otras acepciones, significa "Conocimiento, comprensión, acto de entender". REAL ACADEMIA ESPAÑOLA, Diccionario de la lengua española, vigésimo segunda edición, 2001 [en línea], <http://lema.rae.es/drae/?val=inteligencia> [Fecha de consulta: 28 de agosto de 2013].
[34] CHILE, Ministerio del Interior, 2004. Ley 19 974: Sobre el sistema de inteligencia del estado y crea la Agencia Nacional de Inteligencia, octubre 2004.

las entidades que realizan el proceso de recolección y análisis de la información, a sus normas orgánicas, y a sus materias de seguridad y confidencialidad, características comunes a todas ellas[35]. Finalmente, respecto de su consideración como actividad, dicha función discurre acerca de la manera en que se obtiene el conocimiento útil, tanto mediante actividades de inteligencia propiamente tal como de contrainteligencia[36].

Es posible que no toda la información obtenida sea necesaria o relevante para los objetivos previamente fijados, por lo que, como se argumentará más adelante, se hace imprescindible precisar la forma de tratamiento y destino de la misma, por las potenciales consecuencias gravosas que su abuso podría acarrear a los individuos sometidos a análisis.

Por tanto, el Estado de Chile puede utilizar como recurso la inteligencia, construyéndose en torno a esta técnica una institucionalidad

[35] Es en este sentido sobre el cual se expresa la RAE, al hablar de "Servicio de Inteligencia": "Organización secreta de un Estado para dirigir y organizar el espionaje y el contraespionaje" Real ACADEMIA ESPAÑOLA, ob. Cit. [en línea] <http://lema.rae.es/drae/?val=servicio+de+inteligencia> [fecha de consulta: 15 de agosto de 2013]. Sin embargo, como hemos visto, los servicios de inteligencia van más allá del espionaje.

[36]Dentro de la primera, denominada inteligencia propiamente tal, se encuentra la búsqueda de información útil, para ser considerado por las autoridades correspondientes. En las segunda, se busca la neutralización de las agencias de inteligencia adversarias. VERA, Ob. cit., pp. 23 y 24.

jurídica que pretende regular a todos los organismos y servicios estatales que realicen esta actividad, estableciéndose de esta forma un Sistema de Inteligencia del Estado cuya norma madre es la Ley 19 974 promulgada el año 2004. Al amparo de este sistema, se busca que todo ente público de inteligencia se encuentre circunscrito a un ámbito específico de acción, basado en objetivos previamente delineados, y expresamente coordinados en lo referente al flujo recíproco de información.

Se pueden distinguir tres tipos de inteligencia en el sistema nacional: la que realiza la Agencia Nacional de Inteligencia, cuyo objetivo principalmente es asesorar la toma de decisiones del poder ejecutivo;[37] la inteligencia militar, que opera expresamente en el ámbito de la defensa nacional[38]; y la inteligencia policial, en la protección del orden público y la seguridad pública interior.[39]

Cuando las amenazas al orden público se transformen en ilícitos, la acción del Estado mutará a su faceta persecutoria, utilizando los

[37] Ley 19 974. Art. 7°.
[38] Ibíd. Art. 20°.
[39] Ibíd. Art. 22°.

procedimientos establecidos para la investigación y eventual sanción de éstos acorde al ordenamiento jurídico penal existente. En esta etapa, dicha labor se encuentra radicada en el Ministerio Público y las Fuerzas de Orden y Seguridad.

Tanto la inteligencia como la investigación en el proceso penal son efectuadas por organismos públicos, por lo que deben en su actuar respetar la Constitución, actuar dentro de su competencia y en la forma que prescriba la ley.[40] Por lo tanto, reviste especial importancia la sujeción de dichos órganos a la legislación nacional, en tanto ésta cautela y garantiza aspectos tan relevantes como la protección de los datos.

[40] Constitución Política, Ob. Cit. arts. 6° y 7°.

# CAPÍTULO II. DEL TRATAMIENTO DE DATOS PERSONALES POR ORGANISMOS PÚBLICOS

2.1. Principios y derechos aplicables a la actividad de tratamiento de datos personales por los órganos públicos.

Los principios que informan la actividad de tratamiento de datos personales no se limitan exclusivamente a los contenidos en la ley, sino que se nutren además de las directrices contenidas en los documentos internacionales sobre la materia ratificadas por Chile, así como de la Declaración Universal de Derechos Humanos. Sobre el particular, estableceremos los siguientes.

2.1.1. Resolución 45/95 de la Asamblea General de las Naciones Unidas. Directrices para la regulación de archivos de datos personales informatizados.[41]

Aprobada mediante resolución de fecha 14 de diciembre de 1990, la resolución 45/95 ha implementado un decálogo de orientaciones destinadas a las normativas de los países miembros. Estos principios tienen su correlativo en muchos de los derechos establecidos en la LPDP, y su

[41]ORGANIZACIÓN DE LAS NACIONES UNIDAS, Asamblea General, 1990, resolución 45/95, Directrices para la regulación de los archivos de datos personales informatizados, 14 de diciembre de 1990.

existencia fue tenida en cuenta por los parlamentarios en el íter legislativo[42]. Esto es así con los principios de legalidad, de exactitud, de finalidad y de acceso, los que veremos a continuación.

Para los efectos de esta investigación, conviene detenerse en las directrices contenidas en los números 5 y 6; en la primera de ellas se estableció el principio de no discriminación, el cual instituye la excepción de la recogida de aquellos datos que puedan dar origen a una discriminación ilegal o arbitraria, como el origen racial o étnico, vida sexual, creencias religiosas o filosóficas, etc., los que configuran el embrión del desarrollo del llamado dato sensible.

Del mismo modo, en su numeral 6 se establece la facultad para hacer excepciones, mediante la cual los estados miembros podrán establecer reservas a los principios mencionados, cuando éstos se basen en la protección de la seguridad nacional y el orden y salud pública, siempre que se expresen de manera específica en la ley, y se prevean los resguardos

[42] BIBLIOTECA DEL CONGRESO NACIONAL, 1999, ob. cit., p. 115.

apropiados. Dicho principio incluso opera sobre aquellos datos sujetos a la protección especial del número 5 ya señalados, pero con el resguardo adicional de requerir que éstos se autoricen respetando los límites legales nacionales e internaciones respecto al amparo de los Derechos Humanos y la prevención de la discriminación.

### 2.1.2. Directrices de la OCDE sobre protección de la privacidad.[43]

Asimismo, la Organización de Cooperación y Desarrollo Económicos (OCDE), de la que Chile es parte integrante desde el 07 de mayo de 2010, establece algunos de estos principios en sus Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, siendo enfática en señalar que éstos son simplemente "estándares mínimos que se puedan [en] complementar con otras medidas de protección de la privacidad y de las libertades individuales"[44] y que cualquier excepción, como las

[43] ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS (OCDE). 1980, Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. 23de septiembre de 1980.
[44] Ibíd. Parte Primera. Nº 6.

relacionadas con la soberanía y seguridad nacionales y el orden público, deberían ser las menos posibles y siempre de conocimiento público.[45]

### 2.1.3. Principios y derechos contemplados en la Ley N° 19 628.

Iniciada mediante moción parlamentaria en enero de 1993, la Ley N° 19 628 sobre Protección a la Vida Privada y Tratamiento de Datos Personales (en adelante LPDP) se dictó con fecha 28 de agosto de 1999. Durante estos seis años mutó desde una ley de protección a la vida privada hasta el ambiente específico y acotado de la protección de datos personales, con un tinte y énfasis marcado por aquellos de origen comercial. [46]

Esta ley protege a los titulares de datos respecto del tratamiento que manual o automatizadamente realicen frente a ellos entes públicos o privados, como asimismo ordena y reconoce los principios y derechos a los cuales debe ajustarse esta actividad. A continuación, revisaremos

[45] Ibíd. Parte Primera. Nº 4.
[46] ANGUITA, ob. cit. p. 233 y ss.

someramente el contenido de las principales directrices que informan la normativa nacional de protección de datos personales.

2.1.3.1. Licitud en el tratamiento de datos.

Con respecto a esta categoría, la propia LPDP establece que cualquier persona puede efectuar el tratamiento de datos personales, siempre que dichas operaciones se realicen dentro del marco establecido en la propia ley; para los órganos públicos esta situación se satisface siempre que cumpliendo los postulados establecidos actúen asimismo dentro de su competencia.

2.1.3.2. Información y consentimiento del titular.

Para realizar legítimamente el tratamiento de datos personales, la persona sobre la cual recaerá esta actividad, debe ser debidamente informada del propósito y destino del almacenamiento de datos, así como

de su eventual comunicación al público, y el titular debe prestar su consentimiento previo, el cual debe constar expresamente y por escrito[47].

Sin embargo, estos derechos no podrán ser ejercidos cuando, entre otras causales, su ejercicio afecte la seguridad de la Nación o el interés nacional.[48] Sobre este punto, Jervis nos señala que al tratarse de un concepto indeterminado, su conceptualización deberá entregarse al juez que conoce del requerimiento del titular de los datos en cuestión.[49] Asimismo, siguiendo la doctrina nacional, puede establecerse como lugar común que el concepto de "seguridad de la Nación" es un bien público, que implica que su uso no es exclusivo, y que no puede ser fraccionado entre sus múltiples usuarios. Como garantía institucional, dicha noción merece una protección

[47] ANGUITA, Ob. Cit., p. 299.
[48] CHILE, Ministerio Secretaría General de la Presidencia, Ley 19 628, Sobre Protección de la Vida Privada, agosto de 1999. Art. 15º. "No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva."
[49] JERVIS, Paula, 2003, Derechos del titular de datos y hábeas data en la ley 19 628. Revista de Derecho Informático (2), p.26

desde el punto de vista constitucional[50], y su ponderación frente a otros derechos que puedan pugnar, debe siempre considerarse caso a caso, utilizando, a este respecto, un examen de daño que pueda en primer lugar establecer la identidad del supuesto perjuicio, luego que éste pueda ser determinado en el tiempo inmediato, y finalmente en cuanto a la probabilidad que el daño a este concepto sea real, ponderarlo con los derechos establecidos en la LPDP.

2.1.3.3. Calidad y finalidad de los datos.

Frente a este principio corresponde precisar, por una parte, que los datos recogidos deben ajustarse fielmente a la realidad, es decir, deben ser veraces, completos, exactos y actualizados, y por otra, que éstos sólo pueden ser utilizados con la exclusiva finalidad para la cual fueron recogidos, sin ser excesivos respecto del ámbito para el cual fueron acumulados.[51] Complementando esta idea, Cerda[52] preceptúa que la manifestación del principio de finalidad se traduce en el derecho de

[50] CONTRERAS, Pablo, 2009, Ponderación entre el derecho de acceso a la información pública y el resguardo de la seguridad de la nación, en: Transparencia en la Administración Pública, Santiago, Abeledo Perrot, p. 282.
[51] CERDA, 2012, ob. cit., p. 24.
[52] Ibíd., p. 24.

cancelación o eliminación, que asiste al titular de los datos personales una vez cumplidas las condiciones que justificaron la recogida y trata de los mismos, los que la propia ley entonces denomina como caducos.

2.1.3.4. Seguridad y secreto de los datos.

Para Cerda[53], la LPDP establece una norma genérica relativa a la adopción de medidas de seguridad de parte del encargado del banco de datos respecto de la infraestructura del mismo, de los procesos asociados a ella, y desde el ámbito jurídico. Esta responsabilidad implica un deber de cuidado que cumpla al menos con una debida diligencia, la que debe ser evaluada de manera posterior por los Tribunales de Justicia.[54]

Con respecto al deber de secreto, regulado en el artículo 7° de la LPDP[55], esta obligación recae tanto sobre el responsable del banco de datos,

[53] CERDA, 2012, Ob. Cit., p. 26.
[54] Artículo 11.- 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. CHILE. Ley 19 628, Ob. Cit.
[55] CHILE. Ley 19 628, ob. cit., art. 7°: "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 así sobre los que participan en el proceso de recolección de éstos. Dicho deber se extiende en el tiempo, aún después de cesado en sus funciones.

### 2.1.4. Derechos conferidos a los titulares de datos en la LPDP.

#### 2.1.4.1. Derecho a la información y acceso

Si bien no se estableció de manera expresa, como sí lo hacen otras legislaciones comparadas[56], la posibilidad de otorgar al titular de los datos, previa a la recogida de éstos, los detalles acerca de dicho tratamiento, de acuerdo a lo establecido en los artículos 12° a 15° de la LPDP, el titular de los datos tiene, no obstante, derecho a:

a. Conocer información sobre los datos relativos a su persona;
b. Conocer cuál es el propósito del almacenamiento;
c. Conocer cuál es su procedencia y cuál será el destinatario y;

---

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".

[56] En España, la Ley Orgánica 15/1999 le concede el derecho al titular de los datos que en el inmediato futuro se tratarán, de exigir: a) la existencia del fichero al que serán incorporados los datos; b) carácter voluntario u obligatorio de su respuesta a las preguntas que le planteen ; c) las consecuencias de proporcionar los datos o de su negativa y d) posibilidad de ejercer los derechos establecidos en la ley. ANGUITA, Ob. Cit., p. 306.

d. Conocer la individualización de las personas u organismos a los cuales serán transmitidos sus datos.

De acuerdo al artículo 15° de la LPDP, sin embargo, estos derechos no podrán ser ejercidos cuando, entre otras causales, su ejercicio afecte la seguridad de la Nación o el interés nacional.

2.1.4.2. Derecho de rectificación, cancelación o bloqueo.

La doctrina nacional es clara en señalar que, como una consecuencia del principio de calidad de los datos, deben corregirse, a costa del encargado de la base, toda aquella información que sea inexacta, equívoca, incompleta o desactualizada. Sin embargo, y como excepción, nuevamente se les aplica lo establecido en el artículo 15° de la LPDP, con respecto a la seguridad de la nación o el interés nacional.

Para los efectos de la cancelación, el titular puede solicitar, en cualquier momento, la revocación de la autorización para el tratamiento de

los datos personales, los cuales deberán ser destruidos o eliminados. Misma situación ocurrirá cuando cese la justificación que validó originariamente el tratamiento de los mismos. Para los efectos del tratamiento por parte de los órganos públicos, esta norma coloca un escenario en el cual deben ser eliminados aquellos datos para los cuales no se posee un fundamento legal. [57]

Asimismo, la LPDP, en su artículo 2° letra b) define al derecho al bloqueo como "la suspensión temporal de cualquier operación de tratamiento de datos almacenados". Este se presenta en tres situaciones: en la primera, cuando el titular ha proporcionado en forma voluntaria sus datos personales; en la segunda, cuando se usen los datos del titular para las comunicaciones comerciales y ya no se desee continuar en el respectivo registro, y en tercer lugar, se bloquearán, aun sin requerimiento de su titular, aquellos datos respecto de los cuales no pueda ser establecida su exactitud o cuya vigencia sea dudosa[58]. Para el ejercicio de este derecho no se exige ningún desembolso económico por parte del titular. Del mismo modo que

[57] "tratándose de datos recogidos por una institución cuya finalidad es muy específica y ellos no guardan relación con ella." CERDA, 2012, ob. cit., p. 29.
[58] ANGUITA, ob. cit., p. 310.

con los demás derechos conferidos en la ley, el artículo 15° establece las causales mediante las cuales puede denegarse su ejercicio por parte de sus titulares.

### 2.2. Análisis del artículo 20° de la LPDP

La legislación general en materia de tratamiento de datos personales sujeta a los órganos públicos que realizan esta función a un específico catálogo de normas. Establecido en el Título IV de la LPDP, el estatuto jurídico del tratamiento de los datos personales por organismos públicos[59] tiene como norma fundamental su artículo 20°. Esta disposición se erige como excepción al consentimiento del titular de los datos, siempre que el tratamiento de éstos, sea efectuado por el órgano público en materias de su competencia y en consonancia con las restantes disposiciones de la ley. Por tanto, siempre que concurran ambos requisitos, y sólo en esos casos, el

[59] Paula Jervis utiliza a su vez, en su clasificación de los datos personales a la luz de la ley 19.628, la expresión "datos públicos". JERVIS, Paula, 2005. Categorías de datos reconocidas en la ley 19.628. Revista de Derecho Informático (6), p. 140.

tratamiento de los datos, sin consentimiento de su titular, será una actividad legal.[60]

2.2.1. Primer requisito: sujeción a las normas de la LPDP.

El organismo público deberá en toda actividad de tratamiento que efectúe, ceñirse a las disposiciones de la LPDP. En los hechos, la sujeción implica, aparte de la observancia de la letra de la ley, el reconocimiento de todos los principios establecidos en la misma para ello, y conjuntamente, la declaración de derechos que asisten al titular de dichos antecedentes.

Esta sujeción parte desde un extremo elemental, pues la misma norma se encarga de conceptualizar muchos de los fundamentos que se encuentran recogidos por ella y define las expresiones básicas limitando la labor del intérprete y otorgándole mayor claridad. De esta forma, el organismo público, estará tratando datos no sólo al efectuar un procesamiento genérico de la información sino además cuando realice "cualquier operación o complejo de operaciones o procedimientos técnicos,

[60] Jervis aborda el tratamiento de datos personales por organismos públicos cuando actúan fuera de su competencia. En este caso, señala que dicha actividad es legal siempre que actúe con el consentimiento del titular de los datos. JERVIS, Ibíd., p. 142.

de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma."[61]

Definida la extensión conceptual de la actividad de tratamiento, se hace imprescindible ahondar en la naturaleza del dato objeto de dicho proceso. Toda la institucionalidad de protección de la LPDP se constituye sobre el concepto de dato personal, el que para la letra f) del artículo 2° es el relativo a "cualquier información concerniente a personas naturales, identificadas o identificables".[62] El dato personal comprende además otras categorías, las que se configuran en una relación de género a especie. Éstas, se distinguen unas de otras, entre otros aspectos, en atención a la mayor o menor exigencia del consentimiento de su titular como elemento legitimador de su tratamiento; es en este sentido en que Jervis[63] esboza una clasificación de los tipos de datos personales, distinguiendo a este respecto los datos provenientes de fuentes accesibles al público (inciso quinto del

[61] Ley 19 628, ob. cit., art. 2° letra o).
[62] Ibíd., art. 2° letra f).
[63] JERVIS, Ob. Cit., pp. 118-145.

artículo 4°); los tratados por personas jurídicas privadas (inciso final del artículo 4°); los relativos a obligaciones de carácter económico, financiero, bancario o comercial (Título III de la LPDP); los datos personales sensibles (artículo 10°); los datos personales sensibles de salud (artículo 10°); los datos médicos (artículo 127° del Código Sanitario); los datos públicos (artículo 20°); datos penales (artículo 21°); y, finalmente una categoría residual correspondiente a los datos personales en general (inciso primero del artículo 4°). Nuestra aproximación simplemente distinguirá entre los datos personales sensibles y aquellos que no lo son y cómo se enfrenta el organismo público a esta dicotomía.

2.2.1.1. Datos personales sensibles.

Dentro de los datos personales, la LPDP contempla una categoría especial, los llamados "datos sensibles"[64], éstos son definidos en la letra g)

[64] La primera mención a este presupuesto de acción no nació en la moción original del proyecto, presentada por el senador Cantuarias el 5 de enero de 1993, puesto que en dicho documento ni siquiera se mencionaba la categoría de dato sensible como categoría independiente. Esta categoría recién se agregó al proyecto durante el primer trámite constitucional en la cámara de origen, pero, tal como señalan Hernández y Palacios, ya desde mayo de 1996, mediante un informe de la Comisión de Constitución, Legislación y Justicia se explicaba que datos sensibles "se refieren a las características morales o físicas de las personas que, en principio, no son de interés para los demás y no afectan en general a la sociedad (...) los datos relativos al origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones; también los relativos a la salud y a la vida sexual y los referentes a condenas criminales, cuyo conocimiento

de su artículo 2° como “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.” Se sigue en esto a la legislación comparada y a instrumentos internacionales sobre la materia, en particular a la Directiva 95/46/CE, que tiene en mente, precisamente, evitar que el tratamiento de dichos datos pueda acarrear una discriminación arbitraria en contra de su titular. [65]

El legislador, en su enumeración enunciativa[66], es claro en señalar que se trata de antecedentes que afectan la esfera más íntima, cercana y próxima[67] de su titular; así existe una identificación directa entre el dato sensible y el dato íntimo, pues dicha enumeración sólo pretende

---

queda particularmente restringido, aunque puedan interesar a la sociedad en su conjunto”. Salvo la mención de los datos penales, que fueron objeto de un tratamiento particular, el concepto mismo del dato sensible no sufrió mayores modificaciones.

[65] UNIÓN EUROPEA. Parlamento Europeo. 1995. Directiva 95/46/CE. 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. Octubre 1995.

[66] Sobre este punto, la doctrina se muestra uniforme en señalar dicho carácter: en efecto, es delator el vocablo “tales como” para indicar que dicha enumeración no es exhaustiva. Serán los tribunales los llamados a completar y delimitar la extensión de dicho concepto. Vid. HERNÁNDEZ, y PALACIOS, ob. cit., p. 183.

[67] Ibíd. p. 184.

ejemplificar y de paso objetivizar ciertos datos que dadas las particularidades culturales de nuestra sociedad pueden ser considerados hoy, como eventuales generadores de discriminaciones arbitrarias en contra de su titular, estableciéndose una presunción de que dicha información comparte el carácter de dato sensible, pero que no se agota en ella misma. Es por esta razón que, como veremos, la ley establece una serie de requisitos especiales para su correcto tratamiento, cuyo elemento fundamental es la inversión de la regla de libertad de tratamiento de datos personales dispuesta en el artículo 1° de la LPDP. Pese a estas intenciones, la doctrina nacional estima que el tratamiento de datos sensibles no se encuentra mayormente protegido con respecto a la categoría general de datos personales; en efecto, sólo basta que una ley lo autorice, o el consentimiento de su titular para proceder a su tratamiento, o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, sin establecer categorías especiales ni resguardos particulares a ello.[68]

[68]"En rigor, de acuerdo a las normas de la ley N°19628, los datos sensibles en nuestro país -a diferencia de lo que dispone el derecho comparado-, no se encuentran especialmente protegidos, dado que con la excepción de los datos relativos a la salud, no se requiere para su tratamiento el consentimiento expreso y por escrito de sus titulares, sino sólo la exigencia común de recabar el consentimiento del interesado" ANGUITA, Ob. Cit., p. 300. En el mismo sentido, cf. CERDA, Alberto, 2012, Ob. Cit. p. 25 y HERNANDES y PALACIOS, ob. cit., p. 190

2.2.1.1.1. El consentimiento del titular de datos sensibles

Los datos personales sensibles pueden ser legítimamente tratados mediante la autorización de su titular. Si bien la ley no lo menciona expresamente, creemos, en virtud de la regla general del consentimiento establecido para los datos personales comunes, que dicha autorización debe ser expresa y que debe constar por escrito.[69] Así fluye, expresamente, de lo señalado durante su tramitación, y sobre la base de los criterios informadores del proyecto, discutidos en sala durante el primer trámite constitucional.[70]

2.2.1.1.2. Autorización legal de tratamiento de datos sensibles.

Si bien en principio, se reconoce a los titulares la facultad de decidir qué datos quieren proporcionar a un tercero y con qué finalidad y a su vez, el poder de oponerse legítimamente a dicha apropiación o utilización; "esta regla no es absoluta y puede ser exceptuada siempre que una norma con rango de ley así lo contemple por considerar que prevalece el interés

[69] Vid. CERDA, 2012, ob. cit., p 26, para una crítica a la nula diferenciación de este consentimiento con respecto de las categorías generales de datos personales.
[70] BIBLIOTECA DEL CONGRESO NACIONAL. 1999. ob. cit. p. 254.

general"[71]. Es lo que se denomina la facultad de establecer excepciones, la que es reconocida en cuerpos normativos tanto nacionales como internacionales,[72] y que opera con requisitos especialmente estrictos tratándose de datos sensibles.[73] Se reconoce en consecuencia que la prohibición de tratamiento por parte de terceros –privados u órganos públicos- de los datos sensibles no es en ningún caso absoluta, pues existen mecanismos que permiten establecer excepciones en resguardo de intereses generales de mayor valor. Estas excepciones, deben cumplir con estrictos requisitos, respetando en primer lugar los derechos fundamentales reconocidos en la Constitución y operar exclusivamente en virtud de una ley. Como dice de la Serna Bilbao "corresponde a los representantes de la soberanía popular permitir excepcionar el control del titular del dato y

[71] DE LA SERNA BILBAO, María Nieves. 2011. La institucionalización de la protección de datos de carácter personal. en: ARRIETA, Raúl (Coordinador). Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. p.68.

[72] Esta facultad tiene su consagración definitiva en la resolución 45/95 de 1990 de la Asamblea General de las Naciones Unidas que establece entre sus principios rectores para la reglamentación de los ficheros computarizados de datos personales, la facultad de establecer excepciones siempre que éstas sean "...necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás...", siempre que hayan sido previstas expresamente en una ley, adoptada de conformidad con el sistema jurídico nacional. ORGANIZACIÓN DE LAS NACIONES UNIDAS, resolución 45/95, Ob. Cit., principio A.6.

[73] Así lo sugiere la propia resolución 45/95 al disponer que "las excepciones al principio 5, relativo a la prohibición de discriminación, [origen de los datos sensibles] deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los principios 1 a 4 y sólo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos humanos y de lucha contra la discriminación." Ibíd.

sustituir su consentimiento."[74] El fundamento de esta prohibición de tratamiento se remonta a dos antecedentes: por una parte, el catálogo de los derechos fundamentales establecidos en la Constitución y en los tratados internacionales ratificados por Chile y por la otra, complementariamente, el desarrollo legislativo plasmado en la LPDP.

En el primer punto y como tratamos en el capítulo I, el fundamento de la protección de los datos sensibles se encuentra en el derecho a la intimidad (en su reformulación doctrinaria con faceta positiva de control). Considerando entonces a la intimidad como un derecho fundamental explícitamente reconocido en la Constitución, corresponde determinar si la exigencia de autorización legal para el tratamiento de estos datos cumple con los requisitos mínimos que la restricción de un derecho precisa. Hablamos de restricción, porque la sustracción especial de los datos sensibles del ámbito de control de las personas, es justamente una limitación directa al contenido del derecho[75], y como tal, entendiendo, por

[74] DE LA SERNA Bilbao. ob. cit. p.68.
[75] Nogueira establece que "La limitación en cuanto restricción del derecho es un acto que procede desde fuera e implica alterar la condición natural del derecho. La limitación exterior al

cierto, que los derechos fundamentales no son ilimitados[76], debe cumplir con ciertas exigencias para que esa restricción sea legítima. Nogueira señala que "la limitación de los derechos en nuestro ordenamiento jurídico sólo puede concretarse por el órgano o la autoridad dotada de competencia por la Constitución con ese fin, de acuerdo al procedimiento y las formalidades establecidas para ello, de acuerdo a lo que establece nuestro artículo 7° de la Carta Fundamental, en su inciso 1° y 2°". En consecuencia, agrega, "solo la Constitución y la ley pueden ser consideradas fuentes de limitación de los derechos fundamentales, ya que su carácter de derechos fundamentales deriva de su aseguramiento constitucional expreso o implícito, como asimismo, por el hecho de que su regulación está reservada exclusivamente al legislador (Artículos 19° N°26, 32 Nº 3 y 6; 63 y 64 de la Constitución). Ninguna norma constitucional habilita a ningún otro órgano o autoridad para introducir válidamente limitaciones-restricciones de los derechos fundamentales." Ahora, la limitación legal de un derecho fundamental sólo

derecho se refiere a un límite constitutivo del derecho y no al carácter declarativo del límite ya preexistente" NOGUEIRA, 2005, Ob. Cit.

[76] En este sentido, Tórtora señala que "los derechos fundamentales no son absolutos ni ilimitados, sino que en verdad se encuentran sometidos a una serie de restricciones o limitaciones que provocan que su titular no pueda ejercer válidamente una determinada prerrogativa en ciertas circunstancias." TÓRTORA, Hugo, 2010, Las limitaciones a los derechos fundamentales [en línea] Estudios constitucionales vol. 8 (2) <http://www.scielo.cl/scielo.php?pid=S0718-52002010000200007&script=sci_arttext> [fecha de consulta: 11 de diciembre de 2013].

puede efectuarse si la Constitución ha habilitado expresamente al legislador para ello[77], no obstante no existe autorización alguna de estas características respecto al derecho contenido en el artículo 19° N° 4.

Nogueira, refiriéndose expresamente a esta situación, es decir, la ausencia de reserva de ley del derecho a la protección a la vida privada y a la honra de la persona y su familia (artículo 19 N°4), señala que existen dos soluciones: la primera, el derecho no puede ser limitado por el legislador, "ya que así lo ha deseado el constituyente, fortaleciendo el estatuto constitucional de tales derechos"; la segunda, el legislador puede regular el derecho a la intimidad "aplicando justificaciones determinadas por la propia Constitución, tales como los derechos de terceros o la existencia de bienes jurídicos de rango constitucional."[78]

[77] En este sentido, Tórtora establece que: "[…] el legislador u otra autoridad sólo podrán proceder a limitar un derecho fundamental, cuando previamente haya sido constitucionalmente habilitado para ello. Esta habilitación o autorización sólo podrá provenir de la Carta Fundamental, en virtud del principio de supremacía constitucional consagrado en el artículo 6° de nuestro Código Político; como también del art. 19 N° 26 de la Constitución, que dispone que los preceptos legales podrán limitar las garantías que establezca la Constitución, sólo cuando ésta así lo haya autorizado. De no existir tal habilitación constitucional, el legislador carece de competencia para establecer limitaciones o restricciones a los derechos fundamentales" TÓRTORA, Ibíd.

[78] NOGUEIRA, 2005. ob. cit.

Al igual que Nogueira, consideramos que el derecho a la intimidad sí admite limitaciones, pero sólo cuando lo exijan razones de interés general, como es el caso del orden público o la seguridad nacional, pero siempre en este caso, en virtud de una ley. Apuntamos aquí la insuficiencia del artículo 10° de la LPDP, pues su redacción otorga la falsa apariencia de un débil régimen de tutela de los datos sensibles, situación que como vimos es ampliamente sostenida en la doctrina. La frase "salvo cuando una ley lo autorice" que justifica el tratamiento de estos datos, es insuficiente pues alude a una realidad que no es tal: la ley no puede simplemente autorizar el tratamiento de esta información, pues no tiene la competencia entregada por la Constitución para ello; es por tanto, menester que la construcción legislativa que establezca una facultad de estas características se funde en una fórmula específica de interés general y siempre establecida en forma expresa.[79]

[79] Tórtora alude aquí a la norma contenida en el artículo 30º del Pacto de San José de Costa Rica que señala que "Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas". Sobre el particular agrega "Que los derechos puedan ser limitados en consideración al "interés general", no significa en ningún caso que este interés sea superior a los derechos humanos o a la dignidad de la persona, sino sólo implica que los derechos sólo podrán limitarse o restringirse "excepcionalmente", en atención a dicho interés general. Además, estas restricciones deberán ser establecidas en términos de generalidad normativa, de modo tal que no

En el segundo punto, es decir, el fundamento en la LPDP de la necesidad de autorización legal para el tratamiento de datos sensibles, encontramos el artículo 10° que establece como excepción al principio de no tratamiento de esta información, la autorización legal para dichas actividades. Creemos, sobre la base de lo establecido en la historia de la ley, que dicha autorización legal debe ser "expresa", utilizando al efecto la definición que realiza la RAE respecto de dicho adjetivo como algo "claro, patente, especificado."[80] En consecuencia, la disposición debe encontrarse explicitada de una manera que no deje dudas al intérprete acerca de la naturaleza, extensión, objetivo y finalidad del tratamiento de datos personales sensibles. Por lo que no cabe la aplicación extensiva de normas ambiguas y genéricas, que puedan producir dudas e incerteza respecto del real alcance de las operaciones realizadas por los órganos públicos o privados con dichos datos. En este sentido, el en ese entonces diputado José Antonio Viera–Gallo señalaba durante la discusión en sala en el primer

---

significaran sacrificios o cargas particulares, atentando contra la igualdad ante la ley y de la proscripción de toda forma de arbitrariedad." TÓRTORA, ob. cit.

[80] REAL ACADEMIA ESPAÑOLA, Diccionario de la lengua española, vigésimo segunda edición, 2001 [en línea], <http://lema.rae.es/drae/?val=expresa> [Fecha de consulta: 28 de agosto de 2013].

trámite constitucional que "(...) cuando hablamos de datos personales, es decir, que tienen que ver con la vida íntima o privada de las personas, se genera una reglamentación. En primer lugar, para que ello sea posible se requiere una autorización expresa de la ley, que autorice a un organismo público para recolectar esos datos en el ámbito de su competencia; por ejemplo, el Servicio de Impuestos Internos, los datos tributarios; el Registro Electoral, los electorales; el Ministerio de Salud, los sanitarios. Un organismo público no podría recopilar datos personales que excedan el ámbito de su competencia, como si el Servicio de Impuestos Internos recolectara datos electorales o el Ministerio de Salud obtuviera información tributaria. Sólo podrán almacenar esos datos cuando haya una autorización legal expresa y en el ámbito que les es propio, según lo establece el artículo 6º del proyecto."[81] [82]

2.2.1.1.3. Juicio de Ponderación como criterio para resolver conflictos.

[81] BIBLIOTECA DEL CONGRESO NACIONAL 1999, ob. cit., p. 190

[82] No obsta a lo razonado precedentemente el hecho de que, durante ese momento legislativo, el proyecto de ley no distinguía entre datos personales y sensibles, pese a que claramente la definición expresada se refería a los segundos, ni que el artículo referido por el diputado se convertiría eventualmente en el actual artículo 10° de la LPDP.

El juicio de ponderación, es un método de resolver conflictos entre principios constitucionales del mismo rango, buscando una solución satisfactoria entre ellos, pues, en abstracto, son todos del mismo valor. Una vez establecido que el derecho a la intimidad, y por tanto la protección de los datos sensibles, no son en ningún caso ilimitados y en consecuencia, sucumben tanto ante otros derechos fundamentales como ante bienes jurídicos de interés general (si así se ha manifestado la voluntad del legislador), se hace imperioso dilucidar dos posibles situaciones en las que prevalece el conflicto. Existirán casos en los que el choque de derechos es evidente, pero que no existe regulación normativa que lo dirima y otros, en los que la ley será precisa, pero será necesario otorgarle contenido a las fórmulas de interés general que justifican la limitación del derecho, en orden a evitar cualquier atisbo de abuso.

En el primer caso, y entendiendo que el artículo 19º nº 4 no contempla una explícita reserva legal y cualquier desarrollo se legitima sólo "a través de justificaciones determinadas por la propia Constitución, tales como los derechos de terceros o la existencia de bienes jurídicos de rango constitucional", y en último término, este desarrollo sólo se admite en tanto

sea adoptado por el legislador[83], es forzoso concluir que al no existir desarrollo normativo parlamentario no es posible derivar una limitación, y ante el conflicto, la protección de los datos sensibles prevalece.[84] Lo anterior, siempre que la contradicción se presente frente a razones de interés general, que requieren estar explicitadas en una ley[85], pues de no existir una positivación que dirima el conflicto entre derechos fundamentales, no puede concluirse directamente que la protección de la intimidad primará, pues uno de sus límites inmanentes y que delinean su contenido esencial es precisamente el respeto de los demás derechos esenciales.

En el segundo caso, de existir una norma que autorice el tratamiento de datos sensibles que utilice una fórmula consistente en criterios objetivos de necesidad, será necesario determinar claramente su alcance. Orden, moralidad o salud pública, seguridad o defensa nacional, son claros

[83] Sentencia del Tribunal Constitucional, Rol Nº 239, del 16 de julio de 1996, considerando 9º citado por Noguiera. Vid. NOGUEIRA, Ob. Cit.

[84] En este sentido, la Resolución 45/95 establece que las excepciones a los principios del tratamiento de datos, incluyendo a los datos sensibles, se podrán fundar en causales como la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, pero "siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas." ORGANIZACIÓN DE LAS NACIONAS UNIDAS. 1990. Ob. Cit. Principio 6.

[85] En este sentido, el artículo 10º de la LPDP, la directriz nº 6 de la Resolución 45/95, y los requisitos de limitación de un derecho fundamental que exigen el desarrollo normativo parlamentario.

ejemplos de bienes jurídicos de rango constitucional que propenden a la búsqueda de un bien común y que en determinados casos se erigen en limitantes expresos respecto de derechos fundamentales asegurados en la Constitución.

Muchas veces estas fórmulas genéricas estarán ya dotadas de contenido a través de la ley. Así, encontramos desarrollos legislativos expresos en nuestro ordenamiento jurídico que restringen el derecho a la intimidad (en lo relativo a la protección de los datos sensibles) por ejemplo tratándose del control de enfermedades transmisibles. En este apartado, desarrollado en el Título II del Código Sanitario y complementado en el reglamento respectivo[86] [87], se dispone la existencia de un catálogo de enfermedades de notificación obligatoria que incide en una obligación de los médico-cirujanos de comunicar por escrito el diagnóstico a la autoridad sanitaria más próxima.[88] Esta materia, esencial en el control de epidemias,

[86] Art. 21. Un reglamento determinará las enfermedades transmisibles que deben ser comunicadas obligatoriamente a las autoridades sanitarias, así como la forma y condiciones de la notificación. CHILE. Código Sanitario. Ob. Cit.

[87] CHILE. Ministerio de Salud. 2004. Decreto 158/4. Reglamento sobre notificación de enfermedades transmisibles de declaración obligatoria. 22 de octubre de 2004.

[88] CHILE, Código Sanitario. Ob. Cit. Art. 21. Además esta disposición agrega en su inciso segundo que "Igual obligación afectará a toda persona que en su casa o establecimiento tuviere uno de dichos enfermos, si no hubiere sido éste atendido por un médico-cirujano; a los directores

se encuentra entonces expresamente excepcionada del consentimiento del titular en cuanto al tratamiento de sus datos sensibles relacionados al padecimiento de algunas de las enfermedades consignadas en el citado reglamento, más aún, en su propio artículo 12º dispone la remisión directa a la LPDP.[89] En este caso, el legislador incluye en la norma el juicio de ponderación, estableciendo una forma de resolver el conflicto, privilegiando un principio (la salud pública) en detrimento de otro (la protección de los datos sensibles)[90]

Sin embargo, otras veces, la redacción de la normativa, simplemente designara el bien jurídico que prima sobre el derecho fundamental en un caso determinado, como sería por ejemplo, una norma que autorizara el tratamiento de datos sensibles cuando dicha actividad sea necesaria para la prevención de un peligro real para la seguridad nacional.

---

técnicos de las farmacias que despachen recetas destinadas al tratamiento de estas enfermedades y a quienes dirigen técnicamente los laboratorios clínicos que realicen los exámenes para su confirmación diagnóstica."

[89] El tratamiento de los datos obtenidos como el resultado de las notificaciones y comunicaciones a que alude el presente reglamento, se regirán por las normas de la ley Nº 19.628, sobre protección de la vida privada. CHILE. Ministerio de Salud. 2004. Decreto 158/4. Ob. Cit. Art. 12º.

[90] PRIETO SANCHÍS, Luis. 2008. El juicio de ponderación constitucional, en: CARBONELL, Miguel (editor), 2008, El principio de proporcionalidad y la interpretación constitucional, Quito, Ministerio de Justicia y Derechos Humanos, p. 116.

En este sentido, por ejemplo, es la previsión que efectúa la Resolución 45/95 de la ONU en su punto número 6[91].

El artículo 19º nº 26 establece que "la seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio."
La afectación a un derecho fundamental, por tanto, no podrá perjudicar el contenido esencial del mismo.[92] Sánchez Gil, adscribe a la utilización del principio de proporcionalidad para la determinación de este núcleo, pues un establecimiento permanente, correcto y aplicable en cualquier caso de este contenido esencial no tiene más que una utilidad didáctica ya que no sobrevive a la compleja relación entre bienes, normas jurídicas que los

[91]Las excepciones a los principios 1 a 4 [se incluye al número 5 correspondiente a los datos sensibles] solo pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas.

[92] Sánchez Gil, menciona que la idea del contenido esencial del derecho fue incluida para evitar la excesiva restricción de los derechos fundamentales y evitar su vaciamiento de contenido normativo. SANCHEZ GIL, Rubén. 2007. El Principio de Proporcionalidad. México D.F. Universidad Autónoma de México., p. 111.

tutelan y circunstancias en que interactúan, en la que la valoración es de todo menos sencilla.[93]

Ahora, la autorización legal que permita el tratamiento de los datos sensibles en aras de proteger la seguridad nacional o para una investigación concreta, no puede quedar sujeta al simple "capricho o a la voluntad azarosa de los operadores jurídicos"[94] Es por esto que, para Sánchez Gil, la aplicación del principio de proporcionalidad impone una regla como criterio de decisión: "para ser lícita una medida legislativa que intervenga un derecho fundamental, el fin que se propone debe satisfacerse de manera *equivalente o mayor* al perjuicio que ocasiona al último".[95]

Sin embargo, existe un problema subyacente y que sobrevive a esta solución, sobre todo en casos como el de la hipotética norma legal aludida. El legislador directamente elimina el conflicto, entregando con anterioridad la solución, postergando en abstracto un principio sobre otro. Se elimina, en consecuencia, de antemano cualquier posibilidad de ponderación judicial,

[93]Ibíd. p. 113
[94] Ibíd. p. 114-115.
[95] Ibíd. p. 115. Las cursivas son del autor.

pues el legislador ya ha efectuado tal juicio[96], pero se entregaría la preferencia a un principio carente de contenido evidente. La seguridad nacional es un concepto jurídico indeterminado y su primacía sobre derechos fundamentales no puede determinarse en abstracto, principalmente por el dinamismo de sus fundamentos.

Por tanto, la técnica legislativa que eventualmente permita el tratamiento de datos sensibles, debe hacerse cargo sistemáticamente de esta situación, estableciendo como parte integrante de la autorización la posibilidad de someterla a un juicio de ponderación de carácter jurisdiccional o directamente asumiendo el propio legislador en la propia norma el juicio de ponderación, dictando complementariamente disposiciones que indiquen "el peso de cada razón y, con ello la forma de resolver el conflicto"[97], conjugando de la mejor forma todos los principios constitucionales.

En consecuencia, la mera remisión del artículo 10º al legislador no sólo no se hace cargo de esta problemática, sino que simplemente la ignora

[96] PRIETO. Ob. Cit. pp. 105-106
[97] Ibíd. p. 101.

desde el principio, al no exigir expresamente ninguna razón de interés general para justificar una restricción a la protección de los datos sensibles.

2.2.1.2. Datos personales sensibles de salud.

Pese a que los estados de salud de una persona constituyen un dato sensible, obtenido de la lectura del mismo artículo 2°, letra g), puesto que comprende "los estados de salud físicos o psíquicos"[98], la LPDP entrega una protección mayor a este tipo de información[99]. En efecto, en su artículo 24° se establecen modificaciones al Código Sanitario el que en su artículo 127°, establece como reservados "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud"[100]. Es decir, para su legítimo tratamiento, se requiere el consentimiento expreso y por escrito del paciente, o que sean necesarios para el otorgamiento de beneficios de salud.[101]

[98] Ley 19 628, ob. cit., art. 10°.
[99] Véase nota N°66.
[100] CHILE, Ministerio de Salud Pública. 1967. Decreto con Fuerza de Ley 725: Código Sanitario. 11 de diciembre de 1967. Artículo 127°.
[101] Para Anguita, estos datos son los únicos sensibles que poseen una real protección especial en la actual legislación. ANGUITA, Ob. cit., p. 302.

2.2.1.3. Datos personales en general.

Jervis construye a los datos personales del inciso primero del artículo 4° como una categoría residual dentro de su clasificación; estos datos sólo podrán tratarse existiendo consentimiento expreso de su titular o autorización legal explícita distinta de las ya contenidas en la propia LPDP. En la práctica, todos los tipos de datos regulados en la ley son técnicamente datos personales, es decir, comparten la esencia de la letra f) del artículo 2°, ya que son relativos a cualquier información concerniente a personas naturales, identificadas o identificables; pero se apartan del ámbito de aplicación del inciso primero del artículo 4°, pues poseen normas expresas que regulan específicamente su tratamiento. Es en este sentido que el órgano público deberá respetar, por ejemplo, las normas de tratamiento de los datos relativos a obligaciones de carácter económico, financiero, bancario o comercial contenidas en el título III de la LPDP[102] pudiendo

[102] Pese a que en un inicio, el proyecto de ley comenzó siendo un esfuerzo por regular la intimidad, vida privada de las personas, y la protección de datos personales, durante su tramitación, el eje legislativo puso mayor énfasis en esta última categoría, y con especial ahínco en el tratamiento de los datos de carácter financiero y económico. La doctrina nacional distingue entre datos positivos (relativos principalmente a los activos patrimoniales de su titular, ingresos y ahorros), los que no podrán ser objeto de tratamiento; y los datos negativos (referidos a protestos, deudas y demás obligaciones contraídas por el titular), que son regulados extensamente por el Título III de la LPDP, y que en definitiva, pueden ser legítimamente tratados. Para proceder a estas actuaciones, la ley establece un catálogo de datos que pueden prescindir del consentimiento de su titular, los que enumerados en su artículo 17° corresponden a

tratar sólo los denominados “datos negativos”, con la expresa prohibición de comunicar dicha información cuando se genere en los períodos de cesantía de su titular; o, por otra parte, podrá tratar datos personales penales sólo en la esfera de sus competencias o existiendo autorización legal expresa, con la restricción a la comunicación de los antecedentes una vez prescrita la acción penal o la pena, salvo requerimiento judicial o de otro órgano público legalmente autorizado.[103]

---

obligaciones que consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.” A este punto debe de agregarse la facultad otorgada al Presidente de la República para determinar la procedencia del tratamiento de otras obligaciones de dinero, originadas de instrumentos de pago o de crédito válidamente emitidos. Estos datos no podrán ser comunicados a terceros una vez transcurridos cinco años (siete de la ley original), desde la fecha en que dicha obligación se hizo exigible. Sin embargo, tal eliminación de los registros no es absoluta, puesto que el mismo artículo ya citado establece que los datos igualmente deberán mantenerse, en el caso de que puedan ser requeridos por la justicia durante la sustanciación de algún proceso.

[103] Esta clasificación hace referencia a los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias cuando sean tratados por organismos públicos dentro de su competencia. Aparte de su titular, que posee el derecho de controlar sus propios datos y acceder a sus antecedentes penales, solo los organismos públicos, y siempre dentro de la esfera de sus competencias o en caso de autorización legal expresa, podrán adicionalmente tratar dicha información. Aun en este caso, se restringe expresamente la actividad de tratamiento de datos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. No obstante, los datos pueden seguir tratándose por los organismos respectivos en cualquiera de las otras formas mencionadas en la letra o) del artículo 2°. Se excepciona expresamente a esta restricción a la comunicación de los datos penales cuando estos sean requeridos por los Tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5°, 7°, 11° y 18°.

En conclusión, todo dato cuyo tratamiento se encuentra específicamente regulado en la ley, se encuentra en una relación de especie a género, respecto de los datos personales en general. Estos últimos, se rigen por lo dispuesto en el inciso primero del artículo 4°, es decir, requieren consentimiento previo e informado del titular de los datos o autorización legal expresa contenida en una disposición distinta a la LPDP.

2.2.1.4. Lo público y lo privado en la LPDP.

Existe discusión en la doctrina nacional respecto al sentido y alcance del concepto "fuentes accesibles al público".[104] No se aprecia con claridad, ni en la letra ni en la historia de la ley, si en el ámbito de los bancos de datos éstos se rigen por la publicidad o por la reserva como regla general. Para dirimir esta controversia, hay que distinguir previamente la naturaleza

[104] Mientras algunos autores establecen que toda fuente de datos personales de los órganos públicos son por regla general de acceso público no reservado a los solicitantes. (En este sentido JIJENA, Renato, 2001, ob. cit., p. 99. y JERVIS. Ob. Cit,. p. 123.); Cerda, adopta la reserva como criterio básico para la determinación del acceso a los bancos de datos (Vid. CERDA, Alberto. 2003, La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales. Tesis para optar al grado de Magíster en Derecho. Santiago, Universidad de Chile, Facultad de Derecho, p. 70) Por otra parte, Ramiro Mendoza establece que no es posible aplicar criterios generales para dicha determinación y que la publicidad o reserva de los registros dependerá de las normas particulares de cada órgano público en particular. MENDOZA, Ramiro. 2001, Régimen de los bancos de datos de organismos públicos. Una aproximación del derecho administrativo a la ley sobre protección a la vida privada, Cuadernos de Extensión Jurídica (5), pp. 139-140.

de la fuente, es decir, si su origen es público por ser su responsable un órgano público o, por el contrario, privado, por estar a cargo de particulares. A su vez, no se resuelve manifiestamente si el carácter público o privado de la información propiamente tal, varía en función del soporte que le sirve de sustento y en cualquier caso, en función de la base de datos misma. No es legítimo afirmar que el carácter público de una base de datos "contagia" a toda la información contenida en ella de esa publicidad, pues es necesario remarcar que las bases de datos o soportes informáticos y los antecedentes mismos, se mueven por canales completamente separados. La información sensible no se contamina -necesariamente- del carácter de público del registro en donde se encuentra.

Las fuentes accesibles al público están definidas en la letra i) del artículo 2° como "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes". El órgano público podrá tratar datos personales, obtenidos lícitamente,[105] que provengan o se recolecten de estas fuentes accesibles al público siempre que cuente con autorización de su titular, remitiéndonos a la norma

[105] JERVIS, Ob. Cit., p. 122.

fundamental de tratamiento de datos contenida en el artículo 4°. Sin embargo, en tres hipótesis taxativas[106] y alternativas,[107] podrá tratar dichos datos sin necesidad de consentimiento. Se erigen estos supuestos como la primera excepción expresa a la autorización previa e informada del titular de los datos contenida en la LPDP. En consecuencia, se podrán tratar abiertamente los datos de fuentes accesibles al público en tres casos:

a. Cuando sean de carácter económico, financiero, bancario o comercial;
b. Cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o;
c. Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

[106] En este sentido la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, se refiere a "tres únicas excepciones". BIBLIOTECA DEL CONGRESO NACIONAL, 1999, ob. cit., p. 332.
[107] JERVIS, Ob. Cit., p. 118.

Cuando nos referimos a fuentes cuyo responsable es un privado -persona natural o jurídica-, la determinación de la publicidad o reserva del banco dependerá de si éste permite o no el acceso al solicitante en forma no restringida; en caso afirmativo, se considerará fuente accesible al público.[108]

En el ámbito de los bancos de datos de organismos públicos, la determinación de si éstos se rigen por la publicidad o por la reserva como regla general es más espinosa. Jervis[109] menciona dos soluciones elaboradas por la doctrina, la primera (a la que adhiere) entiende que todas las fuentes de datos personales serán de acceso público, a menos que una ley establezca expresamente lo contrario;[110] la segunda, otorga preponderancia a la reserva, debiendo establecerse expresamente la publicidad.

Al igual que Cerda,[111] nos inclinamos por la segunda solución. Si bien es cierto que desde la dictación de la Ley 20 285, la regla general respecto de las actuaciones de los órganos de la Administración del Estado

[108] Ibíd. p. 124.
[109] Ibíd. p. 123.
[110] JIJENA, Ob. Cit., p. 99
[111] CERDA, 2012, Ob. Cit. p. 21.

es la publicidad,[112] dicho criterio no se traspasa directamente al tratamiento de datos personales.[113] Esta actividad, en virtud de la aplicación del principio de especialidad, se encuentra regulada, aun respecto de órganos públicos, por la LPDP y en particular por su artículo 20°. De esta forma, la publicidad de los actos públicos encuentra coto en toda la actividad de tratamiento de datos, a menos que, por supuesto, y como lo señala la misma legislación de protección a la vida privada, una ley expresamente lo autorice. En consecuencia, el libre acceso a los bancos de datos de órganos y servicios públicos no puede derivarse del principio de publicidad de la actividad estatal, en especial, considerando que como las actividades de recolección y almacenamiento, esenciales a cualquier base de datos, son consideradas por la LPDP como tratamiento, la aplicación de esta norma prima por su especialidad. A mayor abundamiento y haciendo eco de la tendencia comparada de otorgar protección especial a determinados datos

[112] CHILE, Ministerio Secretaría General de la Presidencia, 2008, Ley 20 285 sobre Acceso a la Información Pública, Agosto 2008, Art. 7°.

[113] En el mismo sentido se expresa Mendoza cuando señala que "Cabe desechar de plano una relación intrínseca entre su regulación (fundada en el ánimo de dar protección a la vida privada) [en referencia a la LPDP] y la publicidad y transparencia de la actuación del Estado, exigida por la Ley 18 575, de Bases Generales de la Administración del Estado. MENDOZA, Ob. Cit. p.140. Sustenta la opinión contraria Jervis al establecer que "... en el ámbito público, rige como regla la publicidad (...) De manera que la regla general, a lo menos en el ámbito público, es que las fuentes de datos personales sean públicas, salvo que una norma establezca lo contrario". JERVIS. Ob. cit. p. 123.

relacionados con la esfera íntima de las personas, la propia ley 20 285 establece como causal de secreto o reserva para denegar total o parcialmente el acceso a la información "cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico."[114] Esta norma otorga un especial énfasis a la protección sistemática de los denominados datos personales sensibles. Siendo el consentimiento informado del titular la norma en el ámbito de protección de los datos personales, sólo podrán tratarse datos sin esta autorización previa en los casos expresamente previstos en la legislación y no existe una norma genérica que otorgue publicidad a los bancos de datos de organismos públicos.

Se ha afirmado en contra de lo anteriormente expuesto, que cuando el legislador ha querido otorgar confidencialidad o reserva a una determinada información, así lo ha hecho expresamente, por lo que no cabe sino concluir que en Chile, todas las fuentes de datos personales son por regla general, de

[114] CHILE. Ley 20 285, ob. cit., art 21° N°2.

acceso público.[115] Pensamos, sin embargo, que ésta no es la interpretación adecuada, pues cuando la ley ha otorgado el carácter de secreto a determinados datos, no lo ha hecho con la finalidad de sustraerlo de la aplicación de la publicidad como regla general, sino para darle un mayor énfasis a su protección. En el caso del secreto de la afiliación política,[116] por ejemplo, la razón fundamental de su reserva es otorgarle un ámbito de resguardo adicional por constituir un dato especialmente protegido, incluido dentro de la categoría de datos personales sensibles establecidos en la letra g) del artículo 2° de la LPDP.[117] Cuando el legislador ha pretendido otorgar publicidad a ciertos registros, lo ha dicho expresamente, como lo expresan en este sentido el artículo 211° del Reglamento Orgánico del Servicio de

[115] En este sentido Renato Jijena establece que "cabe entonces concluir que en Chile todas las fuentes de datos personales serán en principio y por regla general y legalmente de acceso público, no restringido o reservado a los solicitantes, salvo que una ley especial (...), o una norma o resolución administrativa o una cláusula contractual de confidencialidad establezcan expresamente lo contrario." JIJENA, Ob. Cit. p. 99. Véase también a Jervis que señala que "De manera que la regla general, a lo menos en el ámbito público, es que las fuentes de datos personales sean públicas, salvo que una ley establezca expresamente lo contrario." JERVIS, Ob. Cit. p. 123.

[116] Nos referimos a este tipo de dato en particular, pues es mencionado por Jijena para justificar la proposición de que en Chile las fuentes de datos son por regla general de acceso público y cuando el legislador ha requerido la reserva, lo ha señalado así expresamente. JIJENA, Ob. Cit. p. 104.

[117] La afiliación política es un dato sensible en virtud de la propia definición de la LPDP y así ha sido refrendado por el Consejo para la Transparencia al denegar la entrega de dicha información aplicando en relación a la disposición citada, el artículo 21° N° 5 de la Ley de Transparencia. (A152-09) CONSEJO PARA LA TRANSPARENCIA, 2011. Jurisprudencia relevante del Consejo para la Transparencia en relación a la protección de datos personales. [en línea] <http://goo.gl/bTe4uO> [Consulta: 22 de diciembre de 2013]

Registro Civil (DFL n°2128 de 1930)[118], el artículo 49° del Reglamento del Registro Conservatorio de Bienes Raíces[119], o lo dispuesto en los artículos 4°, 31° y 32° de la Ley 18 556 Orgánica Constitucional sobre Sistema de Inscripciones Electorales y Servicio Electoral en lo referente a la publicidad de los datos del registro electoral.[120]

[118] CHILE. Ministerio de Justicia. 1930. Decreto con fuerza de ley 2128, 28 de agosto de 1930. Artículo 211°. "Podrán solicitar certificados del Registro Civil, a más de los interesados en una inscripción, todas las personas que lo deseen."

[119] CHILE. Ministerio de Justicia, Culto e Instrucción Pública. 1857. Decreto s/n. Reglamento del Registro Conservatorio de Bienes Raíces, 24 de junio de 1857. Art. 49°. "En orden a la guarda de los Registros incumben a los Conservadores los mismos deberes y obligaciones que a los escribanos. Son, no obstante, esencialmente públicos todos ellos; por consiguiente, es permitido a cualquiera consultarlos en la misma oficina y tomar los apuntes que crea convenientes."

[120] CHILE. Ministerio del Interior. 1986. Ley 18 556 orgánica constitucional sobre sistema de inscripciones electorales y Servicio Electoral. 01 de octubre de 1986.
Artículo 4°.- "El conocimiento público del Registro Electoral procederá en la forma dispuesta en el Párrafo 1° del Título II.
Los datos del Padrón Electoral no podrán ser usados para fines comerciales.
El Servicio Electoral deberá dar cumplimiento a lo previsto en la ley N° 19.628, sobre protección de la vida privada, salvo en los casos señalados en esta ley."
Artículo 31.- "El Servicio Electoral determinará un Padrón Electoral con carácter de provisorio, ciento diez días antes de una elección o plebiscito. Éste contendrá una nómina de las personas inscritas en el Registro Electoral que, conforme a los antecedentes conocidos por el Servicio Electoral antes de los ciento veinte días previos al acto electoral, reúnan a la fecha de la elección o plebiscito correspondiente los requisitos necesarios para ejercer el derecho a sufragio.(...)"
"El Padrón Electoral y la Nómina Provisoria de Inhabilitados son públicos, sólo en lo que se refiere a los datos señalados en el inciso tercero [nombres y apellidos del elector, su número de rol único nacional, sexo, domicilio electoral con indicación de la circunscripción electoral, comuna, provincia y región a la que pertenezcan y el número de mesa receptora de sufragio en que le corresponde votar.]..."
Artículo 32.- "El Servicio Electoral determinará un Padrón Electoral con carácter de auditado, setenta días antes de una elección o plebiscito. (...)"
"El Padrón Electoral con carácter de auditado y la Nómina Auditada de Inhabilitados deberán ser publicados por el Servicio Electoral en su sitio web con setenta días de antelación a la fecha que deba verificarse una elección o plebiscito."

En definitiva, para determinar si un banco de datos cuyo responsable es un órgano público puede ser considerado como fuente de datos accesible al público, será necesario determinar si existe norma expresa que le confiera tal carácter.

2.2.2. Segundo Requisito: El órgano público debe actuar dentro de su competencia.

La competencia es la facultad que la ley le ha otorgado a un órgano de la administración en orden a satisfacer las necesidades públicas que le han encomendado. Que un órgano público actúe dentro de su competencia, implica necesariamente que se atenga al ámbito previamente delimitado por ley de sus atribuciones. Si obra dentro de dicho marco, sus actuaciones serán legítimas en los términos de lo establecido por el artículo 7° de la Constitución Política de la República. Dado lo anterior, cuando un órgano público se enfrenta a la tarea de tratar datos personales, debe hacerlo siempre en el ámbito específico de sus atribuciones establecidas legalmente, es decir, dentro de su competencia, respetando además “las reglas precedentes” establecidas en la LPDP.

El artículo 20° de la LPDP puede presentar problemas respecto a su correcta interpretación, pues su redacción se presta para equívocos. Como ya mencionábamos, cumplidos los requisitos establecidos precedentemente "no necesitará el consentimiento del titular". Esta excepción al consentimiento previo merece ciertas precisiones, pues su alcance, estimamos, no es tan absoluto como se ha sostenido.[121] En todos aquellos casos no expresamente excepcionados en la propia ley 19 628 de requerir el consentimiento del titular de los datos, para prescindir de tal autorización, se precisará una norma expresa que permita tal tratamiento contenida en una disposición legal distinta; y aun no existiendo precepto alguno, el órgano público que actúa dentro de su competencia, estaría autorizado. El mentado artículo hace referencia a la autorización legal para el tratamiento de datos personales sin ningún otro calificativo, es decir, exclusivamente en lo referente a los términos establecidos en el inciso primero del artículo 4° de la LPDP. Se configura de esta forma una autorización genérica a todo

[121] Así, autores como Dintrans o Vera Lama han interpretado el artículo 20° como una autorización genérica comprensiva aun del tratamiento de datos sensibles. Vid. DINTRANS, Constanza, 2007. El tratamiento de datos personales en el proceso de persecución penal chileno. Memoria para optar al título de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile. Facultad de Derecho. pp. 91-92; DINTRANS, Constanza, 2005. Tratamiento de datos personales por la Policía de Investigaciones. Comentario a sentencia de la Corte de Apelaciones de Santiago, Rol 494-2004. Revista de Derecho Informático (6). p.179.; VERA, Ob. Cit., p. 161.

órgano público (sin distinción referente a la magnitud de sus objetivos y los bienes jurídicos o intereses generales que su actuación cautela) para tratar datos personales en general, fundada en el principio de competencia.[122] La razón de esta excepción al consentimiento previo aplicable respecto del tratamiento de datos efectuado por órganos públicos, es que, pensamos, la norma de competencia se funde y se confunde con la autorización legal requerida en el artículo 4° de la LPDP.

La norma de competencia establece el marco de acción en que legítimamente el órgano público puede intervenir; dicho de otra forma, delimita el ámbito de sus atribuciones, y si consideramos que toda acción de cualquier órgano debe estar debidamente fundamentada, podemos interpretar que éste deberá conocer toda la información necesaria para ejercer propiamente sus funciones. En este caso, podemos prescindir de una

[122] Algunos autores, sin embargo, señalan la inconveniencia de autorizar el tratamiento de datos personales en general que efectúan los órganos públicos, sin requerir una normativa especial que verse sobre el asunto. En tal sentido se expresa Mendoza al señalar que: "al desechar el principio de especialidad de la ley en la creación de bases de datos y dejar su legitimad casi en manos del principio de competencia, el cual es medido según el órgano de la Administración que realice el tratamiento de datos, se deja un marco de discrecionalidad confiando sólo en la buena fe del órgano (se dice para el cumplimiento de sus funciones)." MENDOZA, Ob. Cit., p. 149. Jervis agrega sobre el particular que "no es posible establecer un principio general de legitimidad para el tratamiento de datos por parte de los organismos públicos y que serán en último término los Tribunales de Justicia y la Contraloría los que determinan si un organismo público actúa dentro de sus competencias como responsable de un banco de datos." JERVIS, Ob. Cit., p. 142.

autorización específica que permita el tratamiento de datos personales -en sentido amplio- contenida en una ley, pues se infiere de la propia norma de competencia, que cada órgano está facultado para conocer todos los datos necesarios para su actividad, incluyendo datos personales. Concluye fundamentalmente en el mismo sentido Dintrans, quien considera que esta exención de consentimiento previo es la manifestación del principio de legalidad al que deben someterse los órganos del Estado[123]. Todo esto no significa que la autorización legal expresa no sea necesaria, pero en caso de ausencia de norma, deberán interpretarse las atribuciones y funciones entregadas por ley para poder encuadrar dentro de ellas el tratamiento de datos personales, debiendo considerarse elementos como la naturaleza del dato, la finalidad del tratamiento y la función del órgano al enfrentarse a esa actividad[124]. Todo esto, sin perjuicio de los derechos que asisten a los titulares, contenidos en la propia ley.

Nos referimos con anterioridad a que esta excepción al consentimiento previo merece ciertas precisiones, pues se ha interpretado el artículo 20° en términos amplísimos, extendiéndose esta autorización

[123] DINTRANS, 2007, Ob. Cit., p. 91
[124] JERVIS, Ob. Cit., p. 141 – 142.

también al tratamiento de datos sensibles, lo que destruye todo el régimen reforzado de protección, que al menos en doctrina, tiene dicha información, considerados como datos especialmente protegidos. Esta afirmación permite entender el particular refuerzo que beneficia a este tipo de datos, entendidos en términos amplios como todos aquellos antecedentes de la esfera íntima de las personas, susceptibles de generar discriminaciones arbitrarias a su titular como consecuencia de su tratamiento.

Como ya hemos mencionado, los datos sensibles requieren, al tenor del artículo 10° de la LPDP, de una norma que autorice su tratamiento. Por tanto, nos encontramos con dos normas distintas que establecen exigencias distintas para tratar datos, pues se refieren, en esencia, a cosas distintas: los datos personales en general y los datos sensibles en particular. En consecuencia, y armonizando la actual legislación con el debido respeto a la intimidad y a la autodeterminación informativa de las personas, la autorización legal para tratar datos personales en general (derivada de las propias normas de competencia del órgano público) no debe confundirse con la específica autorización requerida para tratar datos sensibles que dispone el artículo 10°. Concluimos entonces que el órgano público no

podrá tratar datos sensibles, aun en la esfera de su competencia, sin una norma legal expresa establecida en los términos de lo preceptuado en el artículo 10°.

De lo razonado anteriormente, se desprenden importantes consecuencias. Como veremos al analizar las normas fundamentales en materia de inteligencia y persecución penal, se ha optado por una técnica legislativa que no es concordante con lo establecido en el marco de la LPDP, lo que presenta variados desafíos a la hora de armonizar el correcto funcionamiento de dichos órganos con la debida protección de los datos personales.

# CAPÍTULO III. DEL SISTEMA NACIONAL DE INTELIGENCIA Y EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES

## 3.1. Antecedentes Generales

El Sistema Nacional de Inteligencia y la Agencia Nacional de Inteligencia fueron creados por la ley 19 974, del 5 de octubre de 2004. El trámite legislativo se inició mediante Mensaje del Presidente de la República, ingresado al parlamento con fecha 10 de octubre de 2001. Su promulgación vino a reemplazar a la Dirección de Seguridad Pública e Informaciones, creada por la Ley N° 19 212. Señala Vera[125], que tiende a pensarse que el proyecto de ley nació como una respuesta a los atentados en Estados Unidos del 11 de septiembre de 2001, pero las bases del mismo pueden encontrarse con bastante anterioridad. En efecto, ya desde 1997, que existía intención de parte de la Cámara de Diputados de elaborar un proyecto de ley que regulase las diversas agencias de inteligencia del Estado, su funcionamiento e interoperatividad.[126]

En el mensaje del proyecto, se establecieron las siguientes afirmaciones preliminares que justificaban la reglamentación presentada:

[125] VERA, Ob. Cit., p. 124

[126] Ibíd. p. 127. Además, vid. HOLZMANN, Guillermo, 1996, Bases, fundamentos y propuesta para un proyecto sobre " Sistema Nacional de Inteligencia", Universidad de Chile, Instituto de Ciencias Política, 44 p.

a. En Chile existían entidades públicas que realizaban actividades de Inteligencia;

b. Para un Estado moderno, la actividad de Inteligencia es un instrumento gubernamental legítimo y necesario; y,

c. La reglamentación vigente en materia de servicios de Inteligencia, adolece de insuficiencias en relación con la eficacia de tal institucionalidad, así como de la perspectiva de la garantía de los derechos de las personas frente a la actuación de tales entidades y de la fiscalización de las actividades de los servicios de inteligencia.[127]

Como principios rectores, se establecieron los siguientes presupuestos:[128]

a. Principio del respeto al ordenamiento jurídico: los servicios de inteligencia, así como quienes los integren, deberán siempre actuar apegados a la Constitución Política de la República y al ordenamiento jurídico;

[127] BIBLIOTECA DEL CONGRESO NACIONAL, 2004, Historia de la ley 19974 Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia, <disponible en línea: http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/3784/1/HL19974.pdf> [Fecha de consulta: 25 de agosto de 2013] p. 6

[128] Ibíd. pp. 10 y ss.

b. Principio del respeto al régimen democrático: En su actuar, los órganos deberán siempre respetar el régimen democrático y la estabilidad institucional del país;

c. Principio de respeto a los derechos constitucionales: Los procedimientos realizados deberán apegarse estrictamente a los derechos de las personas establecidos en la Constitución Política de la República;

d. Principio de la autorización judicial previa: al utilizar las llamadas técnicas intrusivas, deberá siempre solicitarse la autorización judicial, ante el ministro de la Corte de Apelaciones respectiva;

e. Principio de proporcionalidad: las técnicas y medidas utilizadas deberán ser las necesarias y adecuadas a la consecución de los objetivos;

f. Principio de reserva: se establece el secreto, tanto para quienes efectúen el control de las actividades, como para los funcionarios que realicen las labores de inteligencia; y,

g. Principio de utilización exclusiva de la información: Los estudios y antecedentes que se elaboren, obtengan o intercambien los órganos del sistema de inteligencia sólo podrán usarse para los respectivos cometidos.

### 3.2. Institucionalidad de Inteligencia en Chile

Apunta Barrera[129] que el modelo institucional seguido en Chile por la legislación de inteligencia integra por una parte una agencia civil, dependiente del Ministerio del Interior, con facultades de inteligencia exterior, interior y contrainteligencia, y por otra organismos de inteligencia policiales y militares, los últimos también con funciones de seguridad interior.

#### 3.2.1. Sistema de Inteligencia del Estado.

Se refiere al conjunto de organismos de inteligencia, independientes entre sí, funcionalmente coordinados, que dirigen y ejecutan actividades de inteligencia y contrainteligencia.

##### 3.2.1.1. Ámbito de competencia del Sistema de Inteligencia del Estado.

[129] BARRERA, Felipe, 2009, Análisis de la Actividad de Inteligencia del Estado y su Control Público Jurídico, Memoria para acceder al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, Santiago p. 62

De acuerdo a lo establecido en el artículo 4° de la ley 19974, el objetivo del Sistema de Inteligencia del Estado será: “proteger la soberanía nacional y preservar el orden constitucional, y que, además, formul[en] apreciaciones de Inteligencia útiles para la consecución de los objetivos nacionales.”

Estableciendo un punto de partida, debemos remitirnos a las normas establecidas en la Constitución, la que, en su artículo 1°, establece que “Es deber del Estado resguardar la seguridad nacional, dar protección a la población y a la familia (…)”. Del mismo modo, en su artículo 101° se prescribe que “Son las Fuerzas Armadas las esenciales para la seguridad nacional y la defensa de la patria”.

Precisando las normas citadas, cabe determinar entonces, cuál es el contenido y alcance del concepto de seguridad nacional, con el objetivo de establecer la extensión de éste, e intentar en definitiva, arrojar luces sobre su relevancia a efectos de la autorización para el tratamiento de datos personales sin el consentimiento de su titular.

El Libro de la Defensa Nacional establece que se entiende como Seguridad Nacional "Toda acción encaminada a procurar la preservación del orden jurídico institucional del país, de modo que asegure el libre ejercicio de la soberanía de la Nación, tanto en el interior como en el exterior, con arreglo a las disposiciones establecidas, a la Constitución Política del Estado, a las leyes de la República y a las normas del Derecho Internacional, según corresponda".[130]

En base a estas consideraciones, la doctrina nacional ha establecido un marco operativo mediante el cual se puede contextualizar el trabajo de las agencias de inteligencia. En éste ámbito, puede establecerse que el objetivo de dichos organismos es la producción de inteligencia, es decir, información útil para apoyar la toma de decisiones por parte de las autoridades superiores de la nación. Así, Vera[131] señala que el objetivo de la producción de inteligencia se dirige en primer lugar a proteger la soberanía nacional, entendiéndola en su cara interna, como la obligación de mantener

[130] MINISTERIO DE DEFENSA NACIONAL, "Libro de la Defensa Nacional", disponible en línea: [http://www.defensa.cl/archivo_mindef/Libro_de_la_Defensa/2010/2010_libro_de_la_defensa_3_Parte_Politica_de_Defensa_Nacional.pdf] (fecha de consulta: 28-09-2013)
[131] VERA, Ob. Cit., p. 149

la supremacía del poder estatal sobre el territorio nacional, manteniendo a este último por sobre otros poderes sociales; y en su ámbito externo, como la mantención de la independencia del Estado frente a potencias externas y la mantención, a su vez, de su igualdad con éstas. Asimismo, ha de velar por la preservación del orden constitucional, entendida como la vigencia y supremacía de la Constitución de la República. Del mismo modo, Barrera se refiere a la mantención de la seguridad nacional interna y externa, agregando que la expresión "supone un amplísimo concepto que abarca una serie de aspectos progresivamente incorporados en el tiempo." [132]

Sin embargo, la caracterización de la seguridad nacional resulta problemática por la misma razón de su propia amplitud: en efecto, se ha descrito a dicho ámbito como uno "indeterminado" sobre el cual no puede asignársele una definición operativa , teniendo que ser determinado, caso a caso, por los Tribunales de Justicia[133]. Aun cuando, como hemos visto, puedan establecerse criterios delimitadores de la actividad de seguridad, Contreras y García señalan que, dado el carácter indeterminado de dicho

[132] BARRERA, Felipe, Ob. Cit., p. 49
[133] FERNANDEZ, Miguel Ángel, 2005, El principio de publicidad de los actos estatales en el nuevo artículo 8° inciso 2° de la Constitución, en: Zúñiga, Francisco (coordinador), 2005, Reforma Constitucional, Editorial LexisNexis, Santiago, p. 198.

concepto, siempre quedará un espacio para la interpretación, la que siempre será controvertida: "En la seguridad de la Nación, la valoración puede determinarse a favor de la libertad del individuo, restringiendo su contenido al mínimo o, por otra parte, reforzando la dimensión de garantía institucional de la cláusula."[134] Por lo demás, su amplia concepción implicaría que su contenido esencial sólo puede tomar forma en la medida de que pueda ser contrastado con otros principios en juego[135].

Luego, y en cuanto al segundo objetivo de la formulación de Inteligencia, es decir, la consecución de los objetivos nacionales, Vera señala que existen objetivos permanentes, fijos en el horizonte de proyección[136]. Para alcanzarlos, los gobiernos ejecutan, de acuerdo a sus prioridades y decisiones, los llamados objetivos actuales, variables según las circunstancias y la voluntad política de las autoridades de turno.

---

[134] GARCÍA, Gonzalo y CONTRERAS, Pablo, 2009, Derecho de acceso a la información en: Chile: Nueva regulación e implicancias para el sector de la defensa nacional, en Estudios Constitucionales (7) N° 1, Centro de Estudios Constitucionales, Universidad de Talca, pp. 162 y ss.

[135] "En consecuencia, la seguridad de la Nación no tiene un significado inmutable; depende de cómo se relaciona con otros conceptos esencialmente controvertidos, como es la libertad de expresión, la moral o un medio ambiente limpio." Ibíd., p. 163

[136] Se incluyen dentro de éstos, la preservación de la nación chilena, la conservación de su identidad, el mantenimiento de su independencia, la consecución de un desarrollo económico alto, la convivencia ciudadana pacífica. VERA, Op. Cit., p. 153.

### 3.2.2. Agencia Nacional de Inteligencia. Ámbito de Competencia

Es un servicio público centralizado, de carácter técnico y especializado, que está sometido a la dependencia del Presidente de la República a través del Ministro del Interior, cuyo objetivo es producir inteligencia para asesorar al Presidente de la República y a los diversos niveles superiores de conducción del Estado. En relación a su competencia, establecida en el artículo 7° de la ley 19 974, es decir, la formulación de información útil, nos remitiremos a lo ya señalado precedentemente respecto del Sistema de Inteligencia[137].

### 3.2.3. Órganos de Inteligencia Militar. Ámbito de Competencia.

De acuerdo a la ley N°18 948, Orgánica Constitucional de las Fuerzas Armadas, éstas "constituyen los cuerpos armados que existen para la defensa de la patria, y son esenciales para la seguridad nacional"[138]. La inteligencia militar, por su parte, comprende de acuerdo a lo establecido en el artículo 20° inc. 1° de la Ley 19 974: "…la inteligencia y la

[137] SUPRA en la página 76.
[138] CHILE, Ministerio de Defensa Nacional, 1990, Ley 18 948 Ley Orgánica Constitucional de las Fuerzas Armadas, febrero 1990.

contrainteligencia necesaria para detectar, neutralizar y contrarrestar, dentro y fuera del país, las actividades que puedan afectar la defensa nacional"[139]. Esta última es considerada a su vez por la doctrina nacional, como "…el conjunto de medios materiales, humanos y morales que una Nación puede oponer a las amenazas de un adversario en contra de sus objetivos nacionales"[140]. La expresión "dentro y fuera del país", de la disposición ya citada, otorga el mandato legal para la actuación fuera de las fronteras nacionales, lo que conlleva la interrogante de la efectividad de las medidas legales de protección en el exterior.[141]

3.2.3.1. Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional.

[139] Debido a lo somera de la regulación relativa a la inteligencia militar, consistente en sólo dos artículos, Vera sostiene que la real regulación de dichas instituciones y los reales alcances de sus medidas deben encontrarse en reglamentos secretos. Para los efectos de esta investigación, nos detendremos en la regulación efectuada por parte de la ANI. Para Vera la misma limitación con respecto a dicho organismo, puede aplicarse a los órganos de inteligencia militar. VERA, Ob. Cit., p. 193.

[140] Ibíd., p. 192.

[141] Así parece entenderlo Carlos Ruiz, cuando, al afirmar desde la perspectiva española: "No parece que deba ser igual la situación de los servicios de inteligencia que operan en el exterior de la de los que operan en el interior del territorio nacional español. En efecto, la Constitución Española reconoce el derecho de los ciudadanos a la intimidad, la inviolabilidad del domicilio y el secreto de las comunicaciones, lo que implica un correlativo deber de los poderes públicos (incluidos los servicios de inteligencia) de respetarlos. Pero ¿gozan de esos derechos ciudadanos extranjeros que se encuentran fuera de España? […] La respuesta parece que es negativa." RUIZ, Carlos, 2007, Problemas actuales del derecho de los servicios de inteligencia, Inteligencia y Seguridad (2): 13-46, p. 38.

Es el organismo encargado de asesorar y proporcionar inteligencia para la correcta y oportuna toma de decisiones en los niveles político – estratégicos del Ministro de Defensa Nacional y Jefe del Estado Mayor de la Defensa Nacional.

3.2.3.2. Dirección de Inteligencia del Ejército de Chile.

Organismo dependiente del Estado Mayor del Ejército que tiene por objeto asesorar al Comandante en Jefe del Ejército en el conocimiento, estudio, planificación, dirección y control de las actividades referidas a Inteligencia, Contrainteligencia y Operaciones Especiales.[142]

3.2.3.3. Dirección de Inteligencia de la Armada.

Órgano dependiente de la Comandancia en Jefe de la Armada, ~~con~~ que tiene el propósito de obtener y procesar información y difundir inteligencia naval destinada a contribuir a la formulación de políticas institucionales, y la adopción de medidas que resguarden la seguridad de las instalaciones y del personal de la Armada.

[142] VERA, Ob. Cit., p. 196

3.2.3.4. Dirección de Inteligencia de la Fuerza Aérea de Chile.

Organismo dependiente del Estado Mayor General de la Fuerza Aérea cuyo fin es asesorar al mando en las áreas de Inteligencia y Contrainteligencia.

3.2.4. Órganos de Inteligencia Policial. Ámbito de Competencia

El artículo 22° de la ley 19974 establece que esta función corresponde exclusivamente a Carabineros de Chile y a la Policía de Investigaciones de Chile, sin perjuicio de lo establecido en el inciso segundo del artículo 20°[143]. Su ámbito de acción, de acuerdo a la misma norma, se limita al orden público y la seguridad pública interior.[144]

3.2.4.1. Dirección Nacional de Inteligencia de Carabineros.

[143] "Excepcionalmente, dentro de las funciones de policía que le corresponden a la autoridad marítima y a la aeronáutica, la inteligencia naval y la aérea podrán realizar el procesamiento de información de carácter policial que recaben." CHILE. Ley 19 974. Ob. Cit., Art. 20. Inc. 2º.
[144] VERA. Ob. Cit., p. 200.

Cuerpo que tiene la misión de producir y difundir permanentemente inteligencia policial, en materias de Orden y Seguridad Pública y Seguridad Institucional, para asesorar la toma de decisiones del Mando.

3.2.4.2. Jefatura Nacional de Inteligencia Policial de la Policía de Investigaciones.

Se encuentra destinada a controlar la acción de los medios de búsqueda de información, con el objeto de prevenir o contrarrestar la perpetración de actos atentatorios contra la seguridad del Estado, coordinar el intercambio de información con otros organismos afines y confeccionar cuadros estadísticos con antecedentes e información respecto al acontecer nacional.[145]

3.2.5. Unidad de Análisis Financiero.

Si bien no se encuentra incluida dentro del Sistema de Inteligencia de la ley 19974, dicho órgano persigue el objetivo de prevenir e impedir la utilización del sistema financiero y de otros sectores de la actividad

[145] Ibíd., p. 208

económica, para la comisión de alguno de los delitos contenidos en la misma ley, como el ocultamiento de bienes provenientes de alguno de los delitos contemplados en el artículo 27° de la ley 19913.

En el desempeño de sus funciones, sus informes y peritajes sólo podrán ser derivados al Ministerio Público, a efectos de iniciar el proceso penal correspondiente, estándole prohibido el utilizar dichos documentos para cualquier otro fin (art. 2° inc. 2°). Lo anterior tendrá especial relevancia cuando analicemos las funciones de la ANI, en especial la facultad de dicho organismo de requerir información a las demás reparticiones públicas.

3.3. Tratamiento de datos personales por parte de los órganos de inteligencia

Como hemos establecido en el capítulo II, el artículo 20° de la LPDP prescribe que el tratamiento de los datos personales por parte de los órganos públicos sólo podrá hacerse en el marco de sus competencias y con sujeción a las normas allí establecidas; bajo tales supuestos, ~~el~~ este tratamiento no requerirá el consentimiento de su titular. Desde la óptica del principio de

competencia, afirmamos que la solución correcta requiere la aceptación del tratamiento de los datos personales. No obsta al presente análisis que la mayoría de las normas de competencia y atribuciones de los órganos que componen el Sistema de Inteligencia se encuentren reguladas en órdenes internas, fuera del alcance del escrutinio público. Cabe recordar un incidente, ocurrido en noviembre de 2003, cuando personal en servicio activo del ejército ingresó al Consulado de la República Argentina, y fueron descubiertos por el personal diplomático apostado allí[146]. Una vez iniciado el proceso en contra de los uniformados descubiertos, su defensa argumentaba que al encontrarse sus actuaciones encuadradas en sus respectivas normas internas y reservadas, no podría hacerse un reproche de su conducta. La Corte Suprema, conociendo de estos hechos mediante recurso de casación, rechazó las alegaciones de los condenados, argumentando que el cumplimiento de dichas órdenes no transforman en lícitas actuaciones que no lo son[147]. Lo comentado recientemente sustenta nuestra postura inicial, en el sentido de que ninguna orden interna puede

[146] EL MOSTRADOR, "Agente de contrainteligencia estaría tras robo en consulado argentino", Santiago, 10 de noviembre de 2003 disponible en línea [http://goo.gl/Whb7uS] [Consulta: 15 de noviembre de 2013]

[147] CORTE SUPREMA, Sentencia Rol C – 5059 – 2005, 30 de enero de 2007 [Disponible en línea: http://goo.gl/usiU92] [Fecha de consulta: 15 de noviembre de 2013]

ampliar las competencias que por definición, sólo pueden establecerse en la ley.

### 3.4. Los métodos especiales de obtención de información.

Los llamados "métodos especiales de obtención de información", establecidos en el título V de la ley 19 974, requieren de la aquiescencia de una autoridad jurisdiccional por su especial impacto en la intimidad de las personas investigadas. De la tramitación de la ley, puede establecerse que su relevancia fue especialmente tenida en cuenta. Así, por ejemplo, se estableció en la discusión en sala que: "Jamás una autoridad administrativa, bajo ninguna circunstancia, podrá, por sí y ante sí, tomar una medida que importe el levantamiento del derecho a la intimidad y a las comunicaciones. Siempre será la decisión judicial, de una manera tipificada en el proyecto y en la Constitución, la que establezca, bajo los procedimientos y normas consagradas en el proyecto, la procedencia de una alteración al derecho del resguardo pleno de las comunicaciones."[148]

[148] BIBLIOTECA DEL CONGRESO NACIONAL, 2004, Ob. Cit., p. 134.

Sin embargo, el problema de la intromisión en el derecho a la intimidad no se agota en la autorización judicial para utilizar estas técnicas: la protección de los datos personales sensibles requiere una autorización legal expresa para el tratamiento de éstos.

Los métodos especiales de obtención de información se encuentran establecidos en el artículo 24° de la ley 19 974. De su origen y tramitación puede establecerse la taxatividad de los mismos, tema que fue latamente discutido en la tramitación de la ley[149]. Estos son:

3.4.1. La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas.

[149] El proyecto original, en su artículo 28º, no establecía una lista taxativa de métodos especiales de obtención de información: "Para los efectos de la presente ley, se entiende por técnicas intrusivas y métodos encubiertos aquellos procedimientos que, en base a la simulación, la disimulación, la observación o la tecnología, permiten acceder a información contenida en fuentes cerradas. En particular, constituyen técnicas intrusivas y métodos encubiertos, entre otros, los siguientes: intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; escucha y grabación electrónica; allanamiento encubierto, levantamiento del secreto bancario, e intervención de sistemas y redes informáticas." BIBLIOTECA DEL CONGRESO, 2004 Ob. Cit., Pág. 21. Durante la tramitación en la Comisión de Defensa Nacional, una indicación de los diputados Bauer, Bertolino, Burgos, Cardemil, Errázuriz, Ibáñez, Leal y Ulloa, se decidió por que los métodos se establecieran de manera taxativa.

Frente a este método, debe mencionarse que la expresión "Intervenir", según la RAE, corresponde a "Espiar, por mandato o autorización legal, una comunicación privada"[150]. A su vez, "intervenir" proviene de la voz latina "*intervetio*" que implica "interponerse" o "venir entre". Es decir, la expresión coloca al cuerpo en una postura intermedia entre emisor y receptor de las comunicaciones, ideal para conocer el contenido y cantidad de éstas. Vera, al comentar esta norma, interpreta que la autorización se refiere tanto al contenido como a la cantidad de éstas. Puede ser tan importante el saber qué fue lo hablado como la cantidad de veces que se hizo.[151]

Para realizar estas actuaciones, los terceros, operadores de servicios de telecomunicaciones, deben sujetarse a las directivas establecidas en el Decreto Supremo N° 142, del 2005[152], que establece la obligación de ceñirse estrictamente por los marcos de la orden judicial en ese sentido.

[150] Diccionario de la Real Academia Española [en línea] [consulta: 10 octubre de 2013] disponible en internet: [http://lema.rae.es/drae/?val=intervenir]
[151] VERA, Ob. Cit., p. 224
[152] CHILE, Ministerio de Transportes y Telecomunicaciones, 2005, Decreto Supremo N°142/2005, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación, 22 de septiembre de 2005.

3.4.2. La intervención de sistemas y redes informáticos

Cabe precisar que estas medidas sólo podrán ser utilizadas cuando el servidor que se solicita intervenir se encuentre en el territorio nacional.

3.4.3. La escucha y grabación electrónica incluyendo la audiovisual.

Para Vera, en este acápite se comprenden la captación de sonidos o filmación a larga distancia, sin precisar tales conceptos, que deberán ceñirse estrictamente a los casos en que se produzca una real y efectiva afectación del derecho a la privacidad[153]. Parece ser adecuado que los órganos de inteligencia deben limitarse estrictamente a lo establecido en la decisión judicial, la que deberá emitirse teniendo en cuenta siempre el principio de proporcionalidad que justifique la utilización de estas medidas.

3.4.4. La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

[153] VERA, Ob. Cit., p. 228.

Esta medida, de clausura, fue agregada por el senador Fernando Cordero en el Segundo Informe de la Comisión de Defensa Nacional, con el objeto de prever que futuros desarrollos tecnológicos volvieran obsoleto el desarrollo de este artículo.[154]

3.4.5. Requisitos para la utilización de métodos especiales de obtención de información.

Junto con la tutela judicial ya mencionada, debemos señalar que la propia ley 19 974, en su título V, establece los parámetros sobre los cuales deben operar dichas medidas.

3.4.5.1. Cuando determinada información sea estrictamente indispensable para el cumplimiento de los objetivos del Sistema.

Al establecer estas medidas, se buscó dotar de contenido y profundidad al principio de proporcionalidad, establecido como uno de los principios que informan la presente legislación. Lo que se busca mediante esta exigencia es que los métodos especiales de obtención de información se transformen en la *ultima ratio* del proceso de inteligencia. Con respecto a

[154] BIBLIOTECA DEL CONGRESO NACIONAL, 2004. Ob. Cit., p.296.

los objetivos, nos remitiremos a lo expuesto anteriormente respecto de la competencia del sistema.

3.4.5.2. Cuando la información necesaria no pueda ser obtenida de fuentes abiertas.

La expresión utilizada por la ley merece comentarios. En primer lugar, se extraña una definición legal que precise los alcances de la frase "fuentes abiertas". Al respecto, la doctrina nacional[155] la hace extensiva a datos que son de libre acceso a todas personas, como la información contenida en la prensa. La intención del legislador ignora la problemática de usar una categoría establecida en la LPDP, llamada "fuente accesible al público". Como ya hemos mencionado, la utilización de los datos provenientes de dichas fuentes, sólo pueden ser utilizados cuando éstos se adecúen a los supuestos establecidos en la propia ley, en su artículo 4°.

Luego, y lo que nos parece mucho más complejo, la propia ley entiende sus funciones de acceso a los datos, sin importar su naturaleza o sensibilidad. Sin embargo, al hablar de "procedimientos especiales de

[155] VERA, Ob. Cit., p. 214

obtención de información", la ley es clara en establecer que la autorización judicial se refiere sólo al método utilizado para acceder a los antecedentes que antes se encontraban vetados a su conocimiento; incidiendo en este caso en una limitación legítima del derecho fundamental a la inviolabilidad del hogar y de toda forma de comunicación privada contenido en el artículo 19º nº 5 de la Constitución, sin aludir en ningún caso al tratamiento propiamente tal de los datos obtenidos por estas actividades. La distancia conceptual entre los cuerpos legislativos de inteligencia y protección de datos personales favorece estas discusiones; mientras que desde la óptica de inteligencia, la autorización al método de acceso transforma una fuente cerrada en abierta, permitiendo un tratamiento ilimitado de los datos allí contenidos; la irrupción de la protección informática limita el ámbito de una actividad que desde la doctrina tradicional de inteligencia no tenía reparos. Ahora, los conceptos de "fuentes abiertas" o "fuentes cerradas" sucumben a expresiones como "fuentes accesibles al público", "datos personales" o "datos sensibles", pues la LPDP permea a todo el ordenamiento jurídico en su conjunto, sin más límites que los establecidos en la ley. Bajo esta perspectiva, y en la línea de lo tratado en el capítulo segundo, el libre acceso a fuentes que en principio estaban retiradas del ámbito permitido a

los órganos de inteligencia, no contamina a la información resguardada en ellas, por lo que mantiene intacta su propia naturaleza. Así, los datos sensibles conservan su reforzada protección otorgada por el artículo 10° de la LPDP, estando obligados los órganos de inteligencia a omitir su análisis, a menos que una norma expresa, no existente actualmente en nuestra legislación, se lo permita.

Como la propia ley 19 974 establece de manera taxativa cuáles son los métodos especiales de obtención de información, nos encontramos en capacidad de señalar que ésta no se hace cargo del concepto de vida privada e intimidad, y no incluye dentro de ésta la moderna concepción de autonomía informativa, que incluye "el derecho del individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal."[156]Al no hacerse cargo de esta idea, entonces podemos ver cómo quedan fuera del régimen de control judicial hechos o antecedentes que no necesariamente puedan encontrarse en el ámbito cerrado del hogar y de las comunicaciones e

[156] CERDA, Alberto, 2012, Ob. Cit., p. 7.

igualmente pueden afectar los derechos establecidos dentro de lo que la doctrina considera como su núcleo esencial.

3.4.5.3. Tienen por objetivo resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico.

Para Vera[157], existen dos posibilidades de interpretación de esta norma. En primer lugar, sólo existirían como presupuesto de acción el enfrentarse a las amenazas del terrorismo, el crimen organizado y el narcotráfico cuando estos hechos afecten la seguridad nacional. Para otra opción de interpretación, aparte de los hechos mencionados en la ley, se agrega la causal de "resguardo a la seguridad nacional". Frente a esta última opinión, que parece la más acertada de acuerdo a lo establecido como principios de la legislación, cabe sin embargo, realizar una apreciación: en cuanto a la seguridad nacional, valga lo dicho anteriormente al señalar la porosidad del concepto, y cómo su determinación queda inicialmente entregada a la mera definición administrativa; serán, por tanto,

[157] VERA, Ob. Cit., p. 215

los tribunales de justicia, al otorgar las autorizaciones correspondientes, los que deberán proveer de contenido y sentido al concepto aplicable.

3.5. La autorización judicial de los métodos especiales de obtención de información.

De acuerdo a lo establecido precedentemente, los objetivos buscados mediante la utilización de los métodos especiales de obtención de información, sobrepasan el límite establecido por la Constitución en su artículo 19 N° 5, es decir, la inviolabilidad de las comunicaciones, por lo que es la ley, por expreso mandato constitucional, la que establece el procedimiento debido para su legítima utilización. La doctrina nacional ha sido concordante en señalar que las normas que limiten este derecho deben encontrarse establecidas de forma clara en la Ley, perseguir fines legítimos, adoptadas por autoridades competentes, y ajustadas razonable y proporcionalmente[158]. Es por esto que se requiere en nuestro ordenamiento jurídico, la autorización judicial. En este caso será competencia del Ministro

[158] NOGUEIRA, Humberto, 2007, Derechos Fundamentales y Garantías Constitucionales, Santiago, Librotecnia, Tomo I, p. 456, citado en VERA, Ob. Cit., p. 213.

de la Corte de Apelaciones donde se realizará la diligencia, el otorgar la autorización de estos métodos.

Si bien dichas medidas ya se encuentran contenidas en otros cuerpos normativos[159], Vera nos recalca que en este caso la autorización presenta diferentes características[160]. En primer lugar, la autorización no recae sobre una gestión jurisdiccional, puesto que los antecedentes (al menos en teoría) no tendrán una relevancia procesal[161]. La misma Corte Suprema mantuvo esa tesis durante la tramitación de la ley, como argumento para informar desfavorablemente el entonces proyecto[162]. Luego, la propia presencia de la autorización judicial ha sido puesta en duda, dadas las complejidades de la

[159] Así, por ejemplo, los arts. 218°, 222°, 226° de Código Procesal Penal, regulan la retención de correspondencia, la interceptación de comunicaciones y otros métodos intrusivos no establecidos expresamente, sujetándolos a la anuencia del Juez de Garantía que conoce de la causa, mientras que el art. 14 N°3 de ley 18 314 permite éstos métodos durante la investigación de conductas terroristas, similar a lo regulado en el art. 24° de la ley 20 000, con respecto a los delitos relacionados con el tráfico ilícito de estupefacientes y sustancias sicotrópicas.

[160] VERA, Ob. Cit., p. 222

[161] Esta es una faceta más de la extraña naturaleza del sistema de inteligencia, y sobre el que recaen no pocas dudas: su vaciamiento hacia eventuales procesos judiciales, con el objeto de buscar las responsabilidades correspondientes. En efecto, del entramado de normas sobre el silencio de los actos de las agencias de inteligencia, no se ha establecido un conducto sobre la cual dicha información pueda ser transmitida al Ministerio Público, órgano con el mandato constitucional privativo de la investigación de los hechos constitutivos de delito, ni acerca de cómo puede hacerse valer en un juicio, así como tampoco sobre cuál será el efectivo valor probatorio de la misma.

[162] "[Del proyecto de ley] aparece que la actuación de la judicatura no está enmarcada en un proceso de carácter judicial, que tienda a investigar la comisión de un hecho que revista los caracteres de delito y, por lo mismo, como no tiene carácter jurisdiccional la actividad consistente en conceder o denegar la autorización que solicite el Director o Jefe del Servicio de Inteligencia" CORTE SUPREMA, Oficio N°2927, 30 de noviembre de 2001

naturaleza de la misma: al ser un procedimiento reservado, la obligación de fundamentar las sentencias "se ve destruida frente al secreto impuesto por la ley: la ciudadanía no puede comprobar si sus magistrados, en teoría garantes de la manifestación soberana de aquella, han actuado o no con sujeción a la ley y a las garantías constitucionales consagradas por la carta fundamental"[163]. Además, la propia naturaleza no contenciosa del procedimiento (al no existir una contraparte que pueda realizar efectivamente sus descargos) no establece la posibilidad de plantear recursos en contra de la resolución. Sólo se encuentra contemplado el recurso de reposición a favor de quien solicita las medidas -los directores de los servicios- y para el exclusivo caso de que éstas sean denegadas.

Finalmente, no podemos dejar de mencionar las dudas que suscita en algunos autores la posibilidad de revisar jurisdiccionalmente la adecuación de medidas impuestas por el ejecutivo, como señala Santaolalla: "Pero el Estado de Derecho no ha encontrado más remedio que el que deriva de la legitimidad de un Gobierno democrático y del conjunto de controles

[163] MEDINA, Nicolás, 2012, Procedimientos especiales de obtención de información: Análisis del título V de la ley Nº 19.974 y algunas consideraciones pertinentes a la protección de derechos fundamentales, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, p. 86

institucionales, entre los cuales los políticos del Parlamento. Habrá de presumirse que un Gobierno salido directa o indirectamente de las urnas será sensible con los derechos y libertades constitucionales, y que no impondrá otros sacrificios que los estrictamente necesarios derivados del interés general. Si no se comporta así, podrá ser despojado de su condición a través de los oportunos cauces constitucionales". [164] No podemos concurrir con la idea expuesta precedentemente. En nuestro ordenamiento jurídico la defensa de los derechos reconocidos por la Constitución, se encuentra entregada a los Tribunales de Justicia, a través de los mecanismos establecidos en ella misma: las facultades conservadoras[165]. La utilización de una salvaguarda frente a los derechos infringidos se hace aún más patente en el ámbito de inteligencia, al ser los procedimientos secretos, y por lo mismo, fuera de todo alcance del afectado para realizar sus descargos y defensas. Parece adecuado adoptar como propio el voto de minoría de la misma Corte Suprema al informar desfavorablemente el proyecto: "por estimar que es necesario que la autoridad judicial tutele las garantías

[164] SANTAOLALLA, Fernando, 2002, Actos Políticos, Inteligencia Nacional y Estado de Derecho, en: Revista Española de Derecho Constitucional, N°65, Centro de Estudios Políticos y Constitucionales, Madrid, mayo – agosto, 2002. p 111.

[165] Vid. KOMPATZKI, Daniela, 2004, El recurso de protección y las denominadas facultades conservadoras de los Tribunales de Justicia, Valdivia, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad Austral de Chile.

consagradas en la Carta Fundamental, evitando, de esa manera, que quede radicada exclusivamente en la autoridad administrativa, la facultad de usar las denominadas técnicas intrusivas o métodos encubiertos, lo que podría devenir en arbitrariedades."[166]

3.6. Tratamiento de datos sensibles por parte de los organismos de inteligencia.

Dentro de las disposiciones contenidas en la ley 19 974, conviene detenerse en lo preceptuado en el artículo 8°[167], que establece las funciones

[166] Voto de minoría de los ministros señores Garrido, Ortiz, Tapia, Cury, Álvarez H. y Kokisch. CORTE SUPREMA, Ob. Cit.

[167] Artículo 8º.- Corresponderán a la Agencia Nacional de Inteligencia, en adelante la Agencia, las siguientes funciones:
a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República.
b) Elaborar informes periódicos de inteligencia, de carácter secreto, que se remitirán al Presidente de la República y a los ministerios u organismos que él determine.
c) Proponer normas y procedimientos de protección de los sistemas de información crítica del Estado.
d) Requerir de los organismos de inteligencia de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad Pública, así como de la Dirección Nacional de Gendarmería, la información que sea del ámbito de responsabilidad de estas instituciones y que sea de competencia de la Agencia, a través del canal técnico correspondiente. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados.
e) Requerir de los servicios de la Administración del Estado comprendidos en el artículo 1° de la ley Nº 18.575 los antecedentes e informes que estime necesarios para el cumplimiento de sus objetivos, como asimismo, de las empresas o instituciones en que el Estado tenga aportes, participación o representación mayoritarios. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados, a través de la respectiva jefatura superior u órgano de dirección, según corresponda.

de la ANI, y para algunos, aplicable extensivamente a los demás órganos del Sistema[168]. Nos detendremos únicamente, por ser atingentes a la problemática del tratamiento de datos sensibles, en las disposiciones contenidas en las letras a) y e).

"Corresponderán a la Agencia Nacional de Inteligencia, en adelante la Agencia, las siguientes funciones:

a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República."

Con respecto a esta función, cabe precisar que de acuerdo a lo establecido en el artículo 2° letra o) de la LPDP, tanto "recolectar" como "procesar" corresponden a "tratamiento" de datos personales. Vera,

---

f) Disponer la aplicación de medidas de inteligencia, con objeto de detectar, neutralizar y contrarrestar las acciones de grupos terroristas, nacionales o internacionales, y de organizaciones criminales transnacionales.
g) Disponer la aplicación de medidas de contrainteligencia, con el propósito de detectar, neutralizar y contrarrestar las actividades de inteligencia desarrolladas por grupos nacionales o extranjeros, o sus agentes, excluyendo las del inciso segundo del artículo 20.
CHILE. Ley 19 974. Ob. Cit.

[168] Véase nota N° 138.

comentando dichas atribuciones, establece la potestad de la ANI para efectuar todo tipo de tratamiento de datos personales, incluso los sensibles: "Muchas veces las organizaciones de inteligencia recopilan información y analizan situaciones en que hay involucrados 'datos personales' o 'datos sensibles."[169] Sobre esta afirmación cabe hacer un análisis más detallado. No nos parece clara la autorización que el autor efectúa con respecto a los datos sensibles. Como hemos visto, la autorización para efectuar tratamiento de este tipo especial de datos requiere para su procedencia la autorización de la ley, la que debe encontrarse explicitada de manera que no deje lugar a dudas de su intención y alcance. Llevado al caso en particular, la norma parece remitirse de manera genérica al tratamiento de datos personales, por lo que su interpretación no puede extenderse, a primera vista, a los datos sensibles. La tendencia legislativa actual tiende a establecer excepciones expresas respecto de datos sensibles, como en el caso de los relacionados a los estados de salud de su titular. Así, podemos encontrar el artículo 127° del Código Sanitario[170], modificado por la misma

[169] VERA, Ob. Cit., p. 162.

[170] Art. 127. (…) Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. (…)

LPDP; y la dictación de la ley 19970, que Crea el Sistema Nacional de Registro de ADN, el que en su artículo 3° establece la característica de sensible, de los datos que se ingresen a su registro[171]. De este modo, creemos que Vera confunde dichas categorías, ignorando la distinción entre estos tipos de datos, que, como ya hemos mencionado, no es trivial para la ley.

e) Requerir de los organismos de inteligencia de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad Pública, así como de la Dirección Nacional de Gendarmería, la información que sea del ámbito de responsabilidad de estas instituciones y que sea de competencia de la Agencia, a través del canal técnico correspondiente. Los mencionados organismos estarán obligados a suministrar los antecedentes e informes en los mismos términos en que les sean solicitados.

Al comentar la presente norma, Vera[172] adopta una postula permisiva, al establecer que la obligación de los organismos públicos sólo está limitada por los casos en que expresamente se encuentra prohibida la comunicación

[171] Artículo 3º.- Naturaleza de los datos y su titularidad. La información contenida en el Sistema y, en particular, las muestras biológicas y las huellas genéticas, se considerarán datos sensibles de sus titulares, según lo dispuesto en la ley Nº19.628, sobre protección de la vida privada.
[172] VERA, Ob. Cit., p. 164

de dichos datos. Frente a esta función, no establece diferencias respecto de la calidad de sensibles o no de los datos solicitados.

Nos mantenemos en abierta contradicción frente a esta solución. Como hemos establecido anteriormente, el tratamiento de datos sensibles se encuentra especialmente protegido, por lo que su procesamiento debe ~~de~~ ceñirse precisamente a alguna de las hipótesis del artículo 10° de la LPDP. En concreto, tal como ha mencionado el Tribunal Constitucional, la técnica legislativa debe utilizarse de una manera que, en tanto "…regulen el ejercicio de estos derechos, [debe]n reunir los requisitos de 'determinación' y 'especificidad'. El primero exige que los derechos que puedan ser afectados se señalen, en forma concreta, en la norma legal; y el segundo requiere que la misma indique, de manera precisa, las medidas especiales que se puedan adoptar con tal finalidad".[173] [174] En este sentido, Cordero

[173] CORDERO, Luis, 2009, Video vigilancia e intervención administrativa: las cuestiones de legitimidad, en: ARRIETA, Raúl y REUSSER, Carlos (coordinadores), 2009, Chile y la protección de datos personales. ¿Están en crisis nuestros derechos fundamentales?, Santiago, Ediciones Universidad Diego Portales, p. 87.

[174] En el mismo sentido se pronuncia la sentencia 198-94 del mismo tribunal, al establecer como inconstitucional la facultad entregada al Consejo de Defensa del Estado de investigar sin más limitantes los hechos y antecedentes que pudiesen constituir delito: "[la ley analizada] no contempla en forma íntegra, completa y exacta el procedimiento ni los casos precisos como debe aplicarse, pues se refiere a situaciones absolutamente discrecionales, en las que deben actuar los funcionarios del servicio autorizado para recoger e incautar la documentación y los antecedentes probatorios y objetos que estimen necesarios para la investigación. Es decir, al no especificarse

establece los criterios que debe reunir una ley para facultar a una autoridad administrativa a realizar actos que puedan afectar derechos fundamentales[175]:

a) La insuficiencia de remisión a la habilitación constitucional por parte de la ley, puesto que la medida autorizada no puede afectar los derechos en su esencia;
b) La necesidad de fijar pautas objetivas en la intervención, siendo insuficiente la remisión a las normas reglamentarias;
c) La Intervención siempre debe de estar sujeta a control;
d) El Control heterónomo, siempre debe estar reservado al juez, siendo insuficiente el autocontrol administrativo y;
e) Debe existir la posibilidad real de reacción o defensa frente a dichas medidas.

De la doctrina analizada, podemos entonces concluir que dichos estándares no son alcanzados en la ley en comento, puesto que de algunos

---

el procedimiento y no señalarse los casos precisos en que las medidas proceden, se está vulnerando la inviolabilidad de las comunicaciones y documentos privados, que sólo pueden interceptarse, abrirse o registrarse en los casos y formas determinadas por la ley". Tribunal Constitucional, Sentencia Rol 198-94.

[175] CORDERO, Ob. Cit., p. 88

articulados aislados y genéricos, no podemos inferir la autorización para tratar los datos sensibles. La autorización judicial, como ya vimos, sólo procede en ciertos casos taxativamente establecidos por el legislador, y su utilidad resulta insuficiente para la necesidad de adecuación con el resto de la legislación de protección de los datos personales, puesto que la resolución judicial sólo versa sobre el uso de los métodos, y no puede subrogar la ausencia de la autorización expresa requerida por el artículo 10° de la LPDP para el tratamiento de datos sensibles.

Las posibilidades otorgadas por esta competencia son bastante amplias en consideración a lo anteriormente expuesto. Como ejemplo, la Dirección General de Bibliotecas, Archivos y Museos, en su reglamento, establece la obligación de las bibliotecas de llevar un registro de los usuarios con su nombre, domicilio, obras retiradas en préstamo, fecha de retiro y fecha de devolución[176]. Dicho reglamento no establece prohibición alguna de comunicación de los datos involucrados. A través de una solicitud de los hábitos de lectura de una persona, pueden establecerse parámetros que den indicios, o que finalmente, revelen características íntimas de una

[176] MINISTERIO DE EDUCACIÓN PÚBLICA, Decreto 6234, Reglamento para la Dirección General de Bibliotecas, Archivos y Biblioteca, 30 de enero de 1930, art. 82°.

persona, como sus preferencias políticas, ideológicas o sexuales. Dicho tratamiento de datos sensibles incide directamente sobre la privacidad e intimidad de las personas objeto de dichas medidas, lo que ilustra los riesgos involucrados en seguir la línea de argumentación sugerida por Vera. A nuestro parecer, el organismo público enfrentado a dicha solicitud, debiese negar la comunicación de la información sensible contenida en sus registros, tanto por vulnerar el principio de finalidad, como por carecer, de fundamento legal el órgano requirente, de fundamento legal de la norma expresa que lo habilite a tratar, y específicamente a requerir, datos sensibles, en los términos del artículo 10° de la LPDP.

Finalmente, no podemos dejar de mencionar las situaciones en las cuales, la mera recolección de datos supuestamente inocuos pueden ser contrastados con otros que aparentemente tienen esa misma calidad, para lograr una visión más completa de la esfera íntima de un individuo. Es lo que en la doctrina se denomina "teoría del mosaico"[177], que entre nosotros,

[177] La "Teoría del Mosaico" fue formulada inicialmente por Fulgencio Madrid Conesa, en su obra "Derecho a la intimidad, informática y Estado de Derecho". Ha sido utilizado como una elaboración del concepto de "vida privada" e "intimidad". Más allá de una mera dimensión negativa, tal como una inhibición de intromisión, una concepción moderna habla de una participación y control del sujeto pasivo para controlar y permitir la comunicación al exterior de sus propias características. "Quizá lo que es relativo es lo público, con la consecuencia de que

Nogueira, asevera que “En el concepto de vida privada se incluyen también datos que, a primera vista, pueden ser irrelevantes desde la perspectiva de protección de la privacidad de la persona, pero que, en conexión con otros datos, que también pueden ser aislados, de carácter irrelevante, considerados en su conjunto pueden hacer totalmente transparente la personalidad de un individuo”[178]. Es claro entonces, que se hace patente la necesidad de mostrar una regulación coherente con la protección de los datos personales, tanto en lo referente al derecho a la autodeterminación informativa, como en especial al derecho a la intimidad, en tanto la sensibilidad del dato muchas veces se hace evidente *a posteriori* a través del cruce de información.[179]

### 3.7. Legislación comparada

---

hay ciertos datos públicos que pueden tener una trascendencia para la intimidad si se conectan entre sí. Se produciría una suerte de metamorfosis que convierte los datos públicos en privados o íntimos.” RUIZ, Carlos, 1994, En torno a la protección de los datos personales automatizados, Revista de Estudios Políticos (84): 237-264, p. 243.

[178] Nogueira Alcalá, Humberto, 2001, El Derecho de Declaración, Aclaración o de Rectificación en el Ordenamiento Jurídico Nacional. Ius et Praxis, *7*(2), 327-356.

[179] En este sentido, la ley uruguaya de protección de datos dispone expresamente que “Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. URUGUAY, 2008. Ley 18.331. Protección de datos personales y acción de “habeas data”. Art. 18 Inciso 3º.

Finalmente, nos detendremos en forma breve en la regulación comparada, principalmente en la argentina y española, para observar cómo dichos países han abordado la extensión de las atribuciones de los organismos de seguridad e inteligencia, con respecto al tratamiento de datos personales en general, y en particular, a la posibilidad de realizar operaciones con los datos sensibles.

### 3.7.1. Argentina:

El artículo 4° de la ley 25 520, de Inteligencia Nacional, proscribe, en su número 2° "obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción"[180]. Pese a que el título II de dicha ley, tal como en nuestro país, enmarca el funcionamiento del Sistema de Inteligencia Nacional a la

[180] ARGENTINA, 2001, Ley 25 520 Ley de Inteligencia Nacional, diciembre de 2001.

Constitución y a las leyes argentinas[181], nos encontramos con una norma adicional, que establece los parámetros específicos de la actuación de éste, y deja fuera de dudas la improcedencia del tratamiento de datos sensibles por parte de éstos, cuando versen solamente sobre aquellos.

3.7.2. España:

La Ley Orgánica 15/1999[182] prescribe, respecto de los ficheros de las Fuerzas y Cuerpos de Seguridad, en su artículo 22°: "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán

[181] En particular, el artículo 23° N° 2 de la ley N° 25326, Protección de datos prescribe que: "El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad." Vid. N°124

[182] ESPAÑA, Jefatura de Estado, 1999, Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 14 de diciembre de 1999.

clasificarse por categorías en función de su grado de fiabilidad". Nuevamente nos encontramos con una regulación a nivel de tratamiento de datos personales que otorgan un marco legal de referencia y establecen los controles a que deberán sujetarse dichos órganos, que en el caso de los llamados datos "especialmente protegidos", en su número 3 del mismo artículo citado prescribe que "La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales."[183]

### 3.7.3. Estados Unidos

Promulgada el 26 de octubre de 2001, poco después de los atentados terroristas en Nueva York y Washington del 11 de septiembre, la USA

[183] Ibíd.

PATRIOT ACT (por sus siglas en inglés[184]), establece diversas provisiones destinadas al fortalecimiento de los controles de seguridad de una nación que buscaba respuestas efectivas después de dichos ataques.

Se consideraron variadas extensiones de legislaciones previas[185], realzando la búsqueda de eficacia en la obtención de información. Entre sus previsiones más importantes, se encuentra la sección 215[186], que modifica la FISA Act de 1978, autorizando al gobierno la obtención de cualquier "cosa tangible", incluso sin sospecha razonable de que dicha información pueda conectarse directamente con actividades terroristas. Entre las críticas a lo regulado, se encuentra la vaguedad y amplitud de las bases de datos que pueden ser registradas, la que ha sido comúnmente llamada "sección de librería".

---

[184] "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001"*, en español, "Acto del 2001 uniendo y fortaleciendo América proveyendo las herramientas apropiadas requeridas para obstruir e interceptar el terrorismo". ESTADOS UNIDOS DE NORTEAMÉRICA, Public law 107–56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 26 de octubre de 2001.

[185] Entre ellas, la *Foreign Intelligence Surveillance Act of 1978*, que permite la vigilancia electrónicas dentro de las fronteras del país, la *Electronic Communications Privacy Act of 1986*, que establece controles a la interceptación de comunicaciones y la *Bank Secrecy Act of 1970*, que obliga a los agentes financieros a colaborar con las autoridades en los casos de sospecha de lavado de activos.

[186] ESTADOS UNIDOS, ob. cit., sec. 215

Otro punto que ha sido discutido, es la provisión 206[187], que permite a los organismos de seguridad el obtener una autorización para acceder a los registros privados, sin la debida especificidad de la identidad del investigado o el lugar donde dicha actuación se llevará a cabo. Las provisiones de autorización judicial en estos casos, han sido tan debilitadas, que la provisión 216 faculta al órgano jurisdiccional a dar su anuencia a la realización de acciones de interceptación de comunicaciones en cualquier punto de la nación, sin otorgar mayores detalles. Las reducciones a los requisitos legales de esta medida de control, establecidas en su sección 218, han aumentado exponencialmente el número de autorizaciones judiciales solicitadas.[188] Otro punto, autorizado por la ley en su sección 505, es el amplio margen de acción de las llamadas "cartas de seguridad nacional", mediante las cuales los órganos de seguridad pueden requerir, sin ninguna orden judicial, a entidades u organizaciones que otorguen los antecedentes relativos a particulares, los que no podrán ser divulgados.

[187] Ibíd. sec. 206.
[188] AMERICAN CIVIL LIBERTIES UNION, Reclaiming patriotism. A call to reconsider the Patriot Act, 2009, [en línea] <https://www.aclu.org/sites/default/files/pdfs/safefree/patriot_report_20090310.pdf> [fecha de consulta: 10 de enero de 2014], p. 11.

Ha sido la sociedad civil la encargada de manifestar sus aprehensiones frente a dichas provisiones. Diversas campañas se han montado con el objetivo de lograr que las provisiones más controvertidas sean repelidas, al término de los cuatrienios de duración de la misma.[189] Recientemente, la masiva filtración de documentos pertenecientes al funcionamiento de los organismos de seguridad, y las extensivas consecuencias internacionales que ello ha significado para los Estados Unidos, ha reactivado el debate acerca de la utilidad y la legalidad de dichas medidas.[190] Así, el derrotero judicial de la inspección de la legalidad de dichas medidas ya se encuentra en camino. Mientras que en Klayman v. Obama, del 16 de diciembre de 2013[191], se reconoció que la recolección masiva de datos telefónicos por parte de la Agencia de Seguridad Nacional violaba los derechos establecidos en la Cuarta Enmienda de la Constitución de los Estados Unidos (que protege a sus ciudadanos y sus domicilios,

[189] La misma ley establece, en lo que se ha llamado la *"sunset provisión"* [provisión del ocaso], que la misma se renovará automáticamente de no mediar ley expresa que derogue sus contenidos.

[190] THE GUARDIAN, "NSA collecting phone records of millions of Verizon customers daily" Londres, 6 de junio de 2013[en línea] < http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> [consulta: 10 de enero de 2014].

[191] ESTADOS UNIDOS, United States District Court for the District of Columbia, Klayman et. al. v. Obama et. al. [en línea] <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48> [consulta: 20 de enero de 2014].

papeles o correspondencia de toda pesquisa o aprehensión arbitraria, sin una causa probable que lo justifique), en ACLU v. Clapper, dictado el 27 de diciembre de 2013, se estableció que, si bien se reunió una gran cantidad de datos, no existían evidencias que indicasen que dichos datos se utilizaron en otras materias que no fuesen el combate al terrorismo. Serán los tribunales superiores los llamados a uniformar la jurisprudencia y sentar precedentes que otorguen una mayor certeza jurídica.[192]

### 3.7.4. Unión Europea.

Como parte del Servicio Europeo de Acción Exterior, el Centro de Análisis de Inteligencia de la Unión Europea (EU INTCEN), tiene como función la producción de análisis de inteligencia, advertencias tempranas y consciencia situacional a la Alta Representante del Servicio. Dicho órgano monitorea y evalúa antecedentes globales sobre terrorismo, armas de destrucción masiva y otros peligros internacionales; actúa como punto de entrada a la Unión Europea para información clasificada, proveniente de los

[192] ESTADOS UNIDOS, United States District Court for New York, American Civil Liberties Union et. al. v. James R. Clapper et. al. [en línea] < https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf> [consulta: 22 de enero de 2014]

servicios de inteligencia civiles y de agencias de seguridad de los Estados Miembros; además de asistir al Presidente del Consejo Europeo en el ejercicio de sus funciones en el área de las relaciones exteriores.[193] [194]

Su origen puede remontarse a la nota del Secretario General del Consejo de la Unión Europea, de fecha 15 de noviembre de 2001, en donde se esbozaba la idea de la cooperación entre los diversos Estados miembros para lograr una alerta temprana de las amenazas, que en ese momento se habían manifestado en Estados Unidos, y recoger la más amplia gama de información, desde las más diversas fuentes.[195]

[193] Sin embargo, no existe, al menos públicamente, un canal obligatorio que vincule a los diversos organismos de inteligencia de los Países Miembros con respecto a la comunicación de los datos que posean en sus bases de datos. Del mismo modo, con un personal limitado a unos 21 analistas, pareciese ser que se limita a un órgano meramente asesor y consultivo. Vid. JONES, Chris, Secrecy reigns at the EU's Intelligence Analysis Centre, en: Statewatch Journal (22), enero 2014 [en línea] < http://www.statewatch.org/analyses/no-223-eu-intcen.pdf> [consulta: 15 de enero de 2014].

[194] PUBLIC UE, EU Intelligence Analysis Centre (EU INTCEN) Fact Sheet 2012 [en línea] < http://www.asktheeu.org/es/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf> [consulta: 15 de enero de 2014].

[195] CONSEJO DE LA UNIÓN EUROPEA, Report by the secretary general/high representative to the council on intelligence cooperation, 15 de noviembre de 2001 [en línea] < http://www.asktheeu.org/en/request/173/response/579/attach/4/sn04546%20re01.en01.doc> [consulta: 15 de enero de 2014].

Sin embargo, la opacidad de sus normas y funciones específicas han sido notadas por sectores, quienes señalan que no existen disposiciones concretas y públicas respecto de sus áreas de desempeño. Diversos intentos de adquirir información sobre los procedimientos adoptados han resultado en negativas por parte del organismo.

## 3.8. Ideas finales

Como hemos visto, la función de inteligencia es vital para un Estado moderno, le permite adelantarse a potenciales conflictos, y otorga una asesoría vital a las autoridades, al entregarles a éstas la información útil que necesitan para la toma de decisiones.

Debido a las complejidades de los desafíos y amenazas que enfrentan los Estados, es natural que muchas veces sea necesario el tratamiento de los llamados datos sensibles. Por su alta relevancia pública, y por los riesgos que su posible mal uso acarrearía a las personas, creemos que su regulación debe someterse a los más altos y estrictos controles. Es en este sentido que es vital la correspondencia de sus enunciados normativos a la legislación

general de tratamiento de datos, y lamentamos que la ley 19974, dictada con mucha posterioridad a la LPDP, no haya sido capaz de armonizar sus disposiciones con ésta, en especial con el requerimiento de una norma que no dejase lugar al intérprete acerca de la procedencia del tratamiento de datos sensibles.

# CAPÍTULO IV. DE LOS ORGANISMOS DE PERSECUCIÓN PENAL Y EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES

4.1. Órganos de persecución penal.

La Constitución Política de la República de Chile define el ámbito orgánico del proceso de persecución penal, destinando dicha labor a tres órganos públicos: el Ministerio Público, encargado de dirigir exclusivamente la investigación penal[196]; las Fuerzas de Orden y Seguridad, que obedecen sin más trámite las órdenes impartidas por la Fiscalía durante la investigación; y, finalmente, los Juzgados de Garantía que son los encargados de cautelar los derechos asegurados por la Constitución, estableciéndose el principio de autorización judicial previa ante toda actuación que eventualmente pueda privar, restringir o perturbar dichos derechos.

En el proceso de persecución penal será imprescindible el tratamiento de datos personales. En efecto, será necesario tratar tanto aquellos antecedentes relevantes para sustentar la acusación como aquellos que acrediten la inocencia del imputado[197]; dicha información, a su vez, será

[196] CHILE, Constitución Política. Ob. Cit., Art. 83º

[197] Corresponde al denominado Principio de Objetividad que preside la actuación del Ministerio Público. Se encuentra insinuado en la Constitución y se desarrolla específicamente en el artículo 3° de la Ley Orgánica Constitucional del Ministerio Público al establecer que los fiscales están obligados a investigar "con igual celo no sólo los hechos y circunstancias que funden o agraven la responsabilidad del imputado, sino también los que le eximen de ella, la extingan o la

almacenada en bancos de datos creados para tal efecto, que requerirán ceñirse a las normas de la LPDP. Por otra parte, podrán surgir conflictos en lo relativo a la colisión de derechos, cuando la integridad de la investigación y la publicidad de las actuaciones entre en discusión con el control de los titulares respecto de sus propios datos.

### 4.1. Antecedentes generales.

La normativa nacional de protección de datos establece un régimen reforzado de resguardo de los datos sensibles, exigiendo la existencia de una norma expresa que permita su tratamiento y sólo en tal caso, el consentimiento del titular podrá ser prescindible. Como anticipábamos, dicha norma legal debe estar construida de tal manera que no deje lugar a ambigüedades, siendo clara y precisa respecto al tipo de dato que autoriza tratar, erigiéndose como una excepción al control personal de los propios datos sensibles que dispone el artículo 10° de la LPDP. Esta cuestión es de vital importancia, pues sólo la ley puede legítimamente limitar la protección de los datos personales sensibles, desarrollo del derecho a la intimidad, y en

atenúen." CHILE. Ministerio de Justicia. 1999. Ley 19 640 Establece la ley orgánica constitucional del Ministerio Público. 15 de octubre de 1999.

este caso, afectar el control de aquellos datos que, por incidir en la esfera íntima de las personas, puedan ser utilizados para generar discriminaciones arbitrarias en su titular.

En nuestro ordenamiento jurídico, no existe una norma genérica que autorice en términos expresos el tratamiento de datos sensibles en el proceso de persecución penal como sí existe en otras legislaciones[198]. Esta ausencia de norma evidencia un problema que incide directamente en la legitimidad del tratamiento de este tipo de datos especialmente protegidos, pues su legalidad dependerá fuertemente de la importancia que le demos al artículo 10° de la LPDP en nuestro ordenamiento jurídico, por lo que: o convenimos que dicha disposición es la norma fundamental de protección de este tipo especial de datos y por tanto, queda terminantemente proscrito cualquier tratamiento excepcional sin una norma legal que le de sustento (situación que se extiende al sistema persecutorio penal); o, asumimos que

[198] En esta línea, la legislación española establece que: "la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7°, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales." ESPAÑA, Ley Orgánica 15/1999. Ob. Cit., Art. 22° apartado 3.

la restauración del orden jurídico vulnerado por la comisión de un hecho constitutivo de delito, implica la conjugación de bienes jurídicos de importancia capital que legitiman el tratamiento de dichos datos (aunque siempre en consonancia con los principios rectores del proceso). En cualquier caso, esta situación pone en evidencia la insuficiencia de la legislación de datos personales en un área tan relevante como el sistema procesal penal, donde la información es el elemento fundamental para la búsqueda de la verdad judicial, verdad que no puede ser conseguida a cualquier costo, y que en cualquier caso, debe alcanzarse respetando los derechos y garantías de todos los intervinientes.

A continuación, analizaremos independientemente cada uno de los órganos que conforman la estructura del proceso de persecución penal, sus normas de competencia y aquellas que los autoricen específicamente a tratar datos personales en general y sensibles en particular.

4.2. Ministerio Público.

El Ministerio Público o Fiscalía es un organismo autónomo [e independiente], cuya función es dirigir la investigación de los delitos, llevar

a los imputados a los tribunales, si corresponde, y dar protección a víctimas y testigos.[199] Dicha función la ejerce en forma exclusiva, por mandato constitucional.

4.2.1. Normas de Competencia.

El ámbito de competencia del Ministerio Público, por ser un órgano de rango constitucional, se encuentra en primer término, naturalmente, establecido en la propia Constitución. Sobre el particular, el inciso primero del artículo 83° preceptúa que el Ministerio Público "dirigirá en forma exclusiva la investigación de los hechos constitutivos de delito, los que determinen la participación punible y los que acrediten la inocencia del imputado y, en su caso, ejercerá la acción penal pública en la forma prevista por la ley. De igual manera, le corresponderá la adopción de medidas para proteger a las víctimas y a los testigos. En caso alguno podrá ejercer funciones jurisdiccionales." Dicha disposición es reproducida casi

[199] Esta definición funcional corresponde a la establecida en la página web de la Fiscalía MINISTERIO PÚBLICO [en línea] http://www.fiscaliadechile.cl/Fiscalia/quienes/index.jsp [consulta : 03 noviembre 2013]

textualmente en el artículo 1° de la Ley 19 640 Orgánica Constitucional del Ministerio Público.[200]

A su vez, el Ministerio Público podrá impartir órdenes directas a las Fuerzas de Orden y Seguridad Pública durante la investigación, "las que deberán cumplir sin más trámite (...) sin poder calificar su fundamento, oportunidad, justicia o legalidad."[201]

4.2.2. Tratamiento de Datos Personales por el Ministerio Público.

Los órganos y servicios públicos no requieren una normativa particular que les permita el tratamiento de datos personales con prescindencia del consentimiento de su titular, más allá de su propia norma de competencia, norma que en el caso del Ministerio Público se encuentra, como acabamos de mencionar, en el inciso primero del artículo 83° de la Constitución y 1° de su Ley Orgánica. En este sentido, el Ministerio

[200] CHILE. Ley 19 640. Ob. Cit., Artículo 1º.- El Ministerio Público es un organismo autónomo y jerarquizado, cuya función es dirigir en forma exclusiva la investigación de los hechos constitutivos de delito, los que determinen la participación punible y los que acrediten la inocencia del imputado y, en su caso, ejercer la acción penal pública en la forma prevista por la ley. De igual manera, le corresponderá la adopción de medidas para proteger a las víctimas y a los testigos. No podrá ejercer funciones jurisdiccionales.

[201] CHILE. Constitución Política. Ob. Cit., Artículo 83° inc. 3°. En similar sentido: CHILE. Ley 19 640. Ob. Cit., Art. 4°.

Público, por ser el órgano encargado de dirigir en forma exclusiva la investigación penal, está autorizado para tratar todos los datos necesarios para llevar a cabo su labor de instrucción.[202] Esta norma, que delimita el marco de acción y las atribuciones del organismo en particular, se erige como la autorización legal primaria para tratar datos personales (complementada, como ya veremos, por las normas específicas del Código Procesal Penal). La Fiscalía, no obstante, deberá en la actividad de tratamiento, además de respetar los principios del proceso, acatar toda la normativa de protección de datos, especialmente en lo referido a los principios de finalidad, de acceso a la información y de no discriminación arbitraria, dejando por tanto, indemne la protección reforzada de los datos sensibles, los que sólo podrán ser tratados cuando exista autorización legal expresa en tal sentido, con las precisiones que abordaremos más adelante, asegurándose que la información personal se procese sólo cuando sea necesaria y pertinente para la actividad investigativa.

No existe normativa específica en la legislación chilena que regule la actividad de tratamiento de datos que efectúa el Ministerio Público en el

[202] DINTRANS, 2007. Ob. Cit., p. 92.

ejercicio de sus funciones durante una investigación penal. Sólo a través de la potestad reglamentaria de la Fiscalía encontramos un desarrollo en el Reglamento sobre procedimiento de custodia, almacenamiento y eliminación de registros, documentos y similares de 30 de enero de 2006. Este reglamento tiene aplicación exclusiva a las actividades enunciadas y respecto de todos los registros, documentos y demás antecedentes que formen parte de las investigaciones que lleve a cabo cualquiera fiscalía del Ministerio Público"[203], siendo, por tanto consistente con la competencia del órgano persecutor, estableciendo reglas referentes a las eliminación de los antecedentes recopilados en una causa, en aquellos casos en que la responsabilidad penal ha sido establecida o desestimada por sentencia definitiva ejecutoriada, o en que se haya aplicado el principio de oportunidad; a su vez, se establecen normas respecto a la conservación de los registros (en directa relación con los plazos de prescripción de los delitos investigados) en casos de archivo provisional, sobreseimiento temporal o en aquellos en que se ha decidido no perseverar en la investigación.

[203] CHILE, Ministerio Público, 2006, Reglamento sobre procedimiento de custodia, almacenamiento y eliminación de registros documentos y similares, 30 de enero de 2006, Artículo 1°.

No obstante, en su Título II, el reglamento contempla una serie de normas especiales cuya correspondencia con la normativa de protección de datos personales es, al menos, reñida. En primer lugar, otorga facultades a los Fiscales Regionales o al Fiscal Nacional para disponer un tratamiento diverso para registros de investigaciones o casos específicos atendida su importancia y relevancia, mediante resolución fundada que así lo declare.[204] A su vez, los propios fiscales a cargo de la investigación podrán, en atención a factores como la relevancia del asunto, la identidad de los presuntos involucrados, la existencia de otras investigaciones respecto de las mismas personas, el interés jurídico de la materia debatida, o en definitiva cualquiera otra razón que deberán señalar fundadamente, disponer que no sean destruidos determinados registros, documentos y cualquier otro antecedente por el plazo que establezcan o en forma indefinida, debiendo comunicar tal decisión al fiscal jefe respectivo al momento de terminar el caso. [205]

[204] Ibíd. Art. 12°
[205] Ibíd. Art. 13°

Las normas previamente citadas extienden arbitrariamente el marco de competencia del Ministerio Público al permitir el tratamiento de antecedentes que no corresponden a una investigación en curso y no se sustentan en ninguna norma legal que permita dicha actividad. La situación se agrava al otorgar el reglamento el carácter de "indestructibles" a las carpetas o documentos que correspondan a homicidios calificados y delitos terroristas. A su vez, el Fiscal Nacional podrá otorgar dicho carácter a otras carpetas o documentos mediante oficio o instructivo.[206] Que un antecedente sea "indestructible", le permitiría sobrevivir más allá del término de las investigaciones en las que fue legítimamente recopilado, facultando a su vez el tratamiento de antecedentes en ámbitos extraños a la actividad propia del Ministerio Público, lo que en cualquier caso constituiría un atentado directo a principios rectores de su actuación como serían el principio de legalidad, de objetividad o directamente al principio de inocencia como fundamento informador del proceso y parte esencial de los derechos del imputado.

[206] Ibíd.

La cotidianeidad del trabajo de la Fiscalía contempla un variado catálogo de actividades de tratamiento de datos que escapan al ámbito del citado reglamento y que desde el inicio de la reforma procesal penal, se encuentran informatizadas a través del denominado Sistema de Apoyo a los Fiscales, conocido más comúnmente como SAF, un *software* de gestión y tramitación de causas criminales diseñado por la empresa de servicios informáticos SONDA S.A. Este sistema permite administrar volúmenes ingentes de información referente a causas penales con altos grados de eficiencia y potenciando el trabajo colaborativo entre los equipos involucrados. El SAF está organizado en cinco módulos: de recepción, de asignación, de gestión, de interconexión y de custodia.[207]

El primer módulo tiene como objetivo principal mantener un registro de las denuncias que tomare conocimiento el Ministerio Público y respecto a éstas, ejecutar las siguientes operaciones: generar el rol único de causa (RUC); recibir los casos transferidos; ingresar sujetos y delitos; registrar el

[207] Un resumen detallado de las características del Sistema de Apoyo a Fiscales se encuentra en presentación elaborada en el marco de la Cuarta ronda de análisis del cumplimiento de Chile a la CICC (Comisión Interamericana contra la Corrupción). SAF, Sistema de Apoyo a los Fiscales. 2013 [disponible en línea] www.oas.org/juridico/ppt/mesicic4_chl_sist.ppt [consulta 20 de noviembre de 2013]

hecho delictual y dejar la causa disponible para asignación. Una vez ingresada esta información, el SAF facilita al Fiscal Jefe la labor de asignación y reasignación de casos a los fiscales, para luego colaborar en el desarrollo de la investigación, orientando la ejecución y control de sus actividades, permitiendo el registro de los datos que se estimen relevantes para el desarrollo del proceso penal, como por ejemplo: las diligencias, solicitudes, decisiones, constancias o citaciones; por otra parte, permite el registro de las declaraciones, la realización de consultas relativas al historial del caso, o la modificación de los datos del mismo

Paralelamente, el SAF permite proveer la funcionalidad necesaria para el registro y control de las especies y documentos asociados al caso y que estén bajo la responsabilidad de la Fiscalía (estas especies y documentos eventualmente se constituirán en medios de prueba). Permite en este apartado registrar el ingreso de una especie a custodia y sus respectivos movimientos (salida temporal, reingreso, inspección visual, salida definitiva), como asimismo consultar dichos movimientos y elaborar informes de éstos y de la especie en sí.

Finalmente, el SAF provee un canal de comunicación directo entre la Fiscalía y el Poder Judicial, y a su vez permite a fiscales y otros funcionarios autorizados efectuar consultas referentes a los datos alojados en el Sistema para obtener información relevante, facilitando además su búsqueda mediante la utilización de criterios. Asimismo, permite acceder a informes referentes a diversas categorías, como por ejemplo, los casos terminados o sobreseídos, una clasificación de los casos por tipo, etapa o delito, etc.

En definitiva, este Sistema es coherente con la búsqueda de eficacia y celeridad del proceso penal, facilitando tareas que habitualmente consumen bastante tiempo y no reportan un especial avance en la investigación. No obstante, existen ciertos problemas asociados a la configuración y utilización del SAF que merecen al menos una mención por su conflictiva correspondencia con la protección de datos personales. Podríamos agrupar estos problemas en tres categorías: temporalidad del almacenamiento, calidad de la información y eventual vulneración de los derechos del imputado.

En primer lugar, respecto al tiempo de almacenamiento de la información, el Reglamento sobre procedimiento de custodia, almacenamiento y eliminación de registros documentos y similares, establece expresamente que los antecedentes contenidos en el SAF se mantendrán almacenados indefinidamente. Dicha norma puede afectar directamente al derecho de los titulares a solicitar la eliminación de sus datos personales cuando su almacenamiento carezca de fundamento legal o se encuentren caducos. Atentaría asimismo contra el principio de finalidad el mantener datos más allá del propósito para el que fueron recogidos.

En otro orden de cosas, a principios del año 2013 se dio a conocer a la opinión pública la indagación por parte del fiscal regional de Valparaíso, Pablo Gómez, referente a la manipulación de datos de 21 858 registros de la Fiscalía Centro Norte en el segundo semestre del año 2011. Esta manipulación consistió en "llenar masivamente mediante una función informática —y sin la autorización de los superiores, de acuerdo a la imputación— 21 mil causas con un "sin teléfono" en aquel campo en que no se contaba con un número de contacto, algo que sólo se podía hacer para las zonas rurales; y por supuestamente manipular la base de datos con la

que una empresa externa realizaría la encuesta de satisfacción de usuarios. Todo, presuntamente, para mejorar el cumplimiento de las metas internas."[208] La calidad de los datos es un elemento esencial en la actividad de tratamiento; la LPDP dispone que "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular…"[209] Situaciones como la mencionada ponen en entredicho la responsabilidad de la Fiscalía respecto al manejo de las bases de datos que en virtud de su competencia están autorizados para llevar.

Finalmente, el SAF no puede transformarse en un elemento que genere un prejuicio en los fiscales respecto de las personas por la cantidad de "pasadas" que éstas tengan en el Sistema; situación que puede repercutir negativamente en la posibilidad de optar a una suspensión condicional del procedimiento cuando no obstante no tener antecedentes penales, se

[208] URZÚA, Malú. 2013. Teléfonos ficticios: La otra manipulación de cifras en el Ministerio Público. [disponible en línea] La Segunda online. 23 de marzo, 2013. http://www.lasegunda.com/Noticias/Nacional/2013/03/832764/Telefonos-ficticios-La-otra-manipulacion-de-cifras-en-el-Ministerio-Publico [consulta: 20 noviembre 2013] Ver también sobre el particular: COMANDARI, Paula y RIVAS, S. Fiscalía en observación. [disponible en línea] Qué Pasa. 11 de abril, 2013. http://www.quepasa.cl/articulo/actualidad/2013/04/1-11548-9-fiscalia-en-observacion.shtml [consulta: 20 noviembre 2013]

[209] CHILE. Ley 19 628. Ob. Cit., Art. 9°.

encuentren registradas en el SAF, lo que atentaría directamente contra los principios de igualdad ante la ley, objetividad e inocencia del imputado.

Es, por tanto, en el Código Procesal Penal donde encontramos el desarrollo específico de la forma de tratamiento de los datos personales por parte del Ministerio Público, insinuados en la norma de competencia. La regla general se encuentra en el artículo 180°, el que dispone que "Los fiscales dirigirán la investigación y podrán realizar por sí mismos o encomendar a la policía todas las diligencias de investigación que consideraren conducentes al esclarecimiento de los hechos (...) podrán exigir información de toda persona o funcionario público, los que no podrán excusarse de proporcionarla, salvo en los casos expresamente exceptuados por la ley".[210]

El Ministerio Público, en conclusión, está facultado por mandato constitucional para tratar, en principio, toda aquella información contenida en cualquier soporte posible en el marco de una investigación penal y en el ejercicio de sus atribuciones, sin necesidad de consentimiento de su titular.

[210] CHILE, Ministerio de Justicia, 2000. Ley 19 696, Establece Código Procesal Penal. 12 de octubre de 2010. Art. 180º.

Ésta se erige como la regla general en materia de tratamiento de datos personales; no obstante, existen disposiciones fragmentadas en el ordenamiento jurídico procesal penal chileno de aplicación específica a tipos particulares de antecedentes. En tales casos, el Ministerio Público deberá ceñirse a dichas normas cumpliendo los requisitos en ellas establecidos, para poder tratar esos datos con prescindencia de autorización de su titular.

4.2.3. Tratamiento de datos sensibles por parte del Ministerio Público.

No existe en la legislación nacional una norma expresa que autorice el tratamiento de datos sensibles al Ministerio Público. Algunos autores, entendiendo la necesidad de contar con un sistema persecutorio eficaz, han concluido que la ausencia de norma no es suficiente para aseverar la existencia de una prohibición general para que el Ministerio Público pueda tratar datos sensibles, por lo que, justificando la necesidad de dicho tratamiento, han buscado dotarlo de legitimidad a través de soluciones

interpretativas.[211] Dichas soluciones buscan acomodarse a una conclusión previamente alcanzada: el Ministerio Público está facultado por nuestro ordenamiento jurídico para tratar datos personales, incluso sensibles, sin consentimiento de su titular siempre que sean "necesarios para llevar adelante la actividad investigativa que la Constitución le encomienda"[212]. Estas soluciones encontrarían el sustento en el mandato constitucional para dirigir en forma exclusiva la investigación penal otorgado al Ministerio Público y en el artículo 20° de la LPDP.

Esta disposición, ubicada en el título IV, denominado "Del tratamiento de datos por los organismos públicos" dispone que el "tratamiento de datos personales (…) sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular." Dintrans propone que la conclusión lógica en este caso, teniendo en consideración el principio de legalidad, es que los órganos del Estado están eximidos de contar con el consentimiento del titular de los datos, incluyendo sensibles, para su

[211] En este sentido se ha manifestado Dintrans al plantear que la autorización al Ministerio Público para tratar datos sensibles corresponde a una correcta interpretación de la ley. DINTRANS, 2007. Ob. Cit. p. 92.
[212] Ibíd. p. 91.

tratamiento, pues el citado artículo los autoriza para ello. En dicho tratamiento, por supuesto, deberán respetarse todos los restantes derechos y principios garantizados en la Constitución. El sustento para ello se encuentra en la norma constitucional de competencia del Ministerio Público que se erige como "criterio legitimador y límite del tratamiento de datos personales".[213]

Desde el momento que dicho órgano dirige en forma exclusiva la investigación penal, estaría facultado para el tratamiento de todo tipo de información relevante, necesaria y pertinente al esclarecimiento de los hechos. Por tanto, siempre que los datos sensibles cumplan estas características mínimas en el marco de una investigación podrán ser tratados, aunque con estricto respeto tanto a los principios informadores de la norma de protección de datos como a los propios del sistema penal, principalmente los principios de igualdad ante la ley, objetividad e inocencia.

[213] Ibíd. p.92.

A mayor abundamiento, la misma autora ha afirmado que la legitimidad del tratamiento de datos personales sensibles deriva del propio artículo 20° de la LPDP que permite a todo órgano público tratar cualquier tipo de datos sin consentimiento del titular, siempre que actúen dentro de su competencia y respetando las disposiciones restantes de la norma. Esta autorización general para tratar datos personales -incluso sensibles- para Dintrans parece ser la interpretación apropiada, pues otorga armonía a las disposiciones de la ley, resaltando el carácter especial del artículo 20° que le otorga primacía sobre el artículo 10° de la LPDP. La remisión al respeto a las normas precedentes -agrega- "sólo debe entenderse referido a aquello que no pugne con la excepción que contempla"[214]. Dicha interpretación, menciona, además iría en consonancia la resolución 45/95 de 1990 de la ONU que consagra la posibilidad de establecer excepciones a la prohibición de almacenar datos sensibles, entre otras causales, para proteger la seguridad nacional o el orden público.[215] En el mismo sentido se expresa Vera al analizar el artículo 20º, como ya señalamos en el capítulo anterior.[216]

[214] DINTRANS, 2005. Ob. Cit., p.179.
[215] Ibíd.
[216] VERA. Ob. Cit., p. 162.

En esta línea interpretativa, el resultado es un órgano persecutorio legitimado para investigar todo tipo de datos personales, sin distinción alguna, pues desde el momento que obra por mandato constitucional y dentro de sus competencias (lo que le otorgaría la autorización legal) cumple con los requisitos para actuar, por lo que el derecho a la intimidad no se vería afectado. Sin embargo, esta solución no llena el vacío que genera la ausencia de norma expresa que autorice el tratamiento de datos sensibles.

#### 4.2.3.1. Nuestra Posición.

La normativa chilena de protección de datos intenta ser coherente con la tendencia internacional de otorgar una protección reforzada al tratamiento de los datos sensibles. La LPDP plasma desde un nivel conceptual una diferencia entre los datos personales en general y los datos sensibles en particular, definiéndolos individualmente y regulándolos en disposiciones independientes, con requisitos de tratamiento asimismo específicos. Cuando el inciso primero del artículo 4°, permite el tratamiento

de datos personales (sin consentimiento de su titular) si una ley lo autoriza, dicha ley no puede considerarse como apta a su vez, para otorgar legitimidad a la utilización de información considerada como sensible, pues el artículo 10°, como ya establecimos, requiere de una ley expresa que haga referencia a este tipo de datos sin ambigüedades. Al ser una norma especial, no cabe la aplicación de autorizaciones genéricas si dichas disposiciones no hacen referencia explícita al concepto del dato sensible.

De asumir que el Ministerio Público no puede tratar datos sensibles sin consentimiento, podríamos eventualmente encontrarnos frente a un órgano ineficaz, imposibilitado de utilizar información que de acuerdo a los principios del proceso es relevante, necesaria y pertinente, cuyo maniatamiento legal le impediría utilizar datos imprescindibles no sólo para acreditar la culpabilidad del imputado, sino también para probar su inocencia. Este complejo panorama, con un órgano persecutor ineficaz imposibilitado de tratar toda la información necesaria es, sin embargo, sólo aparente. La normativa procesal penal contempla disposiciones independientes, que llenan vacíos importantes en el tratamiento de datos

sensibles de especial relevancia en una investigación. La norma es precisa, por ejemplo, respecto a los exámenes corporales[217]; la recogida de datos personales a través de la realización de estos procedimientos sólo podrá efectuarse si éstos son necesarios para constatar circunstancias relevantes para la investigación. En cualquier caso, y pese a la necesidad manifiesta de pertinencia, el consentimiento de la persona es imprescindible. Excepcionalmente, dichos exámenes podrán realizarse aun sin aprobación del sujeto, quien puede alegar temor por su salud o dignidad; en cuyo caso la norma es coherente con la legislación de protección de datos, pues establece expresamente que se requerirá autorización judicial previa emitida por el Juez de Garantía correspondiente. De esta forma, se configura una excepción precisa a la prohibición de tratamiento de datos sensibles sin consentimiento del titular.

Sigue esta línea, la recopilación de huellas genéticas (ADN), las que en términos simples, corresponden a aquella información de tal calidad que aporta exclusivamente datos de tipo identificatorio. Se encuentran reguladas en la Ley 19 970 que crea el Sistema Nacional de Registro de ADN. Esta

[217] CHILE. Código Procesal Penal. Ob. Cit., Art. 197°.

normativa es un ejemplo claro de la implementación de las directrices establecidas en la LPDP, pues toda su construcción y terminología remite directamente y sin ambigüedades a ella. En primer lugar, otorga expresamente el carácter de dato sensible a las muestras biológicas y huellas genéticas, y en general a toda información contenida en el Sistema[218]; y, luego, abundando sobre el punto anterior, el Sistema se rige por el principio de secreto y especialmente por el de no discriminación, impidiendo que éste pueda servir de base para cualquier tipo de "...discriminación, estigmatización, vulneración de la dignidad, intimidad, privacidad u honra de persona alguna."[219]

En otro orden de cosas, una de las formas de obtener información en un proceso penal es a través de comunicaciones entre órganos de la administración del Estado; concluimos con anterioridad que en el ámbito público, la regla general en materia de tratamiento de datos personales es la reserva. En el marco de una investigación penal, el Ministerio Público podrá requerir a los órganos y autoridades del Estado toda la información

[218] CHILE. Ministerio de Justicia. Ley N° 19 970 que crea el sistema nacional de registro de ADN. Art. 3°.
[219] Ibíd. Art. 2º.

que considerare relevante y pertinente para ella, aun aquella información que por ley, goce del carácter de secreto. Para esto elaborará un requerimiento de información teniendo en cuenta las prescripciones de la ley respectiva, si la hubiera, o en caso contrario, tomando las precauciones necesarias para asegurar que la información no será divulgada. Ahora, la autoridad requerida podrá oponerse a entregar la información, argumentando dicha negativa en el carácter secreto de la misma. Si este es el caso, y el fiscal considerare indispensable dicha actuación, remitirá los antecedentes al fiscal regional, quien, si es de la misma idea, solicitará a la Corte de Apelaciones respectiva que resuelva la controversia. Aun en caso de rechazo, la Corte "podrá ordenar que se suministren al ministerio público (...) los datos que le parecieren necesarios para la adopción de decisiones relativas a la investigación (...)."[220]

Afirmar tajantemente que no reconocer una autorización genérica para que el Ministerio Público trate datos sensibles es perjudicial para el sistema de persecución penal, es falso. Como hemos señalado, nuestro Código Procesal Penal está salpicado de disposiciones que permiten dicho

[220] CHILE. Código Procesal Penal. Ob. Cit., Art. 19°

tratamiento, y en todo caso, cualquier otro dato puede eventualmente ser tratado, puesto que nuestra propia Carta Fundamental nos otorga la herramienta precisa para ello: la autorización judicial previa.

La protección de datos sensibles busca, como ya hemos afirmado, cautelar el derecho a la intimidad, que pretende resguardar el control de la propia información frente a la amenaza de utilizaciones indebidas e ilegítimas por las nuevas tecnologías de la información. Como derecho fundamental que es, su protección es garantizada por la Constitución, específicamente en el marco de una investigación penal, al disponer que "...las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que esta Constitución asegura, o lo restrinjan o perturben, requerirán de aprobación judicial previa."[221]

No pretendemos afirmar que la autorización judicial previa del juez de garantía se erige como una excepción al consentimiento previo para tratar datos sensibles, pues no está establecido así en la ley de protección a la vida privada; estas excepciones son taxativas y la aprobación judicial no

[221] CHILE. Constitución Política. Ob. Cit., Art. 83. Inc. 3º.

es una de ellas. Esta situación no hace sino reforzar el escenario existente en nuestra legislación, ya que la ley de protección de datos es clara frente a la necesidad de que las excepciones se manifiesten a través de una normativa legal precisa. El hecho de no existir norma jurídica aplicable al tratamiento de datos sensibles no puede conducir a la elaboración de justificaciones *ex post* de una conclusión a la que se ha arribado con anterioridad: la de la necesidad de que el Ministerio Público pueda tratar todos los datos necesarios en una investigación para poder accionar eficazmente.

El derecho a la intimidad es un derecho fundamental como cualquier otro y merece protección tanto como los demás. Si determinados datos no legalmente excepcionados de consentimiento del titular, son necesarios, relevantes y pertinentes a una investigación penal, corresponderá al Ministerio Público solicitar al juez de garantía la autorización judicial previa, para lo que deberá fundamentar debidamente su petición respetando además los principios informadores del proceso penal. De la ponderación del juez, como órgano independiente, dependerá si el derecho a la intimidad es preciso en este caso que sucumba ante bienes jurídicos o intereses generales de mayor valor.

### 4.3. Policía de Investigaciones.

La Policía de Investigaciones de Chile (PDI) es una "Institución Policial de carácter profesional, técnico y científico, integrante de las Fuerzas de Orden, dependiente del Ministerio del Interior y Seguridad Pública, cuyo personal estará sometido a un régimen jerárquico y disciplinario estricto."[222] Entre sus funciones, la fundamental es servir de órgano auxiliar del Ministerio Público en la investigación de los delitos.

#### 4.3.1. Norma de Competencia.

La Constitución preceptúa que las Fuerzas de Orden y Seguridad "existen para dar eficacia al derecho, garantizar el orden público y la seguridad pública interior, en la forma que lo determinen sus respectivas leyes orgánicas"[223]. Cumple este mandato constitucional el Decreto Ley 2460 de 24 de enero de 1979, Ley orgánica de la Policía de Investigaciones de Chile, que establece en su artículo 4° el ámbito de competencia de la

[222] CHILE. Ministerio de Defensa Nacional. Decreto Ley 2460. Ley orgánica de la Policía de Investigaciones de Chile. Art. 1°.
[223] CHILE. Constitución Política. Ob. Cit., Art. 101.

Policía al disponer que su misión fundamental es la de "investigar los delitos de conformidad a las instrucciones que al efecto dicte el Ministerio Público, sin perjuicio de las actuaciones que en virtud de la ley le corresponde realizar sin mediar instrucciones particulares de los fiscales."

En consecuencia, la actividad de la Policía en el proceso penal se integra en dos posibles formas: la primera, acatando, como organismo no deliberante que es[224], sin más trámite las órdenes del Ministerio Público, sin poder calificarlas en forma alguna, salvo requerir la exhibición de la autorización judicial cuando sea el caso; y, la segunda, ejecutando aquellas actividades que les competan realizar por ley.

4.3.2. Tratamiento de datos personales por la Policía de Investigaciones.

La Policía de Investigaciones enfrenta el tratamiento de datos personales de diversas maneras, pero nos enfocaremos sólo en aquellas que

[224] En este sentido el artículo 83° de la Constitución señala que "la autoridad requerida deberá cumplir sin más trámite dichas órdenes [del Ministerio Público] y no podrá calificar su fundamento, oportunidad, justicia o legalidad, salvo requerir la exhibición de la autorización judicial previa, en su caso." En la misma línea el artículo 7° de la Ley Orgánica de la Policía de Investigaciones.

se realicen en el marco de una investigación penal. En este ámbito, la Policía entra en contacto con esta información a través de dos formas: actuaciones que responden a instrucciones del Ministerio Púbico y actuaciones para las que está facultada para actuar sin previa orden del fiscal. A su vez, interviene en las distintas fases del tratamiento: recopilando, almacenando, procesando y estableciendo procedimientos de eliminación de los datos que estén en su poder. Finalmente, en su relación con la INTERPOL, comunica antecedentes relevantes fuera de las fronteras nacionales. En las siguientes páginas intentaremos desglosar detalladamente cada una de estas formas de tratamiento y establecer cómo conecta la labor de nuestra Policía con la protección de los datos personales.

4.3.2.1. Actuaciones con previa orden del Fiscal en una investigación penal.

La Policía de Investigaciones, como órgano no deliberante, debe acatar sin cuestionamientos las órdenes impartidas por el Ministerio Público en el marco de una investigación penal, por lo que para efectos de la recopilación de estos antecedentes, análisis de información, realización de

las pruebas periciales que le hayan sido encomendadas, etc. se limitarán estrictamente al ámbito de las instrucciones recibidas.

4.3.2.2. Actuaciones sin previa orden del Fiscal como parte de sus facultades legales.

Estas actuaciones están contempladas principalmente en el artículo 83° del Código Procesal Penal. Las analizaremos brevemente a continuación.

a) Prestar auxilio a la víctima. Esta actuación contempla el ingreso a un lugar cerrado y su registro, sin necesidad de consentimiento expreso del propietario o encargado ni autorización judicial previa. Esta acción está justificada solo cuando las llamadas de auxilio de personas que se encontraren en el interior u otros signos evidentes indicaren que en el recinto se está cometiendo un delito;[225]

[225] CAROCCA, Alex. 2005. Manual, El nuevo sistema procesal penal. Santiago. Lexis Nexis. p. 106.

b) Practicar la detención en los casos de flagrancia, conforme a la ley. Todo esto de acuerdo a lo establecido en el artículo 130;[226]

c) Resguardar el sitio del suceso. En primer lugar se refiere a las labores de contención del recinto, evitando intrusiones que alteren o borren elementos de la escena antes de su análisis. En segundo lugar, permite la labor del personal policial experto designado por el Ministerio Público respecto a la recopilación, identificación y conservación de los elementos encontrados y que parecieren haber servido a la comisión del hecho investigado, dejando constancia de esto y de los funcionarios policiales en un registro levantado para tal objeto. De no existir personal experto, los funcionarios policiales que hubiesen llegado al sitio del suceso deberán recogerlos y guardarlos de la forma establecida y comunicarlos a la brevedad a la Fiscalía. La autorización se extiende en el caso de los delitos flagrantes cometidos en zonas rurales o de difícil acceso, a la realización inmediata de las primeras diligencias de investigación

[226] Artículo 130°. Situación de flagrancia. Se entenderá que se encuentra en situación de flagrancia: a) El que actualmente se encontrare cometiendo el delito; b) El que acabare de cometerlo; c) El que huyere del lugar de comisión del delito y fuere designado por el ofendido u otra persona como autor o cómplice; d) El que, en un tiempo inmediato a la perpetración de un delito, fuere encontrado con objetos procedentes de aquél o con señales, en sí mismo o en sus vestidos, que permitieren sospechar su participación en él, o con las armas o instrumentos que hubieren sido empleados para cometerlo, y e) El que las víctimas de un delito que reclamen auxilio, o testigos presenciales, señalaren como autor o cómplice de un delito que se hubiere cometido en un tiempo inmediato.(...). CHILE. Código Procesal Penal. Ob. Cit.

pertinentes, dando cuenta al fiscal que corresponda de lo hecho, a la mayor brevedad;

d) Identificar a los testigos y consignar las declaraciones que éstos prestaren voluntariamente, tratándose de las personas detenidas en situación de flagrancia y aquellos que se encuentren en el sitio del suceso;

e) Recibir las denuncias del público;

f) Examen de vestimentas, equipaje o vehículos. Se podrá practicar el examen de las vestimentas que llevare el detenido, del equipaje que portare o del vehículo que condujere, cuando existieren indicios que permitieren estimar que oculta en ellos objetos importantes para la investigación;

g) Levantamiento del cadáver. En los casos de muerte en la vía pública, la orden de levantamiento del cadáver podrá ser realizada por el jefe de la unidad policial correspondiente, en forma personal o por intermedio de un funcionario de su dependencia, quien dejará registro de lo obrado[227], y

f) Efectuar el control de identidad (artículo 85º).

[227] CHILE. Código Procesal Penal. Ob. Cit., Art. 90.

Sólo en estos casos las Policías pueden intervenir directamente y sin previa instrucción en la investigación de un hecho constitutivo de delito. Se buscó recientemente, la ampliación de las facultades de las policías mediante la presentación de un proyecto de ley relativo a las facultades de Carabineros de Chile y de la Policía de Investigaciones para practicar, sin orden previa, las primeras diligencias de investigación de un delito, iniciativa que no ha prosperado y que se encuentra actualmente retirada de tabla desde el 19 de junio de 2012. [228]

4.3.2.3. Etapas del tratamiento de datos.

Tomando en cuenta que la normativa de tratamiento de datos de la Policía de Investigaciones se encuentra desarrollada a nivel interno a través de órdenes generales -muchas de ellas de antigua dictación- que como tales no tienen fuerza vinculante más allá de su institución de origen, analizaremos, a través de las distintas etapas del proceso, la forma en que la

[228] BOLETÍN Nº 7.050-07. Proyecto de ley, iniciado en Moción de los Honorables Senadores señores Espina, Allamand, Chadwick, Larraín y Prokurica, relativo a las facultades de Carabineros de Chile y de la Policía de Investigaciones para practicar, sin orden previa, las primeras diligencias de investigación de un delito.

PDI se enfrenta al tratamiento de datos personales, y si esa forma cumple con los preceptos de la LPDP.

4.3.2.3.1. Recopilación.

La Policía de Investigaciones, como órgano auxiliar del Ministerio Público, recopila antecedentes en cada una de las diligencias que realiza; como tal, sólo puede accionar en el ámbito de las instrucciones que le hayan sido debidamente comunicadas, independiente de aquellas diligencias que por ley se encuentra autorizada para efectuar sin previa orden del fiscal. Dicho de otra forma, la Policía no puede, en el marco de una investigación penal, recopilar autónomamente antecedente alguno, salvo las excepciones legales, aunque en este caso con la obligación de comunicarlas inmediatamente al Ministerio Público. De esta forma y concordando el artículo 4° de su ley orgánica con el artículo 20° de la LPDP, el margen de acción de la Policía, es bastante limitado.

Si en una investigación penal la Policía recopila información como auxiliar del Ministerio Público, sólo actúa como un brazo extensivo del mismo, y por lo tanto, no puede realizar tratamiento autónomo alguno, pues

es este último el único órgano autorizado para efectuar el procesamiento de la información.

El principio de finalidad que informa la LPDP y que se encuentra consagrado en su artículo 9° dispone 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.” Si los datos son recolectados en el marco de una investigación penal y el Ministerio Público es el encargado exclusivo por mandato constitucional de dirigirla, la información sólo puede ser tratada legalmente por este órgano.

4.3.2.3.2. Almacenamiento.

Pese a lo dispuesto en el artículo 22° de la LPDP, la Policía de Investigaciones no contempla a la fecha ninguna base de datos inscrita en el registro de bancos de datos del Registro Civil. No obstante, tiene a su haber diversos registros de información personal destinados a facilitar la labor

investigativa, que se desprenden de lo establecido en su reglamento orgánico[229]. Estos son:

a. Registro de prohibiciones de ingreso y egreso de personas al territorio nacional;

b. Archivo general nacional de extranjeros, y

c. Registro general del movimiento internacional de pasajeros.

Por otra parte, si bien a nivel interno, corresponde al Departamento de Asesoría Técnica la labor de "recopilar, centralizar y procesar toda la información relativa a los delitos y los delincuentes, con el objeto de proporcionar los antecedentes que los Oficiales Policiales requieran, apoyándolos técnica y científicamente en su misión investigadora"[230], es importante determinar el real alcance de esta norma, pues, entendiendo la importancia de la Policía en el proceso de investigación, es imprescindible ahondar sobre la extensión de la autorización legal para tratar datos personales. Sobre todo si, como apunta Dintrans, citando a Lorena Cuevas: "La Policía de Investigaciones de Chile (…) mantiene un registro de datos

[229] POLICÍA DE INVESTIGACIONES. 1987. Decreto Supremo Nº 41, Reglamento orgánico de la Policía de Investigaciones de Chile.
[230] Ibíd. Art. 76º.

personales, obtenidos al cabo del cumplimiento de la labor policial que desempeñan sus funcionarios, que va desde órdenes de detención, aprehensión, arrestos, arraigos, autos de procesamientos, contraórdenes, antecedentes e informaciones obtenidas por la labor policial."[231] Por esta razón, se analizará brevemente la real procedencia, considerando la competencia de la PDI, del tratamiento de determinados antecedentes en el proceso penal.

a. Órdenes judiciales.

Dentro de las funciones de la Policía está la de llevar a cabo las medidas de coerción que se necesitaren,[232] esto como consecuencia de la facultad de nuestros tribunales, en el ejercicio de sus funciones, de ordenar directamente la intervención de la fuerza pública como auxilio para el cumplimiento de las actuaciones ordenadas y la ejecución de las resoluciones dictadas.[233] Dentro de estas medidas y como manifestación de ese poder coercitivo, los jueces pueden decretar la detención de ciertas personas en un proceso penal.

[231] DINTRANS, Ob. Cit. p. 116.
[232] CHILE. Código Procesal Penal. Ob. Cit., Art. 79°.
[233] Ibíd. Art. 34°.

La detención, para estos efectos, será entendida como aquella privación de libertad del imputado, y regulada dentro de las medidas cautelares personales, por el Código Procesal Penal y que, normalmente, será objeto de control judicial en virtud del artículo 132° CPP. La Constitución establece que "nadie puede ser arrestado o detenido sino por orden de funcionario público expresamente facultado por la ley y después de que dicha orden le sea intimada en forma legal."[234] Por tanto, la detención en el proceso penal, exceptuando los casos de flagrancia, debe estar precedida por una orden emitida por el tribunal, la que debe ser diligenciada por funcionarios públicos autorizados (las Policías) e intimada en forma legal.

Frecuentemente, el diligenciamiento de una orden de detención es una actuación que se agota en sí misma. Cumpliendo los requisitos establecidos en la ley, la ejecución culmina con la puesta a disposición de la persona frente al juez que dictó la orden o dejándola sin efecto por la llegada de una contraorden, caso en el que ambas deberán ser eliminadas.

[234] CHILE. Constitución Política. Ob. Cit., Art. 19° N° 7 letra c).

No existiendo autorización, más allá del contenido de la propia orden, las policías no podrán hacer un uso distinto de dicha información. Se remite en este caso al carácter auxiliar de su actuación en el proceso penal.

Sin embargo, muchas otras veces, la ubicación de la persona será imposible o se encargará la detención de condenados que se encuentran evadiendo actualmente la acción de la justicia. En ese caso, hablando de órdenes de detención vigente, el ámbito de acción se amplía pues es necesario almacenar dicha información. La promulgación de la Ley 20 593 que crea el Registro Nacional de Prófugos el año 2012, entrega la competencia exclusiva para almacenar estos datos al Servicio de Registro Civil e Identificación.[235] Las Policías, sólo se reservan un derecho de acceso garantizando la debida confidencialidad de la información.[236]

b. Prohibiciones de entrada y salida del país.

El artículo 155° del Código Procesal Penal contempla entre las medidas cautelares personales, la prohibición de salir del país, de la

[235] CHILE. Ministerio del Interior y Seguridad Pública. 2012. Ley 20 593, Crea el registro nacional de prófugos de la justicia, 22 de junio de 2012.
[236] Ibíd. Art. 7º

localidad en la cual residiere o del ámbito territorial que fijare el tribunal; por otra parte, la ley orgánica de la PDI le entrega la competencia para controlar el ingreso y la salida de personas del territorio nacional, adoptar todas las medidas conducentes para asegurar la correcta identificación de las personas que salen e ingresan al país, la validez y autenticidad de sus documentos de viaje y la libre voluntad de las personas de ingresar o salir de él, y fiscalizar la permanencia de extranjeros en el país. Dicha competencia se concretiza por la actuación de la Jefatura Nacional de Extranjería y Policía Internacional, encargada de cumplir y hacer cumplir las normas legales y reglamentarias que asignen funciones a la Institución.

Dentro de dichas funciones encontramos, entre otras, las de mantener actualizado, por medio de sistemas computacionales u otros, un registro de prohibiciones e impedimentos de ingreso y egreso de personas del territorio nacional, con el fin de dar cumplimiento a las disposiciones legales y reglamentarias sobre la materia; y dar cumplimiento a las medidas de control, traslados, abandono obligado del país, expulsión, y en general, a todo tipo de sanciones, prohibiciones e impedimentos de ingreso y egreso al país, que las autoridades administrativas, judiciales o las contraloras

apliquen en uso de sus atribuciones, dictando las instrucciones pertinentes.[237] En este caso, el reglamento desarrolla una facultad expresamente entregada a la Policía por ley, no excediéndose en sus atribuciones. En consecuencia, la Policía de Investigaciones está autorizada legalmente para tratar las prohibiciones de ingreso y salida del país, dictadas en un proceso penal, y en consecuencia almacenar dicha información mientras se encuentre vigente.

c. Antecedentes penales.

El registro de antecedentes penales se encuentra entregado al Servicio de Registro Civil e Identificación desde la dictación del Decreto Ley 645 del año 1925. Esta norma le entrega la competencia exclusiva a este Servicio para llevar el recuento de las condenas exigiendo una actividad positiva de los Tribunales de Justicia de informar las sentencias condenatorias ejecutoriadas para su inscripción. Establece a su vez una limitación de acceso, restringiendo exclusivamente el derecho a solicitarlo a los fiscales del Ministerio Público, las autoridades judiciales, policiales y de

[237] POLICÍA DE INVESTIGACIONES. Reglamento Orgánico. Ob. Cit., Art. 53º.

Gendarmería de Chile respecto a las personas sometidas a su guarda y control.

La Policía de Investigaciones por tanto no está facultada para tratar datos penales directamente, sino sólo para informarse de ellos cuando sea necesario para el ejercicio de sus actividades en la esfera de su competencia.

d. ADN.

El Sistema Nacional de Registro de ADN le corresponderá en su administración y custodia al Servicio Nacional de Registro Civil e Identificación. Este sistema tendrá carácter reservado y la Policía solo podrá tener acceso previa autorización del Ministerio Público.[238]

4.3.2.3.3. Flujo Transfronterizo de datos.

La Policía de Investigaciones representa oficialmente a Chile ante la Organización Internacional de Policía Criminal INTERPOL desde el año 1946. Este organismo busca la cooperación policial internacional dentro de

[238] CHILE. Ley 19 970. Ob. Cit., Art. 2º.

los límites impuestos por las legislaciones vigentes en los diferentes Estados y de conformidad con el espíritu de la Declaración Universal de Derechos Humanos. [239]

Como parte de INTERPOL la Policía tiene acceso a una nutrida base de datos en tiempo real a través de su Oficina Central Nacional. Esta base otorga acceso a más de 153.000 registros de conocidos criminales internacionales, personas desaparecidas y cadáveres, con sus respectivos antecedentes penales, fotografías, huellas digitales, etc. Además otorga acceso a registros de huellas digitales, ADN, información relativa a delitos relacionados a la pornografía infantil, entre otros. Por otra parte, la organización facilita el intercambio de información policial entre países.[240]

Entendiendo la limitada competencia autónoma de la Policía en lo referente a la gestión de bases de datos en el ámbito penal, su interacción con INTERPOL se encontraría supeditada a actuar siempre en el marco de

[239] POLICÍA DE INVESTIGACIONES. [en línea] http:policia.cl/interpol/portada.htm [consulta: 03 diciembre 2013]
[240] INTERPOL [en línea] http:www.interpol.int/es/Especialidades/Bases-de-datos [consulta: 03 diciembre 2013]

las instrucciones emitidas por el Ministerio Público en una investigación específica.

4.3.3. Tratamiento de datos personales sensibles por la Policía de Investigaciones.

En términos generales, como la Policía de Investigación es un órgano auxiliar, podrá tratar datos sensibles siempre que las instrucciones del Ministerio Público contemplen tal posibilidad contando además con la autorización judicial correspondiente.

Fuera de esos casos, no tiene competencia alguna. Si bien no cabe duda que todo dato personal que se encuentre en registros de la Policía de Investigaciones puede ser considerado como sensible[241], por la evidente carga que dicha información tiene sobre los derechos de intimidad y vida privada en cuanto pueden generar decisiones arbitrarias o discriminatorias en contra de sus titulares, dicha condición no es anterior a su inclusión en un registro, sino que la sensibilidad del dato, surge justamente por su ingreso a la base, por lo que no puede equipararse a aquellos datos sensibles

[241] DINTRANS. 2005. Ob. Cit., p. 178.

*per se*. En cualquier caso, la debida protección de los datos está garantizada por el carácter reservado de los mismos.

Ahora, lo anterior siempre en el caso de que la Policía de Investigaciones esté legalmente facultada para tratar datos personales autónomamente en un proceso penal, pero al ser un órgano auxiliar y estando entregado el registro de una diversidad de datos esenciales para la investigación principalmente al Registro Civil, su labor es bastante limitada. La mera existencia de normativa interna que regule el tratamiento de datos personales no garantiza en modo alguno su legitimidad, ya que al amparo de la normativa de protección de datos, y no existiendo disposición específica que autorice la utilización no sólo de datos sensibles sino de datos personales en general, y finalmente, excediendo los límites de su competencia, que restringe la dirección de la investigación al Ministerio Público y que le otorga un carácter estrictamente auxiliar, toda labor policial independiente sería ilegal.

### 4.4. Carabineros de Chile

Carabineros de Chile es una Institución policial técnica y de carácter militar, que integra la fuerza pública y existe para dar eficacia al derecho; su finalidad es garantizar y mantener el orden público y la seguridad pública interior en todo el territorio de la República y cumplir las demás funciones que le encomiendan la Constitución y la ley.[242]

4.4.1. Norma de Competencia.

La Constitución preceptúa que Carabineros de Chile integra junto con la Policía de Investigaciones, y ambas en forma exclusiva, las Fuerzas de Orden y Seguridad Publica y como tales "constituyen la fuerza pública y existen para dar eficacia al derecho, garantizar el orden público y la seguridad pública interior, en la forma que lo determinen sus respectivas leyes orgánicas." Así, y coherentemente con la exclusividad del Ministerio Público en la dirección de la investigación penal, Carabineros de Chile se erige como su auxiliar, tal como lo manifiesta su Ley Orgánica al disponer que la Institución "colaborará con los fiscales del Ministerio Público en la investigación de los delitos cuando así lo dispongan, sin

[242] CHILE. Ministerio de Defensa Nacional. 1990. Ley 18 961 orgánica constitucional de Carabineros de Chile. Art. 1º

perjuicio de las actuaciones que en virtud de la ley le corresponde realizar sin mediar instrucciones particulares de los fiscales. Deberá cumplir sin más trámite sus órdenes y no podrá calificar su fundamento, oportunidad, justicia o legalidad, salvo requerir la exhibición de la autorización judicial previa, en su caso."[243]

4.4.2. Tratamiento de Datos Personales y Datos sensibles por Carabineros de Chile.

Al igual que la Policía de Investigaciones, Carabineros de Chile enfrenta el tratamiento de datos personales en el marco de una investigación penal en dos formas: actuaciones que responden a instrucciones del Ministerio Púbico y actuaciones para las que están facultados para actuar sin previa orden del fiscal. Para los efectos de este trabajo, y siendo ambas instituciones en igual calidad auxiliares del Ministerio Público, nos remitiremos a lo establecido respecto de la Policía de Investigaciones en todo lo referente al tratamiento de datos personales y datos sensibles, salvo aquello que pugne con las propias competencias de Carabineros de Chile.

[243] Ibíd. Art. 4º

# CAPÍTULO V. DEL TRATAMIENTO DE DATOS PERSONALES SENSIBLES Y LA FIGURA DEL INFORMANTE.

5.1. Antecedentes Generales.

Una de las figuras más controvertidas existentes actualmente en el ordenamiento jurídico chileno corresponde al informante, institución emparentada íntimamente con el agente encubierto, que compartiendo muchas de sus ventajas en el apoyo a la actividad investigativa del Estado, exacerba a su vez todos sus aspectos cuestionables[244], principalmente en lo referido a la delgada línea que lo separa de la inconstitucionalidad.

Es imposible realizar una primera aproximación al concepto desmarcándose del ámbito propio del espionaje, pues es un elemento esencial del mismo. Para Sun Tzu, es esencial que un gobernante conozca las cinco clases de espías, dentro de las cuales se encuentra las que él denomina espía nativo, que se contrata dentro de los habitantes de una localidad y la que llama espía interno que se contrata entre los funcionarios

[244] Así, por ejemplo, encontramos en la prensa noticias acerca de agentes de las fuerzas de orden y seguridad involucrados en un presunto caso de apremios ilegítimos y delitos informáticos, cuya identidad se mantiene en reserva por parte de la PDI. EL MOSTRADOR, Funcionario PDI queda en prisión preventiva por torturas a secundario tras marcha estudiantil, http://www.elmostrador.cl/pais/2013/12/30/funcionario-pdi-queda-en-prision-preventiva-por-torturas-a-secundario-tras-marcha-estudiantil/?fb_action_ids=10151958478869888&fb_action_types=og.recommends&fb_source=other_multiline&action_object_map=%5B454632171307664%5D&action_type_map=%5B%22og.recommends%22%5D&action_ref_map=%5B%5D [consulta 15 de noviembre de 2013]

enemigos.[245] Ambas podemos asociarlas con la figura del informante, plasmándose así la idea de que éste, como subgénero del espionaje, existe desde el origen de la guerra, es decir del propio origen del hombre.[246] Así mientras el agente encubierto se identifica con el espía, aunque con importantes diferencias en tanto es un profesional de la búsqueda de información que siempre opera para un servicio de inteligencia[247]; el informante necesariamente es un sujeto externo vinculado a una actividad cuyo desarrollo precisa de un monitoreo constante por parte de la administración, por considerarse que constituye una amenaza a ciertos elementos esenciales de la configuración de la misma.

Ahora, la percepción de estas figuras por parte de la opinión pública es altamente dispar, pues mientras la labor del agente encubierto, o del espía en su caso, está revestida de una cierta aura de heroicidad, sobre todo para la historia escrita por el bando de los vencedores; la labor de los informantes parece estar condenada a la infamia, pues si bien su delación favorece (idealmente) la consecución de objetivos socialmente importantes,

[245] SUN TZU, El arte de la guerra. 2006. Madrid. Trotta. p. 108.
[246]HERRERA, Juan Carlos. 2012. Breve historia del espionaje. Madrid. Nowtilus. p. 17
[247]Ibíd. p. 14.

implica a su vez la traición a sus círculos íntimos; y la sociedad no tiende a perdonar la deslealtad, aun respecto a círculos ética y moralmente reprobables, condenando al sujeto a deambular cargando el peso del aislamiento, de las eventuales represalias y de la propia conciencia. Así, la labor del informante se ha visto reducida al oprobio, una vez olvidados los supuestos beneficios de su actividad. Desde la traición de Dalila en el Libro de los Jueces o la de Judas para la tradición cristiana; pasando por el incentivo a la delación impuesto por la Inquisición Española hasta las acusaciones en los Juicios de Salem; o la "caza de brujas" impuesta en Estados Unidos por el Senador Joseph McCarthy que condenó, entre los más sonados, al repudio público al director de cine Elia Kazán, por delatar a colegas involucrados en eventuales actividades comunistas. Así, hasta los más recientes casos, del ex soldado y analista de inteligencia Bradley Manning (actualmente Chelsea Manning), condenado a 35 años de cárcel y a baja deshonrosa por filtrar documentos clasificados y de Edward Snowden, ex empleado de inteligencia de la NSA y de la CIA, cuya desclasificación de documentos referentes a programas de vigilancia masiva, si bien ha causado revuelo en el ámbito internacional, le ha

impedido obtener asilo en numerosos países, teniendo actualmente su residencia en Rusia.

Así, la figura del informante, esta revestida de un evidente carácter negativo, plasmado en apelativos peyorativos tales como el de soplón, chivito, rata, rufián[248] que derivan en un estigma que hace imposible el reconocimiento público de la denuncia. Aun así, Stathis Kalyvas demuestra que en organizaciones altamente burocratizadas, tales como la Iglesia Católica, la Gestapo o la Stasi es posible encontrar vestigios de los informantes en sus archivos.[249]

Esta dicotomía moral en la que se ven inmersos los informantes entre favorecer el bien público y traicionar sus círculos íntimos de confianza ha encontrado eco también en la cultura popular tanto para destacar la lucha interna del sujeto que ha incurrido en delación, como en la película El Delator de John Ford del año 1935, en la que un ex miembro del frente de liberación irlandés entrega información sobre un camarada y amigo a cambio de una recompensa; tanto para favorecer la práctica, siempre que el

[248] KALYVAS, Stathis. 2010. La lógica de la violencia en la guerra civil. Madrid. Akal. p. 254.
[249] Ibíd. p.255

beneficio lo justifique, como en Nido de Ratas de 1954, dirigida por el propio Elia Kazán.

Así, la historia ha permitido repudiar la práctica del empleo de informantes cuando favorecen a causas políticas, religiosas o de otra índole, que resultan atentatorias contra los derechos humanos, como los millares de ciudadanos que la Stasi tuvo en nómina como informantes en la República Democrática Alemana; pero ha terminado aceptando su relevancia, sobre todo en el ámbito corporativo, cuando los objetivos de las empresas atentan secretamente contra aspectos de interés general para la población[250].

En consecuencia, inevitablemente la confidencialidad de la identidad del informante y la protección de su integridad se transforman en aspectos si bien no esenciales, sí apropiados para la construcción apropiada de la figura. De esta forma, el informante es un sujeto que conoce información y que la comunica a su receptor, que en principio, la desconoce. La calidad de

[250] Uno de estos casos corresponde al del ex director del Departamento de Investigación de la compañía tabaquera Brown & Williamson, Jeffrey Wigand que denunció la manipulación intencionada de la nicotina en los cigarrillos. EL MUNDO, La entrevista de Jeffrey Wigand, por Miryam Blanco, 8 de febrero de 1996. http://www.elmundo.es/salud/1996/188/01177.html [consulta 23 de diciembre de 2013]

los antecedentes, la utilidad de los mismos y las características del receptor, terminan de configurar una idea que ha encontrado reciente arraigo en la legislación nacional. En principio, podríamos decir que el informante es una figura informal, que no requiere de calificaciones técnicas o profesionales ni siquiera de aptitudes psicológicas; basta el simple hecho del conocimiento de información. Dicha información, a su vez, debe ser relevante, en el sentido de tener un interés público para determinados órganos del Estado. El concepto se termina de configurar por una actitud positiva por parte de quién conoce la información: esto es, darla a conocer a su receptor.

5.2. El informante en la Ley 20 000.

La Ley 20 000 incorpora al informante otorgándole un doble cariz, permitiendo la utilización de esta figura tanto para la recopilación de información propiamente tal como para la infiltración del sujeto en una asociación delictiva. Por tanto, desarrollaremos el ámbito de acción de estas dos figuras y estableceremos que si bien, ambas tienen el calificativo de informante, jurídicamente no son lo mismo por lo que de su utilización se derivan consecuencias distintas.

5.2.1. El informante propiamente tal.

El informante es "quien suministra antecedentes a los organismos policiales acerca de la preparación o comisión de un delito o de quienes han participado en él, o que, sin tener la intención de cometerlo y con conocimiento de dichos organismos, participa en los términos señalados en alguno de los incisos anteriores [como agente encubierto o agente revelador]". Ésta es la definición que presenta la Ley N° 20 000[251] para refrendar la institución del informante, reiterándose casi literalmente la disposición contenida en la antigua ley 19 366 que sancionaba el tráfico ilícito de estupefacientes.

Podemos establecer entonces que existen ciertos elementos esenciales a la figura relativos a la información disponible, al sujeto que la conoce y a la posibilidad de obtener recompensa por su comunicación. En cuanto a la información, sólo es apto para ser informante quien conozca antecedentes relevantes acerca de la preparación o comisión de un delito o de quienes

[251] CHILE. Ministerio del Interior. 2005. Ley N° 20 000 que sustituye la Ley N° 19 366, que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas. Art. 25° Inc. 5°

han participado en él. Conocer cualquier otro tipo de información que no cumpla estos estándares mínimos no califica como legitimador y por lo tanto el aporte a la investigación no podrá encuadrarse en esta figura. En cuanto al sujeto, el conocimiento de la información es sólo el punto de partida. Solamente pueden ser informantes aquellos que no están en la obligación de dar a conocer los antecedentes, por tanto, se excluyen a los agentes policiales y en definitiva todos los que en razón de sus cargos están obligados a denunciar.[252] En cuanto a su recompensa, la noción de remuneración se trató en repetidas ocasiones tanto en la discusión de la ley 19 366 como en la actual ley 20 000, desechándose finalmente por considerarse inconveniente y reñida con principios éticos.[253] En consecuencia, el informante no puede legalmente negociar su información para obtener beneficios económicos ni menos aún de tipo procesal.

[252] CHILE. Código Procesal Penal. Ob. Cit., Art. 175º.

[253] En relación con las referidas modificaciones se manifestó, en el informe de la Comisión especial de droga, que la definición de "informante" contenida en el inciso tercero si bien es técnicamente correcta, no parecía conveniente el reconocimiento expreso que se hace del hecho de que éste puede actuar por recompensa, ya que sería el primer caso en nuestra legislación en que el Estado gratifica la delación con dineros, situación que podría ser éticamente impropia. p. 754. BIBLIOTECA DEL CONGRESO NACIONAL, 1995, Historia de la ley 19366 Sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas, dicta y modifica diversas disposiciones legales y deroga ley N°18403, <disponible en línea: http://goo.gl/WH9dEZ> [Fecha de consulta: 25 de agosto de 2013] Pág. 6.

Ahora, cabe preguntarse si todo tipo de persona que conozca información puede potencialmente ser un informante y la respuesta debiera ser negativa. La información puede conocerse, ya sea de primera fuente, en cuyo caso el sujeto será parte de la organización criminal; o de forma circunstancial o tangencial a la actividad delictiva. Solo en el último caso, la información proporcionada permite considerar al sujeto como informante.

De acuerdo a la Ley 20 000, se sancionará la simple asociación u organización para cometer alguno de los delitos contemplados en ella,[254] por lo que la sola pertenencia a una asociación de estas características, incluso sin haberse cometido ilícito alguno, conlleva una responsabilidad penal que impide al sujeto ser legítimamente un informante. La legislación, para salvar esta dificultad de obtener antecedentes de un miembro de una actividad delictiva, incorpora la figura del cooperador eficaz, que consiste en una atenuante de responsabilidad penal que concurre cuando la colaboración del imputado es considerada fundamental para el "esclarecimiento de los hechos investigados o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o

[254] CHILE. Ley 20 000. Ob. Cit., Art. 16°.

consumación de otros delitos de igual o mayor gravedad contemplados en esta ley."[255]

En conclusión, sólo aquel que no es imputable penalmente en los hechos investigados, puede legítimamente acogerse al artículo 25°, aportando antecedentes en calidad de informante y en virtud de la información proporcionada, solicitar las medidas de protección correspondientes.

5.2.1.1. El informante propiamente tal y los datos sensibles.

Una vez determinado y circunscrito el ámbito del informante, podemos ya denominarlo un método de investigación y como tal veremos sus implicancias con el derecho constitucional a la intimidad.

Entre las distintas fases del tratamiento de datos, el informante interviene en la recopilación. En la investigación actúa como un elemento humano que conoce información relevante o está en condiciones de conocerla y la comunica a los funcionarios policiales. En cualquier caso, las

[255] Ibíd., Art. 22° Inc. 1°.

Policías deberán filtrar todo antecedente recibido, omitiendo todo aquel de estas características, previo a cualquier análisis.

5.2.2. El informante como agente encubierto.

La definición que la ley 20 000 contempla respecto al informante prevé particularidades que exceden técnicamente el concepto mismo de la figura. Se entiende, en una primera parte, la institución del informante como lo que estrictamente es: un sujeto que entrega información relevante a los órganos policiales. La segunda parte de la definición, no obstante, genera complejidades, pues escapa al concepto básico de lo que un informante es y se transforma en una figura muy distinta, que ya no es valiosa para la investigación por el conocimiento actual de información, sino por su identidad misma. Su eventual cercanía con los partícipes de las actividades criminales investigadas, lo convierten en el sujeto ideal para, ahora sí y en propiedad, infiltrarse en una asociación criminal con la finalidad de recoger información valiosa que permita identificar a los participantes o simplemente reunir información necesaria; o, simular la compra o adquisición de sustancias con el propósito de lograr la manifestación o incautación de la droga. Es decir, a este sujeto particular, generalmente

alguien con un historial criminal, se le autoriza por ley para ejercer como agente encubierto o agente revelador, figuras en principio reservadas exclusivamente para funcionarios operativos de los servicios policiales.

La ley establece que para que un informante pueda ejercer como agente encubierto o como agente revelador, es necesario que en primer lugar haya ejercido como informante, es decir, haya suministrado con anterioridad información valiosa a las policías, las que en un intento de capitalizar el recurso valioso en que se convierte la identidad misma del informante, por su conocimiento (eventual) del mundo delictual, sus contactos, y principalmente por la ventaja práctica que significa facilitar la etapa de infiltración, lo convierten, en los hechos, en un agente más de las fuerzas policiales en la causa en particular.

Ahora, el proceso de convertir a un informante en un agente encubierto, a pesar de no existir en la ley más previsiones que lo dispuesto en el inciso primero del artículo 25°, es de todo menos formal. En primer lugar, y como ya mencionamos en el párrafo anterior, se requiere que ya haya actuado como informante. Las circunstancias prácticas del asunto, es

decir, fiabilidad, relevancia y calidad de la información suministrada, valoración del perfil del sujeto, y las particularidades de su historia personal en relaciones a sus vínculos con sujetos investigados, lo convertirán en el sujeto ideal para esta labor. Esta situación, de evidente orden práctica, no está regulada en la ley, por lo que los servicios policiales determinarán en base a sus criterios particulares, y la eventual existencia de reglamentos internos, si un sujeto reúne las calidades necesarias.

Una vez establecida la aptitud del sujeto, éste solo se convertirá en agente encubierto, o revelador en su caso, de mediar autorización del Ministerio Público a propuesta de los servicios policiales correspondientes. Por tanto, no basta que en la práctica el informante ejerza como agente encubierto, sino que su actividad debe estar investida de la legitimidad que otorga esta autorización.

En cualquier caso, y esto vale a su vez para el agente encubierto y agente revelador propiamente tales, se trata de un método de investigación eminentemente intrusivo y que como tal, implica la vulneración de diversas garantías y derechos fundamentales en el proceso. El artículo 24° establece

que toda actuación de investigación referida en la ley se aplicará “de conformidad a las disposiciones del Código Procesal Penal”. Esta remisión nos dirige al artículo 9° del mentado Código en cuanto “toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá autorización judicial previa”. Y en cualquier caso, aun sin la existencia de estas normas, la propia Constitución, como ya hemos reiterado numerosas veces, dispone en su artículo 83º inciso 3º que: “El Ministerio Público podrá impartir órdenes directas a las Fuerzas de Orden y Seguridad durante la investigación. Sin embargo, las actuaciones que priven al imputado o a terceros del ejercicio de los derechos que esta Constitución asegura, o lo restrinjan o perturben, requerirá autorización judicial previa.”

No pretendemos con esto hacer un estudio fundamental sobre la figura del agente encubierto, institución que ya se está tratando con progresiva frecuencia, pero es un punto importante determinar si la sola actuación de éste vulnera de por sí garantías fundamentales. En este sentido, la sola infiltración es generadora de violación a derechos constitucionales,

[256] si convenimos en la protección del derecho a la intimidad o vida privada y de garantías procesales como el derecho a guardar silencio y la presunción de inocencia.

Riquelme[257], contempla dos fases en el proceso de actuación del agente encubierto. Una primera fase exploratoria y otra definida y dirigida, solo pudiendo considerarse a esta última como afectadora de derechos fundamentales.

Por otra parte, se discute la extensión de la autorización judicial previa para el agente encubierto o agente revelador (y en este caso para el informante que actúa como tales), en el sentido de si se convierte en una carta blanca de acción para explorar e infiltrarse y en tal condición recoger todo tipo de información y antecedentes para la causa, permitiendo prescindir de todas las autorizaciones judiciales requeridas para este tipo de diligencias en el Código Procesal Penal y aún más en la propia Constitución; o, por el contrario, si se requieren tantas autorizaciones

[256] RIQUELME, Eduardo, 2006, El agente encubierto en la ley de drogas: la lucha contra la droga en la sociedad del riesgo, Política Criminal, N° 2, (A2), p. 12 [disponible en línea: http://www.politicacriminal.cl/n_02/a_2_2.pdf] [fecha de consulta: 25 de noviembre de 2013].
[257] Ibíd. , p. 9.

judiciales como diligencias se pretendan realizar. La mención de este asunto no es gratuita, pues al tratar la figura del informante, es necesario determinar indubitadamente sus límites. La sola actuación del informante como infiltrado no aporta ninguna diferencia al caso, pero la autorización correspondiente termina por metamorfosear la calidad del sujeto, transformándolo para efectos prácticos en un agente encubierto, con todas las consecuencias legales que eso significa. Argumentar en contrario, supondría negar la esencia misma de ambas instituciones. Desde el momento que el informante modifica su actuar (con la correspondiente autorización) y ejerce legitimado como agente encubierto, deja de ser lo primero pues incorpora un nuevo elemento a su actuar inherente al segundo: el engaño. Utiliza todos los elementos ventajosos para la investigación que le proporciona las particularidades de su identidad y reputación y los dirige con una finalidad de engaño para infiltrarse en una organización de características criminales. La infiltración a su vez es un segundo elemento diferenciador de ambas figuras; mientras el informante no se inmiscuye en la organización, pues su conocimiento de la información es meramente circunstancial (pues de ser interno, estaría, como ya argumentamos, incapacitado legalmente para ejercer como informante), una vez que actúa

como agente encubierto intenta ser admitido en un espacio privado para obtener la información requerida con una finalidad oculta, vulnerando una serie de derechos y garantías en el proceso.

La diferencia entre ambas figuras también se evidencia en aspectos procesales; mientras el informante no goza de beneficios de exención de responsabilidad penal, pues se entiende que en la causa investigada no ha cometido delito alguno; el actuar legitimado como agente encubierto le permite, dentro de los márgenes establecidos, evitar cualquier sanción punitiva cometida con ocasión de la investigación.

5.2.2.1. El informante como agente encubierto y los datos sensibles.

Con respecto al tratamiento de datos sensibles, el asunto es aún más complejo, pues si ya es difícil justificar la actuación de agentes encubiertos desde el punto de vista constitucional, al practicar diligencias que ordinariamente requieren autorización judicial, sin más fundamento que la autorización que legitimó su nombramiento; más aún lo es que el agente pueda recopilar antecedentes de carácter sensible. Exacerbado en este caso

por el hecho de que el agente no es un funcionario policial entrenado, sino que un ciudadano común, frecuentemente con un prontuario criminal.

Aun legitimando toda la serie de actuaciones previas de infiltración y acceso del agente a los círculos íntimos de los sospechosos de los delitos contenidos en la Ley 20 000 -sin la autorización judicial correspondiente-, en base a criterios de celeridad del proceso o de protección de la identidad de los sujetos, no podría extenderse dicha legitimación a la recopilación y análisis de información sensible de los investigados, toda vez que no existe disposición alguna en la norma señalada que lo permita.

En todo proceso penal, y en aplicación de cualquier método investigativo, la presencia de una norma que autorice el tratamiento de datos sensibles es imprescindible. No obstante, y como ya señalamos en el capítulo anterior, aun sin norma y considerando a ciertos datos sensibles como relevantes para la investigación, podrán de todas formas tratarse si se cuenta con autorización judicial, la que de acuerdo a la Constitución debe ser previa, pues sólo a través de indicios y antecedentes legítimamente recopilados, los órganos de persecución penal pueden llegar a adquirir la

convicción de que determinados datos sensibles son pertinentes y relevantes al proceso y no a la inversa, adquiriendo el dato primero y luego percatándose de su relevancia. Todo esto buscando evitar la exclusión de prueba que ponga en peligro la investigación.

### 5.3. El Informante en Inteligencia.

La inteligencia de fuente humana (HUMINT[258]) es la más antigua y tradicional de las fuentes, la que pese al surgimiento de tecnologías cada vez más potentes de procesamiento de datos, conserva intacto su valor esencial dentro del proceso de análisis y producción de información[259]. Sus características particulares configuran una fuente de recursos imprescindible para la labor de inteligencia, pues el contacto interpersonal es irreemplazable, único e inimitable (hasta el momento), por la tecnología. Su valor a su vez se incrementa desde el momento en que los datos obtenidos a través de fuentes abiertas (OSINT), pueden deliberadamente conducir a la desinformación; o que, simplemente aquellos individuos o asociaciones que realizan actividades atentatorias contra la seguridad nacional o el orden público, se sustraen voluntariamente de la utilización de

[258] Todos los acrónimos empleados se basan en sus nombres originales en el idioma inglés.
[259] VERA, Ob. Cit., p. 249.

tecnologías de comunicación que corran el riesgo de ser interceptadas (SIGINT).

No es objeto de análisis la necesidad de las fuentes de inteligencia humana, pues su utilidad no está en entredicho, mas es necesario determinar claramente los límites de dicha actividad. La cuestión no es menor, pues la actualidad nos presenta un panorama internacional bastante ilustrativo respecto a la necesidad de justificar, o no, a cualquier costo -principalmente traducido en disminución o directamente eliminación de derechos y garantías- la protección de la seguridad nacional frente a las amenazas, en especial la del terrorismo.

Si bien, se pueden afectar la más amplia gama de derechos fundamentales mediante estas técnicas, nos limitaremos en este caso al derecho a la autodeterminación informativa y en particular, al derecho a la intimidad y su relación en particular con la figura del informante, como método de recopilación de datos.

El informante en inteligencia es aquella persona, que sin ser miembro de un servicio, suministra información prevalida de las ventajas que otorga las particularidades de su identidad, que lo sitúan, sin necesidad de infiltración activa por parte de la agencia de inteligencia, en la esfera de sujetos u organizaciones de interés para los organismos de seguridad. El informante adquiere especial relevancia cuando las circunstancias del caso hacen difícil o imposible la infiltración de un funcionario de los servicios de inteligencia, situación que sería considerada como ideal, pues como agente operativo, este último es un sujeto entrenado profesional y técnicamente, que tiene aptitudes psicológicas compatibles con su labor y ha sido sometido a rigurosos procesos de selección.

Existirán dos formas en que una persona adquiera la calidad de informante: sea proporcionando voluntariamente antecedentes, sin ningún objetivo más que ser un “ciudadano leal”, premunido de la conciencia de realizar un bien para su país; sea por la búsqueda y detección por parte de las agencias de potenciales sujetos que puedan suministrar información (este caso es una actividad positiva de análisis, cruce de datos, elaboración de perfiles, etc., que permitan establecer candidatos a ejercer como tales).

Sin embargo, los organismos no podrán depender exclusivamente de información proporcionada en forma voluntaria, principalmente por la poca fiabilidad que pueda tener, debido a que puede ser emitida con la deliberada intención de generar distracción o confusión en los servicios de inteligencia.

El manual de manejo de fuentes de la *School of Americas*, si bien orientado al ámbito de la contrainteligencia, sirve como ilustrador en el procedimiento de localización de un informante, al establecer una estructura en etapas sucesivas, aunque muchas veces superpuestas, en el proceso de consecución y utilización de un "empleado" o "colector de información", como es llamado en el documento. Así, en primer lugar, será necesario localizar al empleado potencial, donde sus características personales, su cercanía a sujetos u organizaciones de interés, sus motivaciones, etc., deberán ser tomadas en cuenta por el agente para establecer los candidatos más aptos; luego, será necesario una investigación de los antecedentes de éstos para determinar así el grado de confiabilidad, la calidad de sus motivaciones, indicios de inestabilidad emocional, y en particular, cualquier antecedente que pueda descartarlo; sólo una vez checado el historial del

sujeto podrá establecerse el contacto y la negociación. Estas gestiones culminan con la persona debidamente capacitada y motivada que, controlable, acepta trabajar con el gobierno. Finalizada la negociación y aceptada la labor corresponderá la asignación de tareas, el suministro de documentación necesaria y el adiestramiento específico.[260]

5.3.1. El informante en la Ley 19 974.

El artículo 32° define a los informantes como "aquellas personas que no siendo funcionarios de un organismo de inteligencia suministran antecedentes e información a dichos organismos para efectuar el proceso de inteligencia". Estos sujetos son designados por los directores o los jefes de los organismos de inteligencia del Sistema y no requieren en dicho nombramiento autorización judicial.

Para efectos prácticos, desmembraremos el concepto en sus elementos esenciales y definitorios que a la luz de la legislación chilena configuran esta particular figura.

[260] SCHOOL OF AMERICAS. Manual de Contrainteligencia. [en línea] <http://www.intelpage.info/manuales-oficiales-de-inteligencia.html> [fecha de consulta: 10 de noviembre de 2013]

5.3.1.1. El informante no es funcionario de los servicios de inteligencia.

Frente a eso, podemos mencionar que la principal consecuencia es que no se le aplicarán a esta figura las disposiciones de los títulos VII y VIII de la ley 19 974. En efecto, las normas sobre secreto de la información obtenida y el uso exclusivo de la información de ésta para los fines que se establezcan, sólo son aplicables a quienes tengan la calidad de funcionarios de los servicios de inteligencia, por lo que la impropia utilización de dichos datos sólo podría ser perseguida por las normas comunes establecidas en el Código Penal[261]. La dificultad radicaría en que, precisamente, la obligación de secreto sí rige para los funcionarios de inteligencia, la cual se mantiene aún después de cesadas sus funciones.

5.3.1.2. El informante es designado por los jefes de los organismos de inteligencia del Sistema.

[261] Vid. DÍAZ TOLOZA, Regina, 2007, Delitos que Vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno, Ius et Praxis 13(1) 291 – 314.

Éste puede ser designado por cualquiera de los jefes o directores de los organismos del Sistema, incluyendo a la ANI, a diferencia del agente encubierto, que sólo puede ser nombrado por los jefes o directores de la inteligencia militar o policial, como consecuencia de la ausencia de funciones operativas de la Agencia. Vera[262], al respecto afirma que si bien la mención hace referencia o los jefes o directores, esto no obsta a que los propios funcionarios puedan tener sus informantes.

5.3.1.3. El informante no requiere en su nombramiento autorización judicial.

La razón fundamental de la disposición radica, según la historia de la ley, en que pretender obtener autorización judicial cada vez que se necesite designar a un informante (o agente encubierto en su caso) restaría celeridad al proceso y, en cualquier caso, afectaría la protección misma del secreto de la identidad de los involucrados, con potenciales consecuencias a su integridad física[263]. Podemos advertir los efectos gravosos de seguir con

[262] VERA, Ob. Cit., p. 249.

[263] El Subsecretario del Interior de ese entonces, señor Jorge Correa, señaló en el informe de la Comisión de Defensa Nacional que "[…] Un servicio de Inteligencia no puede funcionar si existe riesgo de que un informante o un agente encubierto puedan ser delatados ante los

esta regulación, puesto que, amparándose en el secreto de la identidad del informante, se pueden utilizar este método para la obtención ilegal de información o su uso malicioso. Del mismo modo, habiéndose empleado un sistema de reserva tan riguroso del procedimiento judicial de autorización para la utilización de métodos especiales de obtención de información, nada obsta a que se hubiese optado por la misma vía para su nombramiento, por lo que la verdadera razón para la exclusión de la autorización judicial radica en lo mencionado originariamente, esto es, la celeridad del proceso.

5.3.1.4. El informante no es recompensado.

El concepto de recompensa no está incluido en la definición legal de la figura, aunque según Vera[264], nada obsta a que en aplicación de los gastos reservados se efectúe remuneración por sus servicios, situación de uso común en el ámbito de los servicios de inteligencia.

5.3.1.5. El informante no está exento de responsabilidad penal.

---

tribunales de justicia […]" BIBLIOTECA DEL CONGRESO NACIONAL, 2004, Ob. Cit., p. 55.

[264] VERA, Ob. Cit., p. 250.

La exención de responsabilidad penal se trata de un régimen de excepción, por lo que sólo puede utilizarse en los casos en que expresamente el legislador así lo establece y sobre el particular, en el articulado de la ley 19 974, no se encuentra ninguna norma en tal sentido.

### 5.3.2. El informante de inteligencia y los datos sensibles

Como hemos apreciado, existen numerosas discusiones respecto del uso de informantes, lo que repercute negativamente en la protección especial de los datos sensibles contemplada en la LPDP. Si bien el sistema de inteligencia se basa en la premisa de la autorización judicial para la protección de la inviolabilidad del hogar y de las comunicaciones, esta aparente protección se ve opacada al consignarla exclusivamente al resguardo de éstas, no extendiéndose al derecho del titular de determinar la cantidad y calidad de información de los datos que desea hacer públicos, en consecuencia sólo se aplica en los llamados métodos especiales de obtención de información, establecidos taxativamente en el artículo 24°, y a los que no pertenece la figura del informante.

Mediante la utilización indiscriminada de esta técnica, puede accederse sin ninguna barrera más allá del autocontrol administrativo a datos de la esfera íntima de las personas, situación que, como veíamos en el capítulo III, carecería de la legitimidad de actuación, al no poseer una ley expresa –y no, como aparentemente ocurre en la actualidad, meras órdenes o decretos administrativos- que facultase al órgano de inteligencia a acceder y tratar dichos antecedentes.

Dada la situación mencionada precedentemente, sólo puede esperarse de parte de la autoridad administrativa el control y la dirección en el uso de estas herramientas de trabajo de inteligencia, con el fin de guiar su actuación hacia las materias de interés de la operación, y buscando eliminar los antecedentes que versen sobre los datos sensibles de las personas sujetas a estos actos.

# CONCLUSIONES

**1.** Esta investigación parte de dos focos aparentemente distantes e inconexos, pero que guardan mucha más afinidad de la que puede pensarse a simple vista: la figura del informante y el tratamiento de datos sensibles. El primero, es un método de investigación que consiste en la recopilación de datos que posteriormente serán analizados para producir inteligencia, y el segundo, es la forma en la que se enfrenta el sujeto encargado de la actividad de tratamiento de información a aquellos antecedentes íntimos de la persona, que al menos en principio debieran permanecer en su esfera privada. El informante, como método de investigación, trata información y frecuentemente se encontrará con estos datos sensibles en su labor de recopilación. La tarea de determinar la legitimidad del tratamiento requirió un análisis que fue el objeto de estas páginas.

Tanto el informante como el tratamiento de datos sensibles tienen un desarrollo legislativo relativamente reciente: la ley 19 628 determina el concepto y el ámbito de la protección de datos personales mientras que la figura del informante se integra en nuestro ordenamiento jurídico exclusivamente en dos áreas: la inteligencia, a través de la Ley 19 974, y el

proceso de persecución penal, en razón de la investigación de los delitos contenidos en la Ley 20 000. Lamentablemente, el ordenamiento jurídico en su conjunto no es en general coherente con las directrices establecidas en la Ley 19 628, al menos desde un punto de vista terminológico, lo que genera conflictos interpretativos al pretender establecer la correspondencia entre las leyes sectoriales y el sistema de protección de datos. Una muestra de esto es el lenguaje completamente distinto que utiliza la normativa de inteligencia, que gira en torno a conceptos propios de su área (como los de "fuentes abiertas" o "fuentes cerradas") que son totalmente desconocidos por la Ley 19 628. Sobre esta discordancia no existe mayor desarrollo doctrinario que salve estas dificultades, sin embargo, pensamos que los conceptos contemplados en la LPDP nutren todo el ordenamiento jurídico en lo referente al tratamiento de datos personales, primando en consecuencia, sobre cualquier construcción propia del área que pugne con ellas. Así, en virtud del principio de especialidad de la ley, conceptos como los mencionados, no tienen cabida en la actividad de procesamiento de la información de carácter personal.

La actividad del informante corresponde, como ya anticipamos, a la recopilación de antecedentes, la que se integra (bajo la terminología impuesta por la ley de protección de datos) dentro de las etapas del tratamiento de la información y, se incluye exclusivamente en dos áreas de la actividad estatal: la inteligencia, integrada por los órganos del Sistema Nacional de Inteligencia; y, la persecución penal, cuya gestión exclusiva corresponde al Ministerio Público y a sus órganos auxiliares. Definimos pues, el ámbito de nuestra investigación estrictamente al delineado por la actividad de tratamiento de datos personales sensibles de dos áreas de la actividad estatal: la inteligencia y la persecución penal, para luego referirnos exclusivamente a la figura del informante una vez que establecimos el contexto orgánico y procedimental en el que se desenvuelve.

**2.** La protección de los datos personales, estimamos, se funda en el derecho a la autodeterminación informativa; como tal, permite justificar exitosamente el control que tienen las personas sobre toda la información relativa a ellas, independiente de su carácter íntimo o su inocuidad. Sin

embargo, la protección reforzada de los datos sensibles no es satisfactoriamente cubierta con este derecho; mientras, decíamos, la autodeterminación informativa gana enteros asegurando una protección amplia de todo tipo de información personal, pierde la especificidad y atención que el dato sensible requiere.

Es aquí donde aludimos a la nueva concepción de intimidad, aquella que las discusiones doctrinarias de los últimos años terminaron por fortalecer, otorgándole una faceta positiva de control de la que anteriormente carecía. Esta intimidad es el verdadero fundamento de la protección específica de los datos sensibles, pues tiene éxito donde la autodeterminación informativa falla. Hay, tanto una identificación conceptual -lo que es íntimo es a la vez sensible- como una remisión a la Constitución –la intimidad es un derecho fundamental-, que en conjunto consagran una envoltura protectora definida y reforzada. Además, al constituir la protección de estos antecedentes el desarrollo de un derecho constitucional, su limitación (entendiendo que la sustracción del control del titular sobre sus datos sensibles es una restricción al contenido del derecho) sólo puede proceder en virtud de una norma legal y sólo respecto de

fórmulas específicas de interés general que garanticen bienes jurídicos de rango constitucional.

**3.** La ley de protección de datos establece en su artículo 20° el régimen aplicable a los órganos públicos en la tarea de tratamiento de información personal; dicha disposición no establece una diferencia radical en cuanto a la forma de realizar esta actividad que la distinga sustancialmente de aquella aplicable a los demás sujetos autorizados. La única distinción consiste en el reconocimiento del principio de competencia en la actividad pública; esto quiere decir que cada vez que el órgano público se enfrente a la actividad de tratamiento de datos personales, bastará con que opere en el ámbito de sus atribuciones previamente delimitadas por ley para que dicha actividad sea legal. En consecuencia, el órgano público no requiere una norma genérica que lo autorice para tratar datos personales. Ahora, esta afirmación es verdad sólo a medias; en la práctica no es recomendable prescindir de una norma legal de estas características, pues la determinación específica de si la actividad de tratamiento de datos en un caso particular está integrada en las competencias del órgano, es una cuestión de hecho que

en último término serán los Tribunales de Justicia los encargados de dilucidar. Esta imprecisión se contrarresta con una norma especial que expresamente integre en las atribuciones del órgano público el tratamiento de datos personales.

**4.** Algunos autores han pretendido establecer que este artículo 20° contempla asimismo una autorización genérica para tratar datos sensibles. Por más justificados que sean sus argumentos, consideramos que no pueden estar más equivocados. Datos personales y datos sensibles son dos conceptos que la Ley y la doctrina insisten en diferenciar; están establecidos en una relación de género a especie, siendo esta última una categoría que predica una protección reforzada, y dicha protección no escapa a la acción de la actividad estatal, aún más, siendo deber del Estado respetar los derechos establecidos en la Constitución, la protección del dato sensible como desarrollo nuclear del derecho a la intimidad, es todavía más imperiosa. Por otra parte, el propio artículo 20° establece que el órgano público debe sujetarse fielmente a "las reglas precedentes", respetando en consecuencia todas las restantes disposiciones y en especial, en este caso,

las relativas al tratamiento de datos sensibles señaladas en el artículo 10°. Esta última disposición contempla la prohibición general de tratamiento de los datos sensibles, condicionando la existencia de excepciones sólo a la creación legislativa. Dicha exigencia es asimismo solventada por el carácter fundamental del derecho a la intimidad, que precisa una norma de estas características para que la restricción al derecho sea legítima. Citando a De la Serna Bilbao: “corresponde a los representantes de la soberanía popular permitir excepcionar el control del titular del dato y sustituir su consentimiento...”. Por lo tanto, y por más razonables que sean las justificaciones para pretender establecer autorizaciones genéricas para tratar datos sensibles (como serían por ejemplo evitar una inteligencia improductiva o un sistema persecutorio ineficaz), si no hay norma legal que permita dicha actividad, todo tratamiento de esta información es ilegal.

Este es el panorama actual en nuestro ordenamiento jurídico. No tenemos disposiciones similares a las establecidas, por ejemplo en España, en cuya legislación de protección de datos encontramos en su artículo 22° que “La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad

de los datos(...) [sensibles], podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta,(...)"; o, en su caso, la legislación argentina de inteligencia que excepciona expresamente "obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción."

**5.** Esta situación de ausencia de norma es, al menos en el proceso de persecución penal, sólo aparente. Nuestro ordenamiento jurídico contempla numerosas disposiciones, integradas principalmente en el Código Procesal Penal, que permiten al Ministerio Público y sus órganos auxiliares, la realización de diligencias que tienen directa repercusión en aspectos sensibles de la persona humana, como por ejemplo la realización de exámenes corporales o la incautación y registro de documentos. Por tanto, no es cierto afirmar que la ausencia de una norma que autorice

genéricamente tratar datos sensibles cuando sean necesarios para una investigación concreta incide directamente en la ineficacia del órgano persecutorio. Por el contrario, el Ministerio Público, aún sin autorización legal para realizar determinadas diligencias relacionadas con información sensible, está facultado en último término para recurrir al juez de garantía y solicitar fundadamente, mediante el procedimiento de autorización judicial previa, la legitimación para tratar información sensible, que sea a su vez necesaria, relevante y pertinente para la investigación, pues su análisis implicaría la afectación, restricción o perturbación de un derecho fundamental reconocido por la Constitución y que en este caso corresponderá al derecho a la intimidad.

**6.** En el ámbito de la inteligencia, la situación es diferente. Existe una disparidad respecto de la transparencia y publicidad de las normas en juego: mientras que en materia de persecución penal, la propia dinámica del procedimiento, instaurada por la reforma procesal penal, tiende hacia ellas; en materia de inteligencia prima en cambio el secretismo y la opacidad. Probablemente existen en el ámbito del Sistema Nacional de Inteligencia

reglamentos u órdenes internas de carácter secreto relativas al tratamiento de datos personales sensibles; su existencia o no, es a nuestro juicio, totalmente irrelevante para efectos de garantizar la legalidad de la actuación, considerando una vez más que el desarrollo de derechos fundamentales sólo puede efectuarse a través de una norma legal. No obstante, consideramos que dado el actual panorama internacional, el dato sensible se ha convertido en un elemento muchas veces no sólo necesario en una investigación, sino a su vez esencial. El ejemplo clásico corresponde a las creencias religiosas y su directa relación con la actividad terrorista fundamentalista. Obviar esta evidente realidad sería totalmente contraproducente, aun así la configuración actual de nuestra legislación consideraría ilegal este tratamiento. En consecuencia, y para salvar todas estas eventuales críticas al actuar del Sistema de Inteligencia, debiera plasmarse esta necesidad en una normativa expresa, que haciéndose cargo de la ponderación entre los principios constitucionales en disputa, contemplara exhaustivamente los casos específicos en los que la protección de los datos sensibles debe sucumbir ante la prevención de un peligro real para la seguridad nacional, estableciendo claramente los mecanismos destinados a otorgarle contenido a este concepto jurídico indeterminado,

para evitar otorgar supremacía *a priori* a una condición cuyo significado podría llegar a depender del capricho de la administración. Será tarea del legislador adecuar la normativa nacional a esta innegable realidad.

**7.** Es éste el contexto en el que se desarrolla la actividad del informante, que como anticipábamos, participa del proceso de tratamiento de datos en la etapa de recopilación de los mismos. Emparentada esta figura íntimamente con el agente encubierto, decíamos que pese a compartir muchas de sus ventajas en el apoyo a la actividad investigativa, exacerba a su vez todos sus aspectos cuestionables. No obstante, desde la doctrina, el tratamiento de esta figura parece ser selectivamente olvidado, en desmedro del agente encubierto, el que tiene ciertamente una elaboración floreciente. Por esta razón consideramos oportuno establecer como uno de los focos de esta memoria un desarrollo de esta figura.

Dadas las particularidades de las construcciones legislativas de la figura del informante en los cuerpos normativos en los que se encuentra

establecida en el ordenamiento jurídico chileno, es imposible establecer una definición unívoca. Mientras en la Ley 20 000 el informante no debe ser parte de la organización criminal, pues de ser así su ámbito se superpone con el del "cooperador eficaz", considerando que la sola asociación en esta ley es delito; nada al respecto se dice del informante de la ley de inteligencia. Aun así, determinamos que el informante es aquella persona ajena a los órganos investigativos que les suministra información necesaria para el proceso de análisis. Es un sujeto, que dadas las particulares características de su identidad, presenta ventajas para los órganos de investigación evitando todo el proceso de infiltración que requeriría la utilización de un agente encubierto. Estas evidentes ventajas son un arma de doble filo, pues esta capacidad de mimetizarse con el grupo criminal o sospechoso de actividad ilícita o atentatoria contra la seguridad nacional, implica probablemente que el sujeto tendrá a su vez un prontuario criminal. Es labor de los funcionarios encargados vigilar no sólo la actividad de estos sujetos sino a su vez examinar exhaustivamente la calidad de la información entregada.

**8.** Esta amalgama de pros y contras aún no aborda el aspecto que sin duda es el más cuestionado de todos los que atañen al informante: la ausencia de un control judicial previo que le otorgue legitimidad. Para justificar esta situación, se esgrimen razones que van desde favorecer la celeridad del proceso hasta proteger su propia identidad, pero aun así la situación es preocupante desde la óptica de la protección de la intimidad. Para moderar esta crítica, cabe mencionar que si bien en la Ley 20 000 no existe un procedimiento de autorización judicial del informante, la mera remisión a las normas del Código Procesal Penal de la ley en cuestión, la convierten en requisito para su designación.

**9.** El informante, como sujeto ajeno a la planta funcionaria de los servicios que lo hayan designado, no trata datos personales en el sentido establecido en la ley de protección de datos; quien procesa la información son los propios órganos públicos que lo hayan designado. Propiamente es un simple método de investigación, por lo que no distinguirá, necesariamente, si la información que reporta contiene o no datos íntimos de las personas, y en cualquier caso, no le corresponde a él calificar esa situación. Esto, no

obstante, no exime de la obligación a los analistas de filtrar todo tipo de datos cuyo tratamiento sea ilegal. Existe en el sistema procesal penal un claro incentivo para el órgano persecutor, vinculado a las normas de exclusión de prueba, para evitar el tratamiento de información sensible no autorizada o consentida; la situación por el contrario no es tan clara en el ámbito de la inteligencia, ya que la naturaleza misma de la actividad y la ausencia de autorizaciones previas permitirían en la práctica un tratamiento que, siendo ilegal, es de difícil fiscalización fuera del propio control interno.

**10.** Nuestro ordenamiento jurídico carece de un eslabón adecuado que vincule firmemente un área tan relevante para el interés general (y asimismo tan intrusiva en la esfera particular) como la actividad de inteligencia con la protección de la vida privada de las personas. La única forma es a través de un desarrollo legislativo que incorpore el tratamiento de datos sensibles expresamente dentro de las atribuciones del sistema, pero sólo cuando dicha actividad sea estrictamente necesaria para proteger la seguridad interna o externa del país y en cualquier caso los servicios de inteligencia no pueden ser juez y parte en esta determinación, debiendo

entregarse a un órgano externo e independiente, que valorando las circunstancias del caso, y con estricta sujeción a las normas de secreto y reserva esenciales a la inteligencia, pueda adoptar en propiedad una decisión.

# BIBLIOGRAFÍA

## Fuentes Bibliográficas


1. AMERICAN CIVIL LIBERTIES UNION, Reclaiming patriotism. A call to reconsider the Patriot Act, 2009, [en línea] <https://www.aclu.org/sites/default/files/pdfs/safefree/patriot_report_20090310.pdf> [fecha de consulta: 10 de enero de 2014], p. 11.

2. ANGUITA, Pedro, 2007, La Protección de Datos Personales y el Derecho a la Vida Privada. Régimen Jurídico, Jurisprudencia y Derecho Comparado, Santiago, Editorial Jurídica de Chile. 626 pp.

3. ARRIETA, Raúl (Coordinador). Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva. 184 pp.

4. BARRERA, Felipe, 2009, Análisis de la Actividad de Inteligencia del Estado y su Control Público Jurídico, Memoria para acceder al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile, Santiago.

5. BIBLIOTECA DEL CONGRESO NACIONAL, 1995, Historia de la ley 19366 Sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas, dicta y modifica diversas disposiciones legales y deroga ley N°18403, <disponible en línea: http://goo.gl/WH9dEZ> [Fecha de consulta: 25 de agosto de 2013]

6. BIBLIOTECA DEL CONGRESO NACIONAL, 2004, Historia de la ley 19974 Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia, [en línea] <http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/3784/1/HL19974.pdf> [Fecha de consulta: 25 de agosto de 2013].

7. BIBLIOTECA DEL CONGRESO NACIONAL. 1999. Historia de la ley 19.628 Protección de la vida privada [en línea] < http://goo.gl/7duzyd > [consulta: 15 junio 2013].

8. BOLETÍN Nº 7.050-07. Proyecto de ley, iniciado en Moción de los Honorables Senadores señores Espina, Allamand, Chadwick, Larraín y Prokurica, relativo a las facultades de Carabineros de Chile y de la Policía de Investigaciones para practicar, sin orden previa, las primeras diligencias de investigación de un delito.

9. CARBONELL, Miguel (editor), 2008, El principio de proporcionalidad y la interpretación constitucional, Quito, Ministerio de Justicia y Derechos Humanos. 349 pp.

10. CAROCCA, Alex. 2005. Manual, El nuevo sistema procesal penal. Santiago. Lexis Nexis. 587 pp.

11. CASTILLO, Cinta, 2001, Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información, Derecho y Conocimiento (1): 35-48.

12. CERDA, Alberto, 2003, Autodeterminación Informativa y Leyes sobre Protección de Datos, Revista Chilena de Derecho Informático (3): 47 – 75.

13. CERDA, Alberto, 2012, Legislación sobre protección de las personas frente al tratamiento de datos personales, documento inédito, Centro de Estudios en Derecho Informático, Universidad de Chile.

14. COMANDARI, Paula y RIVAS, S. Fiscalía en observación. [disponible en línea] Qué Pasa. 11 de abril, 2013. http://www.quepasa.cl/articulo/actualidad/2013/04/1-11548-9-fiscalia-en-observacion.shtml [consulta: 20 noviembre 2013]

15. CONSEJO DE LA UNIÓN EUROPEA, Report by the secretary general/high representative to the council on intelligence cooperation, 15 de noviembre de 2001 [en línea] <

http://www.asktheeu.org/en/request/173/response/579/attach/4/sn04546%20re01.en01.doc> [consulta: 15 de enero de 2014].

16. CONSEJO PARA LA TRANSPARENCIA, 2011, Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la administración del Estado, Diario Oficial, Santiago, Chile, 14 de septiembre, C – I, P. 10.

17. CONSEJO PARA LA TRANSPARENCIA, 2011. Jurisprudencia relevante del Consejo para la Transparencia en relación a la protección de datos personales. [en línea] <http://goo.gl/bTe4uO> [Consulta: 22 de diciembre de 2013].

18. CONTRERAS, Pablo, 2009, Ponderación entre el derecho de acceso a la información pública y el resguardo de la seguridad de la nación, en: Transparencia en la Administración Pública, Santiago, Abeledo Perrot: 277-307.

19. CORDERO, Luis, 2009, Video vigilancia e intervención administrativa: las cuestiones de legitimidad, en: ARRIETA, Raúl y REUSSER, Carlos (coordinadores), 2009, Chile y la protección de datos personales. ¿Están en crisis nuestros derechos fundamentales?, Santiago, Ediciones Universidad Diego Portales.

20. CORTE SUPREMA, Oficio N°2927, 30 de noviembre de 2001

21. CUADERNOS DE EXTENSIÓN JURÍDICA, 2001, Santiago, Chile (5)

22. DÍAZ TOLOZA, Regina, 2007, Delitos que Vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno, Ius et Praxis 13(1) 291 – 314.

23. DINTRANS, Constanza, 2005. Tratamiento de datos personales por la Policía de Investigaciones. Comentario a sentencia de la Corte de Apelaciones de Santiago, Rol 494-2004. Revista de Derecho Informático (6): 175 – 185.

24. DINTRANS, Constanza, 2007. El tratamiento de datos personales en el proceso de persecución penal chileno. Memoria para optar al título de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile. Facultad de Derecho.

25. EL MOSTRADOR, Funcionario PDI queda en prisión preventiva por torturas a secundario tras marcha estudiantil, http://www.elmostrador.cl/pais/2013/12/30/funcionario-pdi-queda-en-prision-preventiva-por-torturas-a-secundario-tras-marcha-estudiantil/?fb_action_ids=10151958478869888&fb_action_types=og.recommends&fb_source=other_multiline&action_object_map=%5B4546321713076 64%5D&action_type_map=%5B%22og.recommends%22%5D&action_ref_map=%5B%5D [Consulta: 15 de noviembre de 2013]

26. EL MOSTRADOR, "Agente de contrainteligencia estaría tras robo en consulado argentino", Santiago, 10 de noviembre de 2003 [en línea] <http://goo.gl/Whb7uS> [Consulta: 15 de noviembre de 2013]

27. EL MUNDO, La entrevista de Jeffrey Wigand, por Miryam Blanco, 8 de febrero de 1996. http://www.elmundo.es/salud/1996/188/01177.html [consulta 23 de diciembre de 2013]

28. ESTADOS UNIDOS, United States District Court for New York, American Civil Liberties Union et. al. v. James R. Clapper et. al. [en línea] < https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf> [consulta: 22 de enero de 2014]

29. ESTADOS UNIDOS, United States District Court for the District of Columbia, Klayman et. al. v. Obama et. al. [en línea] <https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48> [consulta: 20 de enero de 2014].

30. EVANS, Enrique, 1986, Los derechos constitucionales, Editorial Jurídica de Chile, Santiago, 950 pp.

31. FERNANDEZ, Miguel Ángel, 2005, El principio de publicidad de los actos estatales en el nuevo artículo 8° inciso 2° de la Constitución, en: Zúñiga, Francisco (coordinador), 2005, Reforma Constitucional, Editorial LexisNexis, Santiago

32. GARCÍA, Gonzalo y CONTRERAS, Pablo, 2009, Derecho de acceso a la información en: Chile: Nueva regulación e implicancias para el sector de la defensa nacional, en Estudios Constitucionales (7) N° 1, Centro de Estudios Constitucionales, Universidad de Talca.

33. HERNANDEZ, Ana y PALACIOS, Juan, 2008, El dato sensible: su Tratamiento en Chile y en el Derecho Comparado, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile

34. HERRÁN, Ana Isabel, 2002, El derecho a la intimidad en la nueva ley orgánica de protección de datos personales, Madrid, Editorial Dykinson, 388 pp.

35. HERRERA, Juan Carlos. 2012. Breve historia del espionaje. Madrid. Nowtilus.

36. HOLZMANN, Guillermo, 1996, Bases, fundamentos y propuesta para un proyecto sobre "Sistema Nacional de Inteligencia", Universidad de Chile, Instituto de Ciencias Política, 44 p.

37. INTERPOL [en línea]
http:www.interpol.int/es/Especialidades/Bases-de-datos [consulta: 03 diciembre 2013]

38. JERVIS, Paula, 2003, Derechos del titular de datos y hábeas data en la ley 19 628. Revista de Derecho Informático (2)

39. JERVIS, Paula, 2005. Categorías de datos reconocidas en la ley 19.628. Revista de Derecho Informático (6): 111-145.

40. JONES, Chris, Secrecy reigns at the EU's Intelligence Analysis Centre, en: Statewatch Journal (22), enero 2014 [en línea] < http://www.statewatch.org/analyses/no-223-eu-intcen.pdf> [consulta: 15 de enero de 2014].

41. KALYVAS, Stathis. 2010. La lógica de la violencia en la guerra civil. Madrid. Akal.

42. KOMPATZKI, Daniela, 2004, El recurso de protección y las denominadas facultades conservadoras de los Tribunales de Justicia, Valdivia, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad Austral de Chile.

43. MEDINA, Nicolás, 2012, Procedimientos especiales de obtención de información: Análisis del título V de la ley Nº 19.974 y algunas consideraciones pertinentes a la protección de derechos fundamentales, Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, Universidad de Chile.

44. MINISTERIO DE DEFENSA DE CHILE. 2010. Libro de la Defensa Nacional. p. 108. [ en línea ] <http://www.defensa.cl/> [ fecha de consulta 25 de septiembre de 2013]

45. MINISTERIO PÚBLICO [en línea] <http://www.fiscaliadechile.cl/Fiscalia/quienes/index.jsp>

46. MURILLO, Pablo y PIÑAR, José, 2009, El Derecho a la Autodeterminación Informativa, Madrid, Editorial Fundación Coloquio Jurídico Europeo

47. NOGUEIRA, Humberto, 2005, Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales [en línea] Revista Ius et Praxis, Vol. 11(2) < http://www.scielo.cl/scielo.php?pid=S0718-00122005000200002&script=sci_arttext> [fecha de consulta: 10 de diciembre 2013].

48. PFEFFER URQUIAGA, Emilio, 1993, Constitución Política de la República de Chile, 1980. Repertorio de legislación y jurisprudencia chilenas., Editorial Jurídica de Chile. Pp. 274.

49. POLICÍA DE INVESTIGACIONES. [en línea] http:policia.cl/interpol/portada.htm [consulta: 03 diciembre 2013]

50. PUBLIC UE, EU Intelligence Analysis Centre (EU INTCEN) Fact Sheet 2012 [en línea] < http://www.asktheeu.org/es/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf> [consulta: 15 de enero de 2014].

51. REAL ACADEMIA ESPAÑOLA, Diccionario de la lengua española, vigésimo segunda edición, 2001.

52. REPÚBLICA DE CHILE. CÁMARA DE DIPUTADOS, 2013, Legislatura 361°. Sesión 75°, en martes 1 de octubre de 2013, [en línea] Valparaíso, Chile, p. 125 < http://www.camara.cl/pdf.aspx?prmID=10234%20&prmTIPO=TEXTOSESION> [consulta: 19 de diciembre de 2013].

53. RIQUELME, Eduardo, 2006, El agente encubierto en la ley de drogas: la lucha contra la droga en la sociedad del riesgo, Política Criminal, N° 2, (A2), p. 12 [disponible en línea: http://www.politicacriminal.cl/n_02/a_2_2.pdf]

54. RUIZ, Carlos, 1994, En torno a la protección de los datos personales automatizados, Revista de Estudios Políticos (84): 237-264

55. RUIZ, Carlos, 2007, Problemas actuales del derecho de los servicios de inteligencia, Inteligencia y Seguridad (2): 13-46

56. SAF, Sistema de Apoyo a los Fiscales. 2013 [disponible en línea] <www.oas.org/juridico/ppt/mesicic4_chl_sist.ppt>

57. SANCHEZ GIL, Rubén. 2007. El Principio de Proporcionalidad. México D.F. Universidad Autónoma de México

58. SANTAOLALLA, Fernando, 2002, Actos Políticos, Inteligencia Nacional y Estado de Derecho, en: Revista Española de Derecho Constitucional, N°65, Centro de Estudios Políticos y Constitucionales, Madrid, mayo – agosto, 2002

59. SCHOOL OF AMERICAS. Manual de Contrainteligencia. [en línea] http://www.intelpage.info/manuales-oficiales-de-inteligencia.html

60. SCHWABE, Jürgen, 2009, Jurisprudencia del Tribunal Constitucional Federal Alemán, Editorial Fundación Konrad Adenauer, México D.F.

61. SELLÉS, Juan, 2000, Sobre el éxtasis de la intimidad. Anuario Filosófico (33): 907-917

62. SUN TZU, El arte de la guerra. 2006. Madrid. Trotta. 236 pp.

63. THE GUARDIAN, "NSA collecting phone records of millions of Verizon customers daily" Londres, 6 de junio de 2013[en línea] < http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> [consulta: 10 de enero de 2014].

64. TÓRTORA, Hugo, 2010, Las limitaciones a los derechos fundamentales [en línea] Estudios constitucionales vol. 8 (2) <http://www.scielo.cl/scielo.php?pid=S0718-52002010000200007&script=sci_arttext> [fecha de consulta: 11 de diciembre de 2013].

65. URZÚA, Malú. 2013. Teléfonos ficticios: La otra manipulación de cifras en el Ministerio Público. [disponible en línea] La Segunda online. 23 de marzo, 2013. http://www.lasegunda.com/Noticias/Nacional/2013/03/832764/Telefonos-ficticios-La-otra-manipulacion-de-cifras-en-el-Ministerio-Publico [consulta: 20 noviembre 2013]

66. VERA LAMA, Rodrigo, 2008, Sistema de Inteligencia del Estado a la luz del Derecho, Santiago, Librotecnia, pp. 351.

**Fuentes Legislativas.**

1. ARGENTINA, 2001, Ley 25 520 Ley de Inteligencia Nacional, diciembre de 2001

2. CHILE, Ministerio de Defensa Nacional, 1990, Ley 18 948 Ley Orgánica Constitucional de las Fuerzas Armadas, febrero 1990.

3. CHILE. Ministerio de Defensa Nacional. 1990. Ley 18 961 orgánica constitucional de Carabineros de Chile.

4. CHILE, Ministerio de Justicia, 2000. Ley 19 696, Establece Código Procesal Penal. 12 de octubre de 2010. Art. 180º.

5. CHILE, Ministerio de Salud Pública. 1967. Decreto con Fuerza de Ley 725: Código Sanitario. 11 de diciembre de 1967

6. CHILE, Ministerio de Transportes y Telecomunicaciones, 2005, Decreto Supremo N°142/2005, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación, 22 de septiembre de 2005.

7. CHILE, Ministerio del Interior, 2004. Ley 19 974: Sobre el sistema de inteligencia del estado y crea la Agencia Nacional de Inteligencia, octubre 2004.

8. CHILE, Ministerio Público, 2006, Reglamento sobre procedimiento de custodia, almacenamiento y eliminación de registros documentos y similares, 30 de enero de 2006

9. CHILE, Ministerio Secretaría General de la Presidencia, 2008, Ley 20 285 sobre Acceso a la Información Pública, Agosto 2008.

10. CHILE, Ministerio Secretaría General de la Presidencia, Ley 19 628, Sobre Protección de la Vida Privada, agosto de 1999.

11. CHILE. Ministerio de Defensa Nacional. Decreto Ley 2460. Ley orgánica de la Policía de Investigaciones de Chile. Art. 1°.

12. CHILE. Ministerio de Justicia, Culto e Instrucción Pública. 1857. Decreto s/n. Reglamento del Registro Conservatorio de Bienes Raíces, 24 de junio de 1857.

13. CHILE. Ministerio de Justicia. 1930. Decreto con fuerza de ley 2128, 28 de agosto de 1930.

14. CHILE. Ministerio de Justicia. 1999. Ley 19 640 Establece la ley orgánica constitucional del Ministerio Público. 15 de octubre de 1999.

15. CHILE. Ministerio de Justicia. Ley N° 19 970 que crea el sistema nacional de registro de ADN. Art. 3°.

16. CHILE. Ministerio del Interior y Seguridad Pública. 2012. Ley 20 593, Crea el registro nacional de prófugos de la justicia, 22 de junio de 2012.

17. CHILE. Ministerio del Interior. 1986. Ley 18 556 orgánica constitucional sobre sistema de inscripciones electorales y Servicio Electoral. 01 de octubre de 1986.

18. CHILE. Ministerio del Interior. 2005. Ley N° 20 000 que sustituye la Ley N° 19 366, que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas.

19. CHILE. Ministerio de Salud. 2004. Decreto 158/4. Reglamento sobre notificación de enfermedades transmisibles de declaración obligatoria. 22 de octubre de 2004.

20. CHILE. Ministerio Secretaría General de la Presidencia, 2005, Decreto 100, fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. 17 de septiembre de 2005.

21. CHILE. Ministerio Secretaría General de la Presidencia. Ley N° 20 285 sobre acceso a la información pública. Art. 21° N° 2.

22. ESPAÑA, 1978, Constitución española. Artículo 18.4.

23. ESPAÑA, Jefatura de Estado, 1999, Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 14 de diciembre de 1999.

24. ESTADOS UNIDOS DE NORTEAMÉRICA, Public law 107–56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 26 de octubre de 2001

25. MINISTERIO DE EDUCACIÓN PÚBLICA, Decreto 6234, Reglamento para la Dirección General de Bibliotecas, Archivos y Biblioteca, 30 de enero de 1930.

26. ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS (OCDE). 1980, Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. 23de septiembre de 1980.

27. ORGANIZACIÓN DE LAS NACIONES UNIDAS, ASAMBLEA GENERAL, 1990, resolución 45/95, Directrices para la regulación de los archivos de datos personales informatizados, 14 de diciembre de 1990.

28. ORGANIZACIÓN DE LAS NACIONES UNIDAS. Asamblea General. 1948, Declaración Universal de los Derechos Humanos. 10 de diciembre de 1948.

29. POLICÍA DE INVESTIGACIONES. 1987. Decreto Supremo Nº 41, Reglamento orgánico de la Policía de Investigaciones de Chile.

30. UNIÓN EUROPEA. Parlamento Europeo. 1995. Directiva 95/46/CE. 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. Octubre 1995.

31. URUGUAY, 1967, Constitución de la República.

32. URUGUAY, 2008. Ley 18.331. Protección de datos personales y acción de “habeas data”.