Universidad de Chile

Facultad de Derecho

Departamento de Derecho Económico

El Principio de Finalidad Limitada en el Reglamento General de Datos Personales de la Unión Europea y su Aplicación en la Normativa de Datos Personales en Chile

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

AUTOR:

Maximiliano Cristian Peña Gutiérrez

Profesor Guía:

Claudio Magliona Markovitcth

Tabla de contenidos

Contenido

Resumen

La protección de los datos personales es un tema que en la actualidad es sumamente relevante, esto debido a la fuerte digitalización de nuestra sociedad y al constante avance de las tecnologías. Debido a esto, surge la protección de datos personales como una forma de proteger los derechos fundamentales de los individuos antes estas nuevas tecnologías y los efectos nocivos que podrían de generar. Dentro de la protección de datos personales se encuentran diversos principios que juegan un rol central para salvaguardar nuestros derechos, y dentro de estos derechos se encuentra el principio de finalidad, el que quizás es el principio más importante de todos. En esta memoria analizaremos los elementos del principio de finalidad y buscaremos además señalar de manera clara el rol que cumple este dentro de la protección de datos personales, y posteriormente, veremos la aplicación de este principio en Chile, a fin de asentarlo en el nuevo proyecto de ley de protección de datos personales.

Introducción

Actualmente vivimos en una sociedad casi completamente digitalizada. El internet y las tecnologías se han expandido a tal nivel que ya es imposible imaginar un mundo sin ellas. Este avance tecnológico partió de manera minúscula en el siglo pasado, por lo que no se consideraba una regulación legal del mismo, pero en la actualidad y con el peso que ha tomado y la influencia que este tiene en nosotros sería absurdo no creer que se debe de regular. Esta influencia de las tecnologías y las personas se refiere principalmente a que estas invaden cada vez más nuestra esfera de intimidad personal, un área propia y única de cada individuo que en la práctica no debería de poder de ser penetrada por nadie ni nada salvo excepciones únicas. Para establecer esto, debemos recurrir a la ley, ya que esta es la que tiene como rol defender a las personas de cualesquiera lesiones a sus derechos esenciales. Sin embargo, para entregar una adecuada protección a los derechos de las personas, la ley debe de adecuarse tanto a la realidad del lugar de donde se aplica la ley y de las características sociales, tradicionales y económicas del mismo. Es de esta idea de regulación adaptable a la realidad que veremos que surge la protección de datos personales.

Sin embargo, a fin de limitar el alcance de esta memoria, no analizaremos la totalidad de la regulación de protección de datos personales, sino que nos ceñiremos a uno de sus principios: el principio de finalidad o finalidad limitada. Es esencial analizar los elementos del principio de finalidad y cómo se relaciona con los otros principios.

Luego de realizar este análisis de sus elementos y de definir su rol, revisaremos la ley en Chile, en donde hablaremos de la actual regulación sobre datos personales y el principio de finalidad que nosotros tenemos considerado, ya que nuestro país posee una ley bastante desactualizada. Luego de esto, revisaremos el actual proyecto de ley que modifica nuestra actual ley de protección de datos personales y sobre como este abarca el principio de finalidad, a fin de comparar este con el establecido en el modelo europeo. Finalmente se efectuará un breve comentario y recomendación, sobre cómo debería de aplicarse el principio de finalidad en Chile en virtud de esta comparación, a fin de tener un principio de finalidad robusto, claro y que proteja a las personas.

Capítulo 1: El principio de finalidad en la protección de datos personales

Antes de hablar del principio de finalidad en sí, debemos primero hablar de sus orígenes. Este e capítulo se referirá a la historia de la protección de datos personales y su evolución. Para hablar de protección de datos personales primero debemos de hablar de la privacidad, ya que como se analizará en este capítulo, este es el origen de todo este marco regulatorio.

1.1 Origen de la protección de datos personales

La protección de datos como tal es un concepto relativamente nuevo en términos históricos, ya que surge como tal en el año 1890 en el famoso estudio "The Right to Privacy", escrito por Louise Brandeis y Samuel Warren, en el cual se habla de la privacidad como tal y las amenazas que pueden presentarle a esta las nuevas tecnologías, que consistían en las cámaras instantáneas en aquella época y el chisme[1], el cual empezaba a ganar mayor presencia en los periódicos. Este estudio planteó la base para este campo, pero es a mediados del siglo XX y especialmente en Europa donde comienza un mayor desarrollo de este campo, debido a los nuevos desarrollos tecnológicos principalmente en las áreas de la comunicación e información (TIC).

Como se mencionó previamente, este campo surgió hace poco, pero es importante entender que esta deriva de un concepto que incluso podemos decir que es de los más antiguos y ligados a la historia de la humanidad como tal, el cual viene a ser la idea de la privacidad, sobre la cual considero necesario hablar para entender desde su base a la protección de datos.

1.1.1 Historia temprana del derecho a la privacidad

La privacidad o vida privada es uno de los temas de mayor relevancia de la historia y ha ido evolucionando a la par del hombre y pueden de encontrarse alusiones a la misma en diversos textos históricos de índole religiosa y jurídica. Por ejemplo, la Biblia se hace una referencia a esto, en el momento en que Adán y Eva se tapan con hojas para no exponer su cuerpo. Por otro lado, podemos hablar de distintos textos jurídicos en donde se habla de la privacidad, como el Código de Hammurabi o la Ley Romana, textos en los cuales había párrafos hablando de la intrusión a hogares ajenos. También es con los romanos donde aparece por primera vez el derecho de propiedad del yo, en donde se separa al hombre exterior del hombre interior.

[1] En inglés, *gossip.*

Avanzando en la línea temporal, en la Edad Media la privacidad no tenía un valor social como el actual, ya que el individuo existía principalmente como un miembro de la comunidad, por lo que su vida privada se veía afectada y monitoreada por los otros miembros constantemente. A pesar de esta casi nula noción de privacidad de aquellos tiempos, Tomás de Aquino igualmente habla de la misma, principalmente hablando de la intimidad y de lo privado. En la edad moderna, Locke habla de la "libertad negativa" y Rousseau de la intimidad, pero ambos con una vista desde el ámbito de la persona. Ya finalmente, en el siglo XIX debido a los cambios económicos y sociales se genera una transformación en la forma en que las personas vivían su vida, cosa que también afecto a la privacidad, la cual se dividió en dos nociones: la privacidad física y la privacidad mental, evolucionando ambas de maneras distintas. Por un lado, y debido principalmente a la urbanización, la población de las ciudades comenzó a aumentar, lo que llevó a la pérdida de la privacidad física debido a que esta población empezó a vivir en lugares atestados y muy concurridos. Por el otro lado, la gente comenzó a experimentar una nueva "privacidad", ya que, a diferencia de la edad media, ya no estaban siendo constantemente vigilados por la comunidad y sometidos al control moral que estos ejercían en los mismo. En este mismo plano de urbanización, aparecen los periódicos como nueva forma de comunicación e información, los que eran un área llamativa para el fotoperiodismo y el chisme. Es aquí en donde Samuel D. Warren y Louis D. Brandeis fueron los primeros en darse cuenta del peligro de estas dos áreas y en reconocer las amenazas a la privacidad que podían causar las mismas, razones que los llevan a desarrollar su artículo "The Right to Privacy".

1.1.2 Warren & Brandeis, The Right to Privacy

El artículo de Warren y Brandeis publicado en 1890 por The Harvard Law Review es un estudio en el cual argumenta que mientras ocurran cambios políticos, sociales y económicos en la sociedad, las leyes deben de adaptarse a estos, con el fin de cumplir las demandas de la sociedad misma y así asegurar la completa protección de la persona y la propiedad[2].

Reconocen además en su estudio que las nuevas tecnologías como el fotoperiodismo y el chisme, el cual se había vuelto muy importante para los periódicos, podían ser amenazas para la privacidad de las personas. Considerando estos avances, estos dos autores fueron los primeros en demandar el reconocimiento del derecho de la privacidad (the right to be let alone) como un

[2] (Warren & Brandeis, 1890, pág. 193)

derecho general y aparte, el cual asegurase a las personas protección en contra no de violación de su derecho de propiedad, sino que al impacto emocional que podrían de sufrir[3]. Además, usan el principio de la inviolabilidad de la personalidad como piedra angular para este nuevo derecho que llama "the right to be let alone"[4]. Este derecho de "ser dejado" estar solo básicamente aseguraba protección en contra de la divulgación no deseada datos privados, pensamientos, emociones y otros[5].

Este estudio tuvo un gran impacto e influencia en diversas leyes, especialmente en la norteamericana, en donde se le considera como el pilar de origen para las cuatro existentes leyes de agravios que surgieron en la jurisprudencia norteamericana. Otro factor que puede haber contribuido al éxito de esta publicación fueron los cambios sociales y tecnológicos que hicieron que la opinión pública de la época le diese favor a la idea de privacidad. Finalmente, esta ley afecto diversas jurisprudencias, ya que varias trataron de dar una definición para el concepto de privacidad. En el otro lado del mundo, específicamente en Europa, se empezó a estudiar este derecho mucho más tarde que en los Estados Unidos, pero esta desarrolló otro tipo de protección a la misma, una más regional que cubriese a todos los países miembros de la Unión Europea a fin de agilizar el traspaso de datos personales.

1.1.3 ¿Cómo podemos definir la privacidad?

Si bien el enfoque central de este trabajo no es hablar sobre la privacidad, es relevante poder dar una definición a lo que es la privacidad o bien tratar de dar uno, esto para entender de manera clara sobre lo que es la protección de datos personales y saber por qué se entiende de tal forma.

Se mencionó que la privacidad es un concepto tan antiguo como la humanidad misma que sin embargo, a pesar de los muchos intentos que se ha dado por definir a esta, no tiene una definición universal, esto porque si bien la idea de privacidad es aclamada universalmente, su forma concreta variará dependiendo de características sociales, económicas y culturales. De esto ya podemos entender que la privacidad debe de interpretarse bajo el prisma de la era actual y en un contexto ocurrente.

[3] (Warren & Brandeis, 1890, pág. 197)
[4] (Warren & Brandeis, 1890, pág. 205)
[5] (Warren & Brandeis, 1890, pág. 213)

Hay diversos factores que afectan a las personas a la hora de poder definir lo que es la privacidad. Estos pueden variar dependiendo de las culturas, sociedades, avances científicos, incluso puede variar dependiendo de la situación concreta o el contexto, ya que compartir información en distintas situaciones puede considerarse como privada de distintas formas. Podemos mencionar al profesor de derecho Alan Westin quien establece tres niveles que afectan las normas de privacidad: la política, la sociocultural y el nivel personal[6]. En base a estos tres niveles, queda claro que la idea de privacidad varía dependiendo tanto del contexto como de la persona, por lo que se debería de buscar es un estándar promedio que pueda ser legalmente protegido.

Como se mencionó anteriormente, a pesar de los varios esfuerzos que se han hecho para definir lo que es la privacidad no se ha decidido por uno fijo, esto porque, según el profesor Daniel Solove explica en uno de sus artículos, el alcance que se le da a la privacidad en estas variadas definiciones es o bien muy amplia o estrecha[7]. Solove explica que el problema no es que estos conceptos sean incorrectos, sino que el problema es que los diversos autores que han tratado de explicarlo usan métodos tradicionales para conceptualizarlo, cosa que resulta en que solo se eleven ciertos aspectos de la privacidad o bien que la definición sea muy amplia y no den una vista completa de los elementos de la privacidad. El mismo Solove incluso creó seis categorías distintas para estas definiciones sobre lo que es la privacidad, siendo estas: 1) el derecho a dejarte estar solo (right to be let alone), (2) acceso limitado a uno mismo, (3) secreto, (4) control de la información personal, (5) personalidad y (6) intimidad[8]. Siguiendo la noción de ideas de Lucácks, mencionaré a continuación de manera breve estas seis interpretaciones que se le ha dado a la privacidad. Respecto a la primera interpretación tenemos a Warren & Brandeis, quienes en su estudio definen a la privacidad como el The Right to be Alone sobre el que hablamos anteriormente, es decir, asegurar la protección en contra de la divulgación no deseada[9]. El profesor israelí Ruth Gavison considera que el interés que existe sobre la privacidad se relaciona con nuestra preocupación de nuestra accesibilidad a los demás: hasta qué punto somos conocidos por los demás, hasta qué punto tienen acceso físico a nosotros, y hasta qué punto somos objeto de la atención de otros[10]. Richard Posner, jurista y economista, evita dar

[6] (Westin, 2003, págs. 431-434)
[7] (Solove, 2002, pág. 1094; 1099)
[8] (Solove, 2002, pág. 1094)
[9] (Warren & Brandeis, 1890, pág. 193)
[10] (Gavison, 1980, pág. 423)

una definición per se dé la privacidad, pero afirma que "uno de los aspectos de la privacidad es el retenimiento u ocultar información"[11]. Otros autores consideran que la privacidad como un control por sobre la información, como Alan Westine que la define como "la forma en la que el individuo puede determinar qué información de él puede ser conocida por otros"[12]; mientras que Charles Fried afirma que esta es "la forma en la que tenemos control sobre la información de nosotros mismo"[13]. Finalmente, otros autores han argumentado que la privacidad tiene relación íntima con la personalidad, individualidad y dignidad humana[14] y otros la entiende como "el control o la autonomía de las intimidades de la identidad personal[15]. El punto de esta enorme enumeración es demostrar que existen diversas interpretaciones para la idea de privacidad, a la vez de que también existen diferentes aspectos de esta. Todas estas definiciones demuestran un punto importante sobre lo que es la privacidad, pero deja claro que es muy complicado darle una definición uniforme a la misma.

Finalmente, según Adrienn Lukács, una de las mejores definiciones para la privacidad es la hecha por el jurista húngaro Máté Dániel Szabó, quien dice que "la privacidad es el derecho de un individuo de decidir acerca de si mismo/misma". Esta noción de Szabó, según argumenta Lukács, involucra muchos aspectos de lo que se considera como privado, como por ejemplo los mencionados previamente. Siguiendo con la argumentación de Lukács, este considera que la mejor definición o aproximación que se le puede dar a la privacidad es combinar esta definición del húngaro Szabó con las categorías de Solove, ya que estas últimas no hablan sobre cuáles son los elementos centrales de la privacidad, y al conocerlos podemos ver pistas sobre qué áreas de la vida cubre la privacidad[16]. Pero también añade Lukács que, a la hora de combinar esta definición junto a estas categorías, no debemos de olvidarnos del contexto de esta, el cual está en constante cambio.

Como se ha mencionado anteriormente, es sumamente complicado dar una definición universal a la privacidad, lo que lleva a que sea muy difícil de definir el objeto jurídico que se debe de defender por medio del derecho a la privacidad, además que se le suma a esto que como las

[11] (Posner, 1978, pág. 393)
[12] (Westin, 2003, pág. 431)
[13] (Friend, 1968, pág. 482)
[14] (Bloustein, 1964, págs. 973, 974)
[15] (Gerety , 1977, pág. 281)
[16] (Lukács, pág. 259)

características y elementos de la privacidad varían dependiendo de las diferentes estructuras socioeconómicas existentes, se haga casi imposible darle una noción legal exhaustiva. Sin embargo, a pesar de esto, diversos documentos legales reconocen el derecho a la privacidad.

1.2. La privacidad y la protección de datos personales desde un marco legal

Como se mencionó anteriormente, la privacidad es un concepto muy abstracto como para ser definido legalmente, pero de todas formas diversas legislaciones, documentos y países la reconocen como un derecho fundamental. El objetivo de este trabajo no es hablar de la privacidad como tal, sino que, de la protección de datos personales, y dentro de este del principio de finalidad limitad, específicamente sus elementos y rol.

Creemos que la protección de datos personales es uno más de los elementos que conforman a la privacidad, esto porque cuando uno piensa en datos personales, estos normalmente se refieren a nombre, domicilio, IP y otros, que son elementos fuertemente vinculados con la privacidad.

Finalmente, es relevante señalar que, si bien la privacidad no se puede defender de forma exhaustiva legalmente debido a su abstracta concepción, este no es el caso para los datos personales, ya que estos son un aspecto más específico y por ende más susceptibles a ser regulados legalmente. Pero a pesar de esto, creemos que es importante indicar nuevamente que la privacidad es algo que está en constante cambio y depende de diversos factores sociales y económicos, por lo que hay que tener en cuenta que la protección de datos personales también está sujeto a estos mismo factores y cambios.

1.3 Los datos personales

Para entender el que es la protección de datos personales, primero debemos de definir lo que es un dato personal. Podemos definir a los datos personales como aquellos datos que corresponden a cualquier información relativa de una persona física viva identificada o identificable, a la cual también se le pueden sumar las distintas informaciones que recopiladas pueden llevar a la identificación de una determinada persona. En el RGDP, se encuentra la definición de datos personales en el artículo 4 (1), y en nuestra legislación, se habla de los datos personales en el artículo 2 letra f) de la ley 19.628, donde se establece que se entiende por dato de carácter personal “los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”.

Algunos ejemplos de este tipo de datos son:

- Nombre y apellido
- Domicilio
- Dirección de correo electrónico
- Rol Único Tributario (RUT)
- Dirección de Protocolo de Internet (IP)
- Datos de Localización
- Cookie ID
- IMEI de los teléfonos celulares
- Datos que tenga un doctor o un hospital, los que podría identificar de forma única a un individuo

Con esto podemos entender que existen diversos tipos de datos personales, y que son éstos los que la ley busca proteger, aunque no son taxativos, ya que existen otro tipo de datos personales como los biométricos, referidos principalmente a aspectos físicos de las personas[17] y también con los avances tecnológicos no es difícil pensar en que podrán de surgir otro tipo de datos personales en el futuro. Sin embargo, como ya se mencionó anteriormente, todos estos datos corresponden a una persona física viva identificada o identificable.

1.4 Historia de la protección de datos personales

Podemos indicar como el origen o inicios de la protección de datos personales el estudio de "The Right to Privacy", escrito por Louise Brandeis y Samuel Warren en 1890. Sin embargo, para muchos el punto inicial de esta materia es el reconocimiento oficial de la privacidad o vida privada como derecho humano, cosa que se reconoce en la declaración universal de derechos humanos del año 1948 de las Naciones Unidas. En esta, específicamente en su artículo número 12, se establece que "Nadie será objeto de injerencias arbitrarias en su vida privada (…), 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". Lo importante de esto es que se le da al derecho a la privacidad un reconocimiento explícito como derecho fundamental, además de servir como catalizador para nuevas legislaciones sobre derecho a la protección de datos y la privacidad.

[17] Por ejemplo, el escaneo de retinas o las huellas dactilares.

Podemos avanzar incluso en el tiempo a nivel global y ver que todavía no se habla del derecho a la protección de datos, ya que el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, en Pacto Internacional de Derechos Civiles y Políticos, y en la se Convención Americana de Derechos Humanos de 1969 se sigue hablando de la protección de la vida privada, y no surgía un atisbo sobre la protección de datos personales, lo que denota que para la época en que estos instrumentos internacionales se redactaron los avances tecnológicos no representaban el riesgo de la información personal como sucede hoy en día[18].

Sin embargo, en 1988 el Comité de los Derechos Humanos de las Naciones Unidas (Comité en adelante), se pronuncia en su Observación General Número 16 respecto al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, donde se hace referencia al concepto de "vida privada", pero en esta Observación se hace referencia al "derecho a la intimidad"[19].

En este pronunciamiento, se realiza un análisis completo sobre lo que debe de entenderse por injerencias legales y arbitrarias de la vida privada, que se entiende por familia y domicilio y otros puntos, pero en ninguna parte de este artículo se define lo que debe de entenderse como vida privada o derecho a la intimidad. Respecto al tema de los datos personales, esta observación si realiza un pronunciamiento respecto a este en su numeral 10, el cual indica que:

"La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y por que nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales

[18] (López-Torres, 2014, pág. 108)
[19] *http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html*

incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación".

De esto podemos desprender que, en términos generales, el Comité indica que la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto del sector público como privado, deben de adoptar medidas para que la información relativa a la vida privada de una persona no esté disponible para personas no autorizadas a ello. Establece además un "derecho de verificación", que consisten en que todas las personas tienen el "derecho a verificar" si hay datos personales suyos almacenados en posesión del sector público o privado, además de un derecho a saber que datos tienen almacenados de uno y el porqué de esto y un "derecho de rectificación o eliminación" en caso de que los datos personales sean incorrectos o se hayan obtenido de forma ilegal, respectivamente.

Lo planteado anteriormente por el Comité es sumamente relevante, ya que plantea los derechos básicos que toda persona tiene respecto del tratamiento de sus datos personales, aspecto reconocido en diversas regulaciones y que en la literatura de la materia de protección de datos personales se conoce como "el derecho a la autodeterminación informativa", que consiste en el derecho que tienen todas las personas para decidir qué se puede hacer o no con su información personal, lo que responde básicamente a las siguientes preguntas "¿Quién?, ¿Cómo? Y ¿para qué?"[20].

Siguiendo con esta temática, entre los años 1990 y 1991 se lleva a cabo en las Naciones Unidas el 45° período de sesiones de su Asamblea General, en la cual se aprobaron 269 resoluciones, siendo la relevante para nosotros la Resolución 45/95 del 14 de diciembre de 1990, por medio de la cual se aprueban los "Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales"[21]. En dicha resolución la Asamblea solicita a los gobiernos que: 1) tengan en cuenta dichos principios en sus leyes y reglamentos, 2) que las organizaciones gubernamentales, intergubernamentales y no gubernamentales observen dichos principios en el ámbito de su competencia, siendo así este uno de los primeros antecedentes en protección de materia de protección de datos personales. Estos principios rectores aprobados por la Asamblea

[20] (López-Torres, 2014, pág. 109)
[21] https://www.informatica-juridica.com/anexos/directrices-de-proteccion-de-datos-de-la-onu-de-14-de-diciembre-de-1990/

General fueron: Licitud, lealtad, exactitud, finalidad, acceso, no discriminación y seguridad; con los cuales se sientan la base para esta materia, ya que como hemos dejado claro previamente, no existía un instrumento internacional que regulara específicamente esta.

Por otro lado, es importante mencionar que la Organización para la Cooperación y el Desarrollo Económico (OCDE), también tuvo un rol bastante trascendental para esta materia. Si bien su enfoque es el desarrollo económico, en el seno de esta misma se percibió este mismo problema, debido principalmente a las diversas estrategias de desarrollo en materia de comercio que empezaron a surgir en la segunda mitad del siglo XX, particularmente en el comercio electrónico, ya que este implica tanto el intercambio, manejo, uso y tratamiento de datos personales.

Así, en el contexto de la sociedad de la información, en donde el comercio electrónico es utilizado de forma cotidiana, donde existe el gobierno electrónico, donde se realiza de forma continua el tratamiento de datos personales; fue necesario plantear estrategias que garantizaran el tratamiento de la información personal con estricto apego a los derechos humanos y así salvaguardar a la dignidad de las personas sin que esto llegará a representar un retraso en la utilización de las nuevas tecnologías, idea que será clave cuando discutamos el alcance del principio de finalidad, ya que nos pone entre la espada y la pared, la dignidad humana o las nuevas tecnologías.

Por lo dicho anteriormente, además de para que los Estados pudieran adecuar sus marcos jurídicos y establecer las garantías mínimas de protección de los derechos humanos y en particular el derecho a la privacidad y la protección de la información personal, es que la OCDE adopta en 1980 las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales"[22], ya que el problema no radicaba en el manejo de información personal, sino que en la escasa regulación que existía respecto a esta misma.

Estas directrices se enfocan en el tratamiento de datos personales sin distinguir entre sector público y privado y plantean las siguientes directrices: de limitación de recogida de datos personales; de calidad de los datos personales; de especificación del propósito de la recogida de datos personales; de limitación del uso de los datos personales; de salvaguardia de la seguridad

[22] https://www.oecd.org/sti/ieconomy/15590267.pdf

para proteger los datos personales; de transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales, de participación individual y de responsabilidad sobre todo controlador de datos personales. Como podemos apreciar, estos fueron usados de base para la directiva 45/95 y las regulaciones posteriores de tratamiento de datos personales, ya que, si bien se cambiaron algunos nombres o se mezclaron algunos de estos, se siguen manteniendo las ideas generales de estos principios en la legislación de regulación de datos personales.

Como podemos ver, la historia de la protección de datos es sumamente reciente. En 1890 con el estudio de "the right to be let alone" se sienta la base general de privacidad y esta resurge con mayor fuerza en 1948 en la DUDH en donde se establece la protección a la vida privada, derecho que seguirá apareciendo en diversos instrumentos internacionales reafirmando así su importancia.

Por otro lado, recién en 1980 surgen las primeras legislaciones respecto a datos personales como tal, siendo la primera las directrices de la OCDE, esto en respuesta al rápido desarrollo del comercio electrónico y al gobierno electrónico, ya que en ambas se utilizaba de forma constante el tratamiento de datos personales, y a la nula regulación existente en esta materia en aquellos años. Con estas directrices buscaban resguardar los derechos de las personas ante los avances tecnológicos.

Finalmente, en Europa en 1990 se aprueba la directiva 45/95 en la cual se sientan por primera vez las bases sobre la protección de datos personales a nivel continental. Por último, es relevante mencionar que en la actualidad está vigente en Europa el Reglamento General de Datos Personales (RGDP) el cual entró en vigor el 23 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dando un plazo de dos años para que los países y empresas se adaptaran para su cumplimiento.

1.4.1 La protección de datos personales en Europa

Si bien ya hemos hablado bastante de la historia universal de la protección de datos personales en el apartado anterior, considero que es necesario hablar sobre Europa y su desarrollo jurídico en esta materia.

Como sabemos, es en 1948 con la DUDH en donde se establece que la privacidad es un derecho humano fundamental, específicamente en el artículo 12 de dicha declaración, pero sin adentrarse

mucho en el qué es específicamente la privacidad. Esta es para muchos el inicio de la protección de datos en Europa, pero aun faltarían décadas para que este se desarrollara como tal.

La idea de tratamiento de datos como tal surge en Europa en la década del 60, específicamente en mayo de 1967 en la Conferencia de Juristas Nórdicos en la cual se establece que las emergentes Tecnologías de la Información y la Comunicación (TIC en adelante) pueden llegar a generar graves perjuicios en la privacidad del ser humano y aconsejan que aparezcan o se creen regulaciones que manejen esta materia en los diversos países del continente. En virtud de esta recomendación, el Consejo de Europa realiza un estudio de estas nuevas tecnologías y de los derechos básicos y elementales de las personas, estudio que culmina en la resolución 65/509/CE sobre "los derechos humanos y los nuevos logros científicos y técnicos" en el año 1968. Esta resolución llega a la ONU en el mismo año, y esta emite en diciembre de 1968, durante su 23° período de sesiones, la resolución 2450 (A/RES/2450 (XXIII))[23] en la cual se establece la necesidad de fijar límites a las aplicaciones de la electrónica, esto a fin de respetar la vida privada, la protección de los derechos de las personas y buscar el equilibrio entre el progreso científico y técnico y la elevación intelectual, espiritual, cultural y moral de la humanidad.

Posterior a esto, el 23 de enero de 1970, la misma asamblea consultiva del Consejo de Europa emite la resolución 428 titulada "intimidad como un objeto de la obligada protección frente a la intromisión de la tecnología de la información", en la cual se ahonda mayormente sobre esta materia y generando aún más resoluciones de este mismo Consejo, siendo las más relevantes la del año 1973 sobre "protección de la vida privadas de las personas físicas frente al sector privado" y la del año 1974 sobre "protección de la vida privada de las personas físicas frente al sector público". Estas dos resoluciones son bastante relevantes, ya que es en estas en donde se hacen la diferenciación entre el seguimiento privado y el seguimiento público, diferencia que se mantiene hasta ahora y ha generado la creación de diversas instituciones en diversos países para la protección de datos, estas aparte del Estado, a fin de que se ejerza un cierto control sobre este último y que este no se extralimite en sus capacidades.

Siguiendo este hilo, en 1980 el Consejo de Ministros del Consejo de Europa proclama en convenio 108, el cual se titula "Convenio para la protección de la persona respecto al tratamiento

[23] https://undocs.org/es/A/RES/2450(XXIII)

automatizado de datos de carácter personal", cuya vigencia comenzaba en 1981. Este convenio es un punto clave para la historia de tratamiento de datos personales, ya que es con este se buscó por primera vez crear un instrumento internacional jurídicamente vinculante en este campo. Con este convenio se buscaba garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente el derecho a la vida privada, con el respeto al tratamiento automatizado de los datos de carácter personal de dichas personas, además de establecer en el mismo las definiciones de datos personales, ficheros y tratamiento automatizado y la autoridad controladora del fichero. Este fue posteriormente complementado con el Protocolo Adicional del año 2001 a fin de ampliar su ámbito de aplicación, aumentar el nivel de protección de datos y mejorar su eficacia.

Finalmente, en octubre de 1995, tanto el Consejo como el Parlamento Europeo decidieron, con base en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, adoptar la Directiva 95/46/EC a fin de proteger a las personas físicas respecto al tratamiento de sus datos personales y la libre circulación de la misma, esto mejor explicitado en el artículo 1 de la misma, en la cual se establece que los Estados miembros deberán de proteger, en particular, el derecho a la vida privada en lo que respecta al tratamiento de datos personales.

El objetivo central de esta directiva era el estandarizar las prácticas de los diversos países en materia de protección de datos personales, estableciendo principios (entre los que se encuentra el principio de finalidad limitada), derechos y obligaciones a quienes sean los responsables de dicha información (definidos como los responsables), esto atendiendo a la realidad internacional en relación al flujo transfronterizo de dichos datos con motivo de desarrollo de las economías, pero sin dejar de defender los derechos de las personas. Es decir, fue una medida de equilibrio en la Unión Europea, la que buscaba mantener el equilibrio entre el desarrollo económico de los países miembros y el respeto a los derechos humamos de las personas. Por ende lo que se buscó principalmente fue que se crearan diversas estrategias comerciales tanto nacionales como internacionales que implicasen el tratamiento de datos personales, pero que estas mismas no pasaran a llevar los derechos de las personas.

Finalmente, entrando a nuestro siglo actual, hay que destacar dos nuevos hitos en el campo de tratamiento de datos. El primero de estos fue en el año 2000 en Niza, en donde el Parlamento

Europeo, el Consejo de la Unión Europea y la Comisión Europea proclaman la Carta de Derechos Fundamentales de la Unión Europea[24], carta en la cual en su artículo 8 se reconoce el derecho de las personas a la protección de los datos de carácter personal que les conciernen, estableciendo que esta se tratará de forma leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, aunando de los derechos de acceso y rectificación, los cuales cuyo cumplimiento deberán ser velados por una autoridad competente. Así, la Carta de Derechos fundamentales de la Unión Europea se ha transformado en un instrumento de referencia para otros Estados[25], ya que en este por primera vez se consolida la autonomía e independencia del derecho a la protección de datos personales respecto del derecho de la vida privada, todo esto a un nivel regional.

Por último, en el año 2016 se adoptó en la Unión Europea el Reglamento General de Datos Personales[26] (RGDP en adelante), reemplazando a la Directiva 95/46/EC en la materia de regulación de datos personales. El objetivo del RGDP es el de incrementar el control de los individuos y los derechos de las personas sobre sus datos personales, además de simplificar el ambiente regulatorio para el comercio internacional. Otro aspecto de esta es que al ser una regulación y no una directiva es directamente vinculante y aplicable, pero la misma da flexibilidad en ciertos aspectos de la regulación, a fin de que la misma se pueda adaptar a cada país miembro. Actualmente y a la fecha, esta es la regulación vigente en Europa en materia de datos personales, y será junto a la directiva 95/46/EC los instrumentos de los cuales tomaremos el principio de finalidad limitada y analizaremos el alcance que posee.

1.5. Los Principios de la Protección de Datos personales

Como se mencionó anteriormente, respecto a la protección de datos personales surgieron diversos instrumentos para regularla a través del tiempo, como las directrices de la OCDE, el convenio 108, la Directiva 95/46/EC y la RGPD. Si bien todos estos instrumentos tenían distintos alcances legales, todos estos establecieron regulación para esta materia, y todos partiendo de una misma base, está siendo la de crear o establecer principios para esta misma. Estos principios generales son: Limitación de recogida, calidad de datos, especificación del

[24] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE
[25] En Chile por ejemplo se reconoce a nivel legal la protección de datos personales en la ley 19.628 y a nivel constitucional (art. 19 N°4)
[26] Fue adoptada en 2016, pero empezó a ser de aplicación el año 2018, dando un margen de dos años para que los organismos e instituciones se adaptaran al mismo.

propósito, limitación del uso, transparencia, salvaguarda de la seguridad, participación individual, responsabilidad y licitud de los datos. Si bien podemos ver que algunos instrumentos tienen más principios que otros, estos generalmente son los mismos e incluso se tienden a mezclar ambos para generar principios más robustos, pero la idea central es la misma.

Actualmente, y siguiendo al RGDP que es el vigente a la fecha en la Unión Europea, podemos encontrar los principios de esta materia en su artículo 5 (1) de la siguiente forma:

Artículo 5

Principios relativos al tratamiento

1. Los datos personales serán:
    a. Tratados de manera lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia)
    b. Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (…) (limitación de la finalidad)
    c. Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)
    d. Exactos y, si fuese necesario, actualizados (…) (exactitud)
    e. Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (…) (limitación del plazo de conservación)
    f. Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad)
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva).

Como podemos apreciar, en este artículo y sus 6 letras podemos encontrar seis principios, que son el marco dentro del cual se desarrolla todo el tratamiento de datos personales. Además,

podemos apreciar que estos se encuentran indicados de forma bastante simplificada y son fáciles de entender.

1.6 Conclusiones

Como podemos ver, la historia de la protección de datos personales es joven pero llena de contenido y de diversos actores. Indicamos que el génesis de la protección de datos personales data al estudio The Right To Privacy, estudio en el cual se establece por primera vez el derecho a la privacidad. Es en virtud de este estudio que recién podemos empezar a hablar de privacidad, noción que irá evolucionando en el siglo XX y luego permitirá el desarrollo de la protección de datos personales. Sin embargo, creo necesario destacar que la privacidad es un concepto que, si bien es protegido por el ordenamiento jurídico, no tiene una definición universal, esto debido principalmente a que esta abarca tantos campos que al tratar de encasillarla en un área específica dejaríamos de lado otra. De esta idea podemos desprender que la protección de datos surge como una de las tantas acepciones que se le puede de dar a la privacidad, pero que como vimos posteriormente en los puntos 1.4 y 1.4.1 esta se desprendió de esta misma y se comenzó a desarrollar como un área independiente con su propia regulación. Sin embargo, a pesar de esta separación no podemos de dejar de relacionar ambos conceptos, ya que, a nivel de derechos fundamentales, estos se encuentran fuertemente vinculados.

Respecto al desarrollo de la protección de datos personales, podemos destacar diversos organismos e instrumentos, los que aportaron con su pizca de ideas, conceptos y principios y ayudaron a forjar el RGDP, instrumento que actualmente está vigente en la UE y se considera como el marco de regulación de esta materia en Europa. Estos actores fueron la OCDE, el Convenio 108 y la Directiva 95, instrumentos sobre los que ahondaremos en el próximo capítulo, pero bajo la perspectiva del principio de finalidad limitada.

Capítulo 2: Análisis de los elementos del principio de finalidad

En el primer capítulo hablamos largamente sobre los orígenes de la protección de datos personales. Hablamos de su origen en el concepto de privacidad y su evolución a lo largo del siglo XX en el mundo y como incluso esta llegó a desarrollarse como un derecho aparte del de privacidad. Hablamos también de los diversos instrumentos en los que apareció y como estos se fueron consolidando hasta la actualidad, dándonos a entender que existe todo un marco regulatorio de esta materia.

En este capítulo, sin embargo, ya no hablaremos de la protección de datos personales de forma general, sino que nos enfocaremos solamente en el principio de finalidad que mencionamos anteriormente, y específicamente en sus elementos a fin de que podamos entender en que consiste principalmente este principio y cuál es su función. Para esto, primero veremos la evolución histórica de este principio y como fue cambiando en los diversos instrumentos que lo mencionaban. Luego de esto, tomaremos la noción actual del principio de finalidad y la analizaremos en partes separadas para un entendimiento completo de sus elementos.

2.1 Evolución del marco legislativo del principio de finalidad

Antes de analizar los elementos de este principio, creo que es necesario un repaso histórico de este principio, a fin de que entendemos la noción actual del mismo. Hablaremos brevemente de la evolución legislativa del principio de finalidad limitada buscando ver su evolución en el transcurso de los años.

2.1.1 Convención Europea de Derechos Humanos (CEDH)

Como indicamos anteriormente, en la Convención Europea sobre los Derechos Humanos adoptada en 1953 se estableció el derecho a la privacidad en su artículo 8, el cual indica que se debe de respetar la privacidad de todos y la vida familiar, hogar y correspondencia. Prohíbe además cualquier interferencia con el derecho a la privacidad de las personas, salvo casos en donde “se haga acorde a la ley” y “sea necesario en una sociedad democrática”, a fin de así satisfacer ciertos casos específicos a favor del interés público.

Como podemos ver, el artículo 8 de la ECHR se enfoca en la protección de la vida privada, y requiere que exista algún tipo de justificación para su interferencia. Por ende, entendemos que la regla general consiste en la prohibición a la intervención del derecho a la privacidad, y que se permiten ciertas excepciones a esta en casos estrictamente definidos. En estos casos donde se

busca realizar una intervención al derecho a la privacidad, se requiere de una base legal, además de la especificación de un propósito legítimo como precondición para ver la necesidad de la intervención.

Como podemos ver, los conceptos de "base legal" y "limitación del propósito" aparecen por primera vez como una forma de justificar una intervención a la privacidad, esto acorde al art. 8 de la ECHR, pero se desarrollan aún más en los casos de ley privada vistos por la Corte Europea de Derechos Humanos.

2.1.2 Convenio 108

En 1981 entra en vigor el Convenio 108, creado por el Consejo de Europa. Es en este Convenio es donde se introduce y habla por primera vez del concepto de "protección de datos" a nivel continental[27]. Respecto al principio de finalidad, este convenio lo elabora de una forma bastante proactiva: "Los datos de carácter personal que sean objetivo de un tratamiento automatizado: se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades[28]".

Podemos decir que lo establece como uno de los principios clave sobre la protección de datos. Con esto se establece otro punto relevante de este principio: se requiere de una base legal y de la especificación de un propósito legítimo en toda circunstancia que se quiera procesar datos personales, sea tanto en el sector público como privado.

Como sabemos, el Consejo de Europa se basó en distintos instrumentos previos para la elaboración de este Convenio, donde destacan tanto la resolución (73) 22 y la resolución (74) 29, resoluciones que hablaban sobre la protección de datos personales, pero que diferenciaban esta misma para el ámbito privado (73) y el público (74).

La resolución 73 del Consejo de Europa requería que la información fuese "apropiada y relevante respecto al propósito por la cual fue almacenada" y que -a falta de una "apropiada autorización"- se prohibiese su uso "para propósitos distintos a aquellos para los que fueron recopilados" así como a su comunicación a agentes externos.

[27] Previamente países como Alemania y Dinamarca habían establecido sus propias leyes sobre protección de datos, las que sirvieron igual para la creación de este convenio.
[28] https://rm.coe.int/16806c1abd

Por otro lado, en el ámbito del sector público, la resolución (74) tomaba una aproximación diferente. Si bien existían reglas similares que indicaban que la información almacenada fuese apropiada y relevante para el propósito para el que fue almacenada, se incluía una provisión específica que permitía el cambiar el propósito en casos específicos. Esta provisión indicaba que la data podrá ser usada para otros propósitos aparte de aquellos para los que fueron definidos, si esta excepción está "explícitamente permitida por la ley, es permitida por una autoridad competente, o bien si las reglas para el uso de bancos de data electrónico son cambiadas".

Tomando en cuenta ambas resoluciones, podemos dividir al convenio 108 en dos partes distintas a la hora de hablar del principio de finalidad. En primera instancia, en su artículo 5, el Convenio establece los principios fundamentales para la protección de datos, en donde podemos encontrar la legalidad, proporcionalidad y lealtad, pero también la especificación del propósito y el requerimiento de que dicho propósito sea legítimo, reconociendo al principio de finalidad. Por otro lado, también introduce la idea de incompatibilidad, ya que establece que la data no podrá ser usada de "forma incompatible" con los propósitos ya especificados. Finalmente, y haciendo hincapié a lo indicado en la resolución (74) 29, en su artículo 9 el Convenio indica que es posible una derogación a esta provisión de "uso incompatible" solo sí esto es "permitido por la ley" y reafirmado posteriormente de que esto es "necesario en una sociedad democrática", realizando también una analogía cercana a lo establecido en el artículo 8 de la Carta Europea de Derechos Humanos.

Desde la perspectiva del principio de finalidad, podemos destacar que es desde este Convenio que se ha reconocido a este principio como un elemento esencial de la protección de datos, transmitiéndose esta idea a los posteriores instrumentos regulatorios de esta materia. También es este convenio el que agrega la noción de "no incompatibilidad", la cual se ha mantenido vigente desde la adopción de este Reglamento.

Actualmente, este convenio sigue vigente, actualizado, y sirve también para entender de manera más completa el marco regulatorio de la protección de datos personales.

2.1.3 Directivas OCDE

En paralelo a la Convención 108 de 1981, la OCDE desarrolló líneas de guiamiento en el ámbito de la protección de datos personales, esto principalmente al boom del comercio electrónico de la época y a la necesidad de regular, al menos en un rango básico, este misma. Estos lineamientos

contienen las mismas ideas de la Convención 108 respecto a la especificación del propósito y a la incompatibilidad, pero estas definen la idea de incompatibilidad de forma distinta.

Respecto al principio de finalidad, esta directiva lo describe de la siguiente forma: "Principio de especificación del propósito", que consiste en que "el propósito de la recogida de datos deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo"[29].

Como podemos ver, establece dos ideas clave. La primera es que se debe de especificar el propósito para el que se tratarán los datos a más tardar al momento de que estos sean recolectados, y segundo, que, acorde a estos lineamientos, si se permite el tratamiento posterior de los datos recopilados para propósitos distintos a la inicial, siempre y cuando estos nuevos propósitos no sean incompatibles con el propósito original y que se especifique estos nuevos propósitos cada vez que ocurra este cambio. Finalmente, estos lineamientos también hablan de dos excepciones a este requerimiento de uso compatible: cuando el sujeto de data de su consentimiento, o bien cuando sea por la autoridad de la ley.

Como podemos ver, si bien existen diferencias en el concepto de uso compatible y las excepciones a este mismo, es relevante destacar que el principio de finalidad limitada es también sumamente importante a la hora de hablar de protección de datos, ya que aparece ser un elemento estable en el contexto internacional y se ha mantenido firme en los lineamientos de la OCDE respecto a esta materia.

2.1.4 Directiva 95/46/EC

Adoptada en 1995, esta Directiva se construyó basándose en instrumentos previos como el Convenio 108 y las directrices de la OCDE, aparte de que también se consideró para su elaboración la experiencia previa de países miembros en esta materia para su elaboración.

Respecto a los instrumentos previos, en cada uno de estos se hablaba del principio de finalidad limitada de forma distinta, y con respecto a esta Directiva, sus elaboradores decidieron de darle su propio sello. Este fue el que se tomó la decisión de no realizar diferenciación alguna a la hora de hablar de tratamiento de datos, es decir, no se realizaba diferencia si esta se realizaba en el

[29] https://www.oecd.org/sti/ieconomy/15590267.pdf

ámbito privado o el público estableciendo que el requerimiento de especificar el propósito se aplicaría a ambos ámbitos sin distinción.

Además de esta decisión, la Directiva incluye también un nuevo requerimiento para la especificación del propósito que previamente no había sido establecida en los lineamientos de la OCDE o en el Convenio 108 previamente: "el propósito debe ser explícito".

Finalmente, la Directiva 95 incluyó también una provisión para el tratamiento posterior de datos con fines históricos, estadísticos o científicos; donde se menciona que estos no se considerarían incompatibles siempre y cuando los Estados Miembros aseguraran tomar las medidas necesarias para esto. Esta noción no era del todo nueva, ya que ambas resoluciones (73) 22 y (74) 29 ya contenían provisiones respecto al uso estadístico de datos. Los lineamientos de la OCDE al igual que el Convenio 108 en el cual se establecieron excepciones para el tratamiento de datos con fines científicos o estadísticos[30].

Otro aspecto importante de esta Directiva es que esta permitía a los Estados Miembros restringir el rango de algunos derechos y obligaciones en donde se incluía el principio de finalidad en el artículo 6(1)(b), indicando siempre que dicha restricción constituye una medida necesaria para asegurar ciertos intereses relevantes[31]. Esta provisión seguía la misma lógica que el artículo 9 de la Convenio 108.

Como podemos ver, en la Directiva 95 se sumaron diversos elementos, dando a conocer un principio de finalidad con diversos elementos, que se redactó de la siguiente manera: "Los Estados miembros dispondrán que los datos personales: recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerarán incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas[32]".

[30] Artículo 9(3) de la Convención. Este se aplicaba cuando "no exista riesgo obvio de violación de la privacidad de los sujetos de data". Respecto a los lineamientos de la OCDE, en el párrafo 55 de su Memorándum Explicatorio se indica que la ley podrá proveer que data que haya sido recolectada con propósitos de decisión administrativa podrán estar disponibles para planeamiento social, investigatorio o estadístico.
[31] Artículo 13 de la Directiva
[32] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046

2.1.4.1 Implementación de la Directiva

Respecto a la implementación de la directiva, se realizó un informe para su aplicación el año 2003, en el cual se concluyó que la implementación de algunas disposiciones de esta misma era a veces insatisfactoria, entre las cuales se incluía las salvaguardas para el posterior procesamiento de datos con fines de investigación.

Este informe también analizó de forma técnica el cómo se implementó el artículo 6 de la Directiva 85, artículo referido a los principios del tratamiento de datos, obteniendo los siguientes resultado. Este análisis concluyó que, si bien en gran parte de los Estados Miembros se mencionaba a la especificación del propósito y principio de limitación de forma similar a la Directiva, el carácter flexible de estos mismos principios llevaba a una aplicación divergente del mismo, y que dichas divergencias aparecían en diversos aspectos de estos conceptos. Por ejemplo, en algunos países había reglas específicas para el sector público; en otros se definía de manera muy amplia el concepto de propósito y finalmente, había también distinciones en como los Estados Miembros tacleaban el cómo hacer explícitos los propósitos, por ejemplo, si es necesario especificar el propósito en la notificación a la autoridad a cargo de la protección de datos o bien en el aviso al sujeto de datos. Respecto a las reglas sobre cambio del propósito, también queda demostrado en este estudio que también eran sumamente variables, al igual que las salvaguardas para dichos usos específicos.

Respecto a la incompatibilidad, este estudio indicó que el examen usado para determinar esta incompatibilidad variaba desde lo que se considera como “las expectativas razonables” del sujeto de datos hasta la aplicación de exámenes de balance, o bien estar íntimamente unido a las salvaguardas de otros principios como la transparencia, legalidad y lealtad.

Por lo tanto, podemos ver que esta directiva no logró unificar de forma clara los principios de protección de datos personales a lo largo del continente, pero que de todas formas sirvió como una base sólida para asegurar la protección de datos personales.

2.1.5 Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la Unión Europea fue proclama en el año 2000 en Niza, Francia. En el artículo 8 de esta Carta, se establece que la protección de datos es un derecho fundamental y diferente al respeto por la privacidad y la vida familiar, la que se protege en el

artículo 7 de la misma. Esto directamente diferenció a esta Carta de otros instrumentos sobre la materia de derechos humanos, ya que estos por lo general trataban a la protección de datos personales como una extensión del derecho a la privacidad. Esto queda del todo claro cuando comparamos esta Carta con la Convención Europea de Derechos Humanos del año 1950.

Desde la perspectiva del principio de la finalidad limitada, esta Carta establece claramente que la data personal debe ser "tratados de manera leal, para fines concretos". Agrega además como otro requerimiento una base legal legítima para este procesamiento. De forma concreta, el artículo 8 n°2 de esta Carta establece que "Estos datos se tratarán de manera leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Podemos señalar que al indicar este principio de manera textual, se acentúa aún más el rol del mismo en la protección de datos personales.

2.1.6 Reglamento General de Datos Personales (RGDP)

En la segunda década del siglo XXI la Unión Europea decidió, en base a diversos factores, crear un nuevo reglamento sobre datos personales. Diversas instituciones participaron en el desarrollo de este nuevo ordenamiento, destacando el rol del denominado "Working Party" establecido por el artículo 29 de la Directiva 94/45/EN que lo creaba a fin de que actuara como asesor respecto a materia de datos personales.

El objetivo central de la creación de este reglamento fue la unificación de la legislación respecto a la protección de datos en todos los Estados Miembros, además de elevar los estándares de esta misma para el continente y el resto del mundo, pudiendo así proteger a los usuarios frente al mal uso de sus datos.

Otro aspecto relevante de este reglamento es que involucra a países fuera de la Unión Europea, ya que además de establecer estándares superiores de privacidad para las empresas, este rige también a las empresas que no residen en Europa, pero que tratan los datos personales de residentes europeos. Es decir, otorga a los residentes de la Unión Europea mayor control sobre sus datos personales y exige que las empresas mantengan una protección adecuada de los mismos, a fin de resguardar y garantizar el derecho a la privacidad de las personas[33].

[33] Esto se define de mejor manera en el artículo 3 del RGDP, donde se establece el alcance del mismo instrumento

Respecto al principio de finalidad limitada, este reglamento lo mantiene como principio clave del tratamiento de datos, estableciéndolo en su artículo 5 b), en el cual se establece tanto la finalidad del propósito como la idea de incompatibilidad. También cambia un poco la lógica usada de la Directiva 95/45/EU, ya que agrega de forma directa al principio de finalidad la excepción a la incompatibilidad, siempre que este sea con fines históricos, científicos o estadísticos y asegurando a los sujetos de data todas las garantías o salvaguardas correspondientes, esto explicitado de manera más completa en el artículo 89 del RGDP[34].

Con este breve repaso histórico podemos ver claramente el cómo ha ido evolucionando el principio de finalidad limitada y como se entiende esto en la actualidad. En sus inicios, surge como una forma de permitir una invasión a la privacidad, esto porque se estableció en el artículo 8 de la Carta de Derechos Humanos de la Unión Europea que si se debiese de realizar alguna invasión a la privacidad esta debería de tener una justificación legal además de una especificación del propósito del porque se realiza esta. Además de esto, la relación entre protección de datos personales y el artículo 8 de la CEDH ha sido desarrollada por la CEdDH

Luego de esto podemos ver que se le suma otro componente al principio de finalidad en el Convenio 108, siendo este la noción de incompatibilidad y la prohibición de posterior tratamiento de datos si estos eran incompatibles, salvo en los casos que la ley permitiese específicamente este tratamiento y se otorgaran todas las medidas necesarias; y en la Directiva 95/45/EU se dejó de realizar la diferencia de tratamiento de datos para el sector público o privado, unificando así este principio y dejando que ahora tuviera un campo de aplicación general.

Finalmente, en la Carta de Derechos Fundamentales de la Unión Europea, se establece como derecho fundamental la protección de datos, separándolo así del derecho a la privacidad y se indica, en este mismo artículo el principio de la finalidad limitada, ya que se pone de forma explícita la idea de especificación del propósito y la necesidad de una base legítima para el tratamiento. En el RDGP del año 2016, se unifica toda la regulación de protección de datos personales en la Unión Europea y se eleva este mismo estándar de protección, y respecto a nuestro principio se establece claramente la necesidad de la especificación del propósito y la

[34] Este artículo se refiere a las Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

idea de incompatibilidad, además de que se agrega de forma directa a esta última la excepción, que viene a ser el tratamiento posterior con fines históricos, científicos o estadísticos.

2.2. Los elementos del principio de finalidad

Ya tras haber hablado de la evolución temporal del principio, ahora me remitiré a solo hablar de los elementos del principio de finalidad, a fin de entender en que consiste y que busca este principio. Para esto tomaremos la acepción actual de este, la cual es la del 5 (1) (b) del RGDP.

En este instrumento, se establece que el principio de finalidad consiste en que: "los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89 apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales"

Como podemos ya podemos una enorme cantidad de elementos dentro de este principio. Podemos ver los elementos de determinación, explicitud y legitimidad en una primera parte, y luego podemos ver la idea de no incompatibilidad para el tratamiento ulterior de datos. Finalmente, podemos ver una excepción establecida respecto al tratamiento ulterior de datos con fines de archivo en interés público, fines científicos, estadísticos e históricos (tratamiento privilegiado) establecido en el mismo artículo.

2.3. La especificación del propósito y la noción de no incompatibilidad

A fin de realizar un buen análisis del principio de finalidad, se dividirá en dos partes o componentes el principio de finalidad, usando la versión más actual de este mismo, que es la establecida en el RDGP, específicamente en el artículo 5 (1) (b). Estos dos componentes ya han sido mencionados previamente y estos son: 1) la especificación del propósito y 2) la noción de la incompatibilidad. Como último punto previo a este análisis, cabe destacar que la noción de base legal se considerará agregada dentro de la especificación del propósito.

2.3.1 Primer componente: Especificación del propósito

"los datos personales serán recogidos con fines determinados, explícitos y legítimos"

El artículo 5 (1) (b) del RDGP indica como requerimientos para la recolección de datos personales que estos tengan fines "específicos, explícitos y legítimos". Es decir, la data es

recolectada con ciertos fines claros, y estos fines son la razón de ser de las operaciones de procesamiento. La especificación del propósito también sirve como el prerrequisito para la aplicación de otros requerimientos o principios sobre la recolección de datos personales y también permite determinar que data ha de ser la recolectada (data relevante), el periodo por el cual esta será retenida y otros aspectos de como la data personal será procesada para dicho propósito escogido.

De manera breve, la especificación del propósito consta de 3 partes que son las siguientes:

Primero, el propósito debe ser especificado, es decir, este tiene que estar lo suficientemente definido para permitir la implementación de cualquier garantía de protección necesaria para el tratamiento de datos y además para delimitar el alcance del procesamiento.

Segundo, tiene que ser explicito, con esto nos referimos a que debe de estar claramente expresado y de forma inequívoca, es decir, que no genere dudas de su

Por último, el propósito debe ser legítimo. Esto va más allá de la necesidad de tener una base legal para realizar dicho procesamiento como indica el artículo 6 del RDGP y se extiende a otras áreas de la ley, como por ejemplo la no discriminación o uso indebido de la data. Tenemos que indicar que la idea de especificación del propósito del artículo 5 y el requerimiento de una base legal del artículo 6 son dos requerimientos separados y cumulativos.

2.3.1.1 Prerrequisitos para otros requerimientos de calidad de data

Cuando aplicamos la ley de protección de datos, debemos de entender que hay que seguir cierto orden. Primero tenemos que asegurarnos que el propósito por el cual se tratan los datos debe de ser específico, explícito y legítimo. Ya con esto, podemos empezar a aplicar otros principios de la protección de datos como la licitud, lealtad y transparencia (art. 5 a)), minimización de datos (art. 5 c)), exactitud (art. 5 d)), limitación del plazo de conservación (art. 5 e)) e integridad y confidencialidad (art. 5 f)). Como podemos ver, este principio de la limitación de la finalidad es la piedra angular para aplicar el resto de los principios de protección de datos, ya que estos sólo pueden ser aplicados una vez que entendamos el propósito por el cual se tratan los datos.

En el caso en que existan diferentes propósitos desde el principio y se traten distintos tipos de data de forma simultánea, los requerimientos de calidad de data se aplicarán de forma separada para cada propósito.

Finalmente, en el caso en que se procese data con otros propósitos esta deberá de:

- Especificarse el/los nuevo(s) propósito(s) y,
- Se deberá asegurar que se cumplen con otros los otros requerimientos de calidad de data sean satisfechos para los nuevos propósitos.

2.3.2 Segundo Componente: uso compatible

El artículo 5 b) del RDGP indica también que los datos "no serán tratados ulteriormente de manera incompatible con dichos fines". Con esto introducimos la idea de tratamiento posterior de datos y la noción de incompatibilidad. Esta prohibición de uso incompatible es la que pone la limitación para el tratamiento posterior de datos, por ende, se requiere que se haga una distinción entre uso posterior que sea "compatible" y uso posterior que sea "incompatible" y por ende prohibido. Esto se analizará de manera posterior en otra sección, donde se hablará del criterio usado y marco general para realizar esta diferenciación.

Sumando a este análisis posterior que se hará, también se hablará de la provisión especifica referida al procesamiento posterior con fines históricos, estadísticos o científicos. Finalmente, creo necesario indicar que cuando se empezaron a realizar estudios para la implementación del RDGP, la WP indicó que existía cierto debate respecto a esta provisión, ya que no quedaba claro si esta era una excepción a la a la prohibición de incompatibilidad a favor de darle una posición privilegiada a estos propósitos o si bien era una especificación de la regla general, pero no excluyendo otros casos que podrían considerarse como "no incompatible". Sin embargo, con la implementación del RDGP se zanjó este asunto, ya que se siguió la recomendación de la WAP y se incluyó esta provisión de forma directa en el artículo 5 b), por lo que queda claro que esta provisión específica generó un aumento del criterio general de compatibilidad, pero también se estableció en el artículo 89 las correspondientes garantías para esta provisión.

2.4. Primer componente: Especificación del propósito

Hemos ya mencionado diversas veces la noción de "especificación del propósito", pero no hemos definido a que nos referimos con esta. Con esta nos referimos principalmente a la primera parte del principio de finalidad, el cual actualmente se refiere a tres puntos centrales: especificación, determinación y legalidad. Estos componentes serán analizados uno por uno a fin de que quede claro el alcance de este primer componente, posteriormente, en el apartado 3.4

de este trabajo se hablará del rol que cumple y la relación que tiene este con los demás principios de la protección datos.

El artículo 5 b) (1) del Reglamento General de Datos Personales indica que los datos personales deben ser recopilados con fines determinados, explícitos y legítimos.

2.4.1 El propósito debe ser determinado

Los datos personales deben ser recopilados para fines determinados. Esto nos pone dentro de la perspectiva del controlador de datos o responsable del tratamiento[35], ya que es él quien debe considerar con que propósito o propósitos para los cuales usará la data personal y así evitar recolectar data personal que no sea necesaria, relevante o adecuada para dichos propósitos que intentan cumplirse. Esta idea se relaciona directamente con el principio de minimización de datos del art. 5 (1) (c) RGDP.

Como mencionamos anteriormente, la especificación del propósito es la piedra angular para la aplicación del marco legal de protección de datos, ya que a fin de determinar si el procesamiento de datos es acorde a la ley o bien para establecer las garantías o salvaguardas correspondientes de protección a los datos es totalmente necesario indicar el propósito para el cual los datos personales son recolectados. Por lo tanto, la especificación del propósito establece los límites respecto al propósito para el cual los controladores podrían usar los datos personales recolectados, y también aporta al establecimiento de las garantías necesarias para la protección de datos.

2.4.1.1 ¿Cuándo se ha de especificar los propósitos?

Respecto a esto, y en virtud de lo dispuesto en el artículo 5 b) y el considerando 39, es posible inferir que los propósitos deben ser especificados previo a, o como máximo, al tiempo en el que se realiza la recopilación de datos. Esto es un tema bastante curioso, ya que no se indica de forma directa en el artículo 5 b del RGDP el cuándo ha de informarse los fines para la recopilación de datos, pero si se indica que estos deben de "determinarse en el momento de su recogida" acorde a lo establecido en el considerando 39 del mismo. Por otro lado, en directrices de la OCDE, que tenía más que nada un rol meramente regulatorio para el campo comercial, se indica que "el propósito de la recogida de datos deberá especificar a más tardar en el momento

[35] Este se define como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto a otros, determine los fines y medios del tratamiento. Art. 4 (7) RGDP.

en que se produce dicha recogida", dejando en claro que se debe de especificar este como máximo al momento de la recogida.

2.4.1.2 ¿Con cuanta precisión y detalle se debe de especificar el propósito?

El propósito de la recogida de datos debe ser claro e identificable, debe ser lo suficientemente detallado para determinar qué tipo de procesamiento es el adecuado para dicho fin específico y permitir el cumplimiento de la ley y de aplicación de las salvaguardas pertinentes.

Por ende, en los casos en los que los propósitos suelen ser vagos o muy amplios como por ejemplo "mejorar la experiencia de usuarios o fines de mercado" normalmente no cumplen con este criterio de ser específicos[36]. Con esto, podemos dejar en claro que el nivel de detalle en el que se debe de especificar el propósito para dicho tratamiento dependerá mucho del contexto para el cual se recopilen los datos personales. En algunos casos será suficiente un lenguaje simple para dar la especificación adecuada, mientras que en otros se requerirá de mayor detalle.

Sin embargo, este punto de que la información ha de ser precisa no significa tampoco que debamos de detallar de manera minuciosa las especificaciones del propósito, ya que esto incluso puede llegar a ser contraproducente. Un ejemplo de esto es el ocurrente con casos de documentos escritos en los que se hace un enfoque más legal y se mencionan "disclaimers", más que entregar la información necesaria a los sujetos de data o stakeholders.

Por ende, la mejor aproximación a esta situación es la de usar lo que se denomina como "layered approach", que consiste principalmente en que se les otorgue a los sujetos de data la información clave de forma concisa y amigable, mientras que la información adicional sea proveída a quienes consideran que requieren una mayor clarificación. Esto es bastante útil sobre todo en el Internet, ya que la gran mayoría de sitios normalmente indican, cuando uno entra por primera vez a ellos, el fin para el que recopilaran tu data e incluyen un link aparte para más información.

2.4.1.3 ¿Qué ocurre si la data se está recopilando con más de un propósito?

Sabemos que la data personal puede ser recopilada con más de un propósito y que estos, en algunos casos, aunque sean distintos tienen cierto grado de relación o bien puede que no tengan relación alguna. Es en estos casos que surge la interrogante sobre hasta qué punto el responsable

[36]Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág. 16

debe de especificar cada uno de estos propósitos de forma separada y cuanto detalle ha de dar de cada uno.

En el caso de que los propósitos tengan alguna relación, el identificar cual es el propósito general o quienes realizan que operaciones puede ser útil; sin embargo, los controladores han de evitar identificar todo bajo un solo propósito específico a fin de justificar distintos procesamientos posteriores que solo se relacionen de forma remota al actual propósito inicial[37].

Finalmente, a fin de asegurar el cumplimiento del artículo 5 b) del RGDP, cada propósito debiese ser especificado de forma individual, con el suficiente detalle que permita asegurar que dicha recolección de data para dicho propósito sea acorde a lo establecido en la ley y que además puedan establecerse las salvaguardas necesarias para estos.

Es por esto por lo que podemos indicar que en casos en que se procese data con diferentes propósitos, se deben de aplicar todos los requerimientos del artículo 5 a cada uno de estos propósitos específicos. Junto a esto, también debemos mencionar que no toda la data recolectada para un propósito "a" será relevante o útil para un propósito "b", sea o no relacionado con el anterior e identificado al momento de su recolección o de forma posterior. En estos casos lo que se debe de hacer es analizar caso por caso, tanto en la etapa inicial como en el momento en que se indique un nuevo propósito.

2.4.2 El propósito debe ser explícito

Los datos personales deben ser recopilados con fines explícitos. Con esto nos referimos a que no solo debe tener el controlador claro por qué recopila estos datos, sino que estos también tienen que estar establecidos de forma clara, explicados o bien expresados de alguna forma inteligible para los demás. Al igual que la determinación, el propósito debe de estar explicitado a más tardar a la hora en la que se recopilan los datos.

Lo que se busca con esto es que el propósito por el cual se recopilan los datos sea indicado de forma clara, o mejor dicho sin ambigüedad o incertidumbre respecto a su fin o intención. Con esto se busca que la especificación del propósito no solo sea clara para los que realizan el

[37] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág. 16

tratamiento de data, sino que esta especificación también sea clara para las autoridades y para los sujetos de data envueltos en dicho tratamiento[38].

Haciendo alusión a los conceptos relacionados con el principio de finalidad, podemos indicar que este requerimiento de que el propósito sea específico contribuye altamente a la transparencia y a la predictibilidad, que mencionamos anteriormente. Esto se debe a que al indicar de forma clara el propósito para el cual se recolectan los datos, podemos limitar el uso de la data personal por parte de los controladores, además que permite que todos los otros sujetos parte de este procesamiento, como quienes procesan la data para el controlador, los sujetos de data y las autoridades sobre protección de datos personales y otros stakeholders tengan un entendimiento claro de cómo se usará dicha data. De esta forma, se reduce el riesgo de que las expectativas de los sujetos de data difieran de las expectativas del controlador. Respecto al control de usuario, este requerimiento permite en muchas situaciones que los sujetos de data tomen decisiones informadas.

2.4.2.1 ¿De qué forma y a quien se le debe de explicitar el propósito?

El requerimiento de que el propósito sea explícito es distinto a los requerimientos de información que se le deben dar a los sujetos de data y al requerimiento de notificar a una autoridad supervisora. Sin embargo, estos tres requerimientos están estrechamente relacionados y cada uno permite que se cumpla con la transparencia.

Respecto a lo dispuesto en el artículo 9 del RGDP se entiende que existen diversas formas de expresar el propósito para el cual se recolectan los datos. Podemos tomar como ejemplo el notificar al sujeto de datos a través de un aviso o notificación, enviar una notificación a una autoridad supervisora o bien de forma interna en la información otorgada a los oficiales de protección de datos. Incluso, en algunos casos como el británico, se indica que tanto un aviso o una notificación pueden cumplir de forma concreta este requerimiento de indicar explícitamente el propósito, pero que existen otros métodos para hacerlo.

Es también relevante mencionar lo indicado en los Lineamientos de la OCDE, ya que estos se enfatizan en la idea de flexibilidad, indicando incluso de manera directa que la especificación del propósito puede realizar de diversas maneras complementarias o alternativas, como las

[38] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág. 17

declaraciones públicas, legislación, actos administrativos, etc. Lo que importa al final es la calidad y consistencia de la información proveída por el controlador.

Respecto a la responsabilidad del controlador, la especificación del propósito de manera escrita y la creación de la documentación necesaria permitirá demostrar que este mismo ha cumplido con los requerimientos del artículo 5 b). Por otro lado, también ayuda a los sujetos de data a ejercer sus derechos de forma más efectiva, ya que con dicha documentación podría de indicar prueba del propósito original de la recolección de datos y permitir comparar esta con cualquier procesamiento posterior. Siguiendo con esta idea de documentar la especificación del propósito podemos indicar además que esta resulta bastante útil e incluso necesaria en la actualidad, ya que hoy en día muchos procesamientos de data ocurren de forma obscura, compleja y en un contexto ambiguo, especialmente en lo que respecta al Internet. En esta situación es por ende necesario tomar especial medida para especificar los propósitos de recolección de forma clara y transparente.

Por otro lado, muchas veces el contexto y la costumbre serán suficientes para aclararle a todos los participantes el cómo se usará la data personal. Si esto es posible sin ningún tipo de riesgo de incertidumbre o ambigüedad, es posible entonces satisfacer las condiciones del artículo 5 b) con tan solo expresar los elementos esenciales, pero esto no quita el hecho de que aun deba de otorgarse más información para aquellos que la soliciten. Sin embargo, no siempre será necesario esta provisión de entregar información detallada a los sujetos de data en los casos donde estos puedan determinar de forma clara el propósito con solo el contexto y la costumbre. Existe también flexibilidad para que las leyes nacionales de protección de datos hagan excepciones respecto a la notificación de requerimientos en algunos casos.

2.4.2.2 ¿Qué pasa en los casos de grave incumplimiento de este requerimiento?

Es posible que el controlador falle el cumplir con los requerimientos del artículo 5 b) del RDGP. Un ejemplo de esto podría ser el caso en donde no especifique el propósito del procesamiento de datos de forma clara; que la información que entregue este mismo controlador no corresponda al caso; que hayan inconsistencias sobre el propósito que se hagan visibles comparando la información dada a distintos sujetos; o bien que en los casos donde se entregue la información respecto al tratamiento sea injusta, sorpresiva o contenga términos y condiciones unilaterales

sobre el propósito para el cual usarán la data, la que no se ajusta a las expectativas razonables de los sujetos de data.

En virtud de todos estos posibles escenarios, es importante que tengamos claro cuáles son las consecuencias de todos estos incumplimientos, a fin de así evitar estos mismos. Primero que todo debemos indicar que el fallar en indicar o bien indicar de forma incompleta el para qué se procesará la data no significa que el controlador pueda procesar esta misma para cualquier propósito que desee o que es libre de determinar el propósito basándose en sus expectativas subjetivas o interpretación unilateral de información inconsistente. Segundo, esto tampoco significa que aquellos documentos legales minuciosamente diseñados por los abogados del controlador pueden legitimar estos propósitos ya mencionados anteriormente. En estos casos lo que es necesario hacer es el reconstruir el propósito del procesamiento, esto mientras tenemos en consideración los hechos del caso.

Por último, si bien la publicidad de este requerimiento es uno de los indicadores centrales sobre el objetivo de un procesamiento de datos específico, este no es la referencia absoluta. En los casos que indicamos previamente en donde el propósito se especifica de forma inconsistente o bien esta especificación no corresponde a lo que ocurre realmente, tenemos que considerar todos los elementos fácticos, además del entendimiento común y de las expectativas razonables de los sujetos de data basadas en estos hechos, a fin de poder determinar el propósito actual del tratamiento[39].

2.4.3 El propósito debe ser legítimo

Los datos personales deben de recopilarse con fines legítimos. Esto va más allá a la simple referencia al artículo 6 del RGDP[40], el cual señala los criterios para hacer al tratamiento de datos legítimo, donde enumera de forma taxativa seis bases legales para el procesamiento de datos personales, que van desde el consentimiento del sujeto de datos hasta el interés legítimo[41].

A fin de que el propósito sea legítimo, el proceso debe de, en todas sus etapas y en todo momento, estar basado en al menos uno de los pisos legales que indica el artículo 6 del RDGP. Sin embargo, como mencionamos anteriormente este requerimiento del artículo 5 b) es mucho

[39] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203. Pág 19
[40] Este artículo se refiere principalmente a la licitud del tratamiento.
[41] Estos se enumeran en el artículo 4 (1) de la letra (a) a la (f)

más amplio que lo que indica el artículo 6. El artículo 5 (b) también requiere que el propósito para el que se recopilan los datos debe de ser acorde a todas las otras provisiones aplicables sobre protección de datos, además de otras leyes como por ejemplo las de contrato, protección al consumidor, trabajo, etc.

Es decir, la mejor forma de definir este requerimiento es que el propósito para el cual se recolectan los datos debe de ser "acorde a la ley", en su término más amplio. Esto incluye las leyes ya mencionadas previamente, pero también incluye principios constitucionales, precedentes judiciales, derechos fundamentales, jurisprudencia y otros, por lo que podemos indicar que este requisito se refiere principalmente a que el propósito debe de ser acorde a todo lo que se denomine ley, sea cual sea la interpretación de esta.

Por otro lado, este requerimiento también habla de otros aspectos que uno podría considerar distintos a la ley, como por ejemplo la costumbre, ética, códigos de conduta, contexto y hechos del caso, ya que todos estos factores deben de considerarse a fin de determinar si un determinado propósito es legítimo.

La legitimidad de un determinado propósito también puede cambiar con el paso del tiempo, dependiendo de los avances científicos o tecnológicos y los cambios en la sociedad y cultura de este.

A forma de resumen, este requisito se refiere a que el propósito con el que se recopila la información tiene que ser acorde a la regulación y características de la sociedad en donde ocurre, es decir, debe de cumplir con el estándar legal de dicha comunidad y no ir en contra de lo que uno puede determinar cómo las "buenas costumbres" de la misma. El propósito, por ende, debe no caer en lo ilegal o lo amoral.

2.4.4 Rol de la especificación del propósito

Como podemos ver, la especificación del propósito es un componente sumamente importante para la protección de datos.

Dentro de este se encuentran tres elementos clave para la realización del tratamiento de datos personales, siendo estos la determinación, la explicitud y la licitud. Cada uno de estos elementos abarca un área en específico, la determinación refiriéndose a que el responsable ha de tener claro los fines para los que solicitará la data, la explicitud refiriéndose a como este mismo controlador

ha de proporcionarle la información referente al fin del tratamiento y de las medidas que tomará para el mismo, tanto al interesado como a los terceros intervinientes y la licitud que va más allá de la determinación de una de las bases de tratamiento del artículo 6 (1) RGDP, sino que se relaciona con la idea de que el tratamiento ha de cumplir con ciertos estándares más allá de la protección de datos, que podríamos identificar como las buenas costumbres, moral e incluso ética.

Con respecto a lo que mencionamos anteriormente, podemos desprender que este requerimiento para el tratamiento de datos también es relevante para la aplicación de los demás principios de protección de datos, ya que sólo una vez especificado el propósito podremos empezar a aplicar otros principios, pero se desarrollará esto en el punto 3.4.1.

2.5 Segundo componente: La Compatibilidad

El artículo 5 b) del RGD indica que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

A fin de analizar este componente de nuestro principio, primero buscaré dar un marco general para lo que se denomina un "examen de compatibilidad", y después explicaré los factores esenciales que deben de considerarse en este examen.

Tras esto, se detallará la excepción a esta regla de incompatibilidad la cual consiste en la última parte de nuestro principio, específicamente a que el tratamiento posterior de datos con fines históricos, estadísticos o científicos no se considera como incompatible en virtud de lo dispuesto en el RGDP.

2.5.1 La idea de no incompatibilidad

En el RDGP el legislador no impone la idea de compatibilidad como la regla general, sino que va por una doble negativa al establecer la prohibición de la incompatibilidad. Por ende, podemos decir que la regla general es la prohibición del tratamiento posterior de datos si es que estos son incompatibles con el original. Al hacer esto, podemos hablar de que el legislador incluso da cierta flexibilidad respecto al uso posterior, ya que permite cualquier tratamiento posterior siempre que este no sea incompatible (y cumpla con los otros requerimientos de legalidad de igual forma).

Este uso posterior puede estar estrechamente relacionado con el propósito original o bien ser diferente a este, ya que el hecho de que el procesamiento posterior sea con un propósito distinto no significa necesariamente que este nuevo propósito sea incompatible, sino que esto deberá de evaluarse caso por caso. En otras situaciones esta misma flexibilidad puede incluso a ser necesitada a fin de permitir un cambio de enfoque o alcance, esto en situaciones en donde las expectativas tanto de la sociedad o de los mismos sujetos de data hayan cambiado respecto a un uso adicional de dicha data.

Finalmente, puede que existan casos en donde si bien se especificó de forma clara un propósito, el controlador o el sujeto de data pudiesen considerar que algún propósito adicional fuese necesario, aunque después se demostrara que la data recopilada sería bastante útil para otros fines. En estos casos y similares un cambio de propósito puede ser permisible, y el tratamiento posterior no debiese de considerarse como incompatible, esto solo si completa de forma satisfactoria la prueba de compatibilidad.

2.5.2 Marco general para el examen de compatibilidad

2.5.2.1 El tratamiento posterior de datos

Consideramos necesario definir a que nos referimos con el tratamiento posterior de datos. Como se mencionó previamente, el artículo 5 b) RDGP y el considerando 39 del mismo indican que el propósito por el cual se recolectan los datos debe de ser determinado al momento de su recogida o previo a este evento, pero no después del mismo.

Cuando hablamos del requerimiento de compatibilidad, el RGDP no se refiere específicamente al procesamiento para los propósitos generales ni al procesamiento con fines definidos de forma subsecuente. Lo que hace es diferenciar entre el primer procesamiento, el cual consiste en la recolección de datos, y las operaciones subsecuentes a esta. Entonces podemos decir que el primer procesamiento siempre es la recogida de la data y que la segunda podría venir a ser el almacenamiento de esta, la tercera el estudio de estos, etc.

De otra forma, podemos decir que, en cualquier procesamiento de datos personales, el primer acto de procesamiento es la recogida de estos, y que cualquier procesamiento posterior de estos, sea para el propósito especificado previamente o para cualquier otro propósito indicado posteriormente, se debe considerar como “tratamiento posterior” y que, por ende, este debe de cumplir con este requisito de compatibilidad.

2.5.2.2 ¿Una evaluación formal o sustantiva de la compatibilidad?

Si bien la naturaleza de la evaluación de la compatibilidad fue zanjada por el RGDP, creemos que es pertinente revisar en mayor detalle la denominada prueba de compatibilidad.

Cuando hablamos de un examen formal, nos referimos a que se comparará el propósito inicial, dado normalmente de manera escrita, por el controlado con cualquier otro uso posterior a fin de comprobar que estos fines posteriores hayan sido cubiertos de forma explícita o implícita.

Al hablar de un examen sustantivo, nos referimos a ir más allá de las declaraciones formales a fin de identificar el tanto el propósito nuevo como el propósito original, tomando en cuenta para esto que es lo que se entendió o lo que se debió de haber entendido, dependiendo del contexto y otros factores.

Como podemos ver, estos dos tipos de evaluación son bastante diferentes. El primer examen puede verse como el más objetivo y formal, pero trae como consecuencia mucha rigidez y dependencia del texto escrito. Al hacer esto, esto podría incluso alentar a los controladores a especificar el propósito de una forma mucho más legalista y densa, a fin de asegurar un margen para el posterior tratamiento de datos, en vez de proteger a los individuos involucrados.

Por otro lado, el segundo método es más flexible y pragmático, pero también más efectivo. Este incluso permite la adaptación respecto a futuros desarrollos dentro de la sociedad mientras que al mismo tiempo continúan entregando garantías efectivas para la protección de datos personales.

Actualmente, el consenso general del RGDP es que se debe de aplicar un examen sustantivo, ya que es más flexible y adaptable. Si bien este examen es sustantivo, el mismo dependerá de diversos factores que el mismo RGDP señala en su artículo 6 (4) que se analizarán posteriormente.

2.5.2.3 Distintos escenarios y la necesidad de la prueba de compatibilidad

Antes de entrar en detalle sobre los distintos tipos de factores que hay que considerar para realizar la prueba de compatibilidad es necesario indicar que en la práctica puede que existan diversos escenarios para esta misma prueba. En otras palabras, en algunos casos no se requerirá analizar de forma alguna la necesidad de este examen, mientras que en otros deberá de realizarse un análisis detallado.

Caso 1: la compatibilidad es obvia a primera vista

El procesamiento posterior se considera compatible, ya que la data recolectada se procesa principalmente para cumplir con el propósito específico para dicha recolección, y de una forma adecuada para alcanzar esos propósitos. Por ende, el procesamiento cumple claramente con las expectativas razonables del sujeto de data, incluso si no se especificaron todos los detalles desde el comienzo.

Caso 2: la compatibilidad no es obvia y se requiere de un análisis posterior.

En estos casos, puede que exista un tipo de conexión entre el propósito específico y la forma en que los datos son tratados subsecuentemente, pero que no sea del todo claro la relación entre el propósito original y el tratamiento posterior. También es posible que el uso posterior de la data recolectada sea con fines diferentes o no directamente relacionadas con el propósito.

En todos estos posibles casos es necesario evaluar los diversos factores clave para la compatibilidad, como la relación entre el propósito inicial y el propósito de un tratamiento posterior de datos, el contexto en el que la data se recolectó, las garantías aplicables a este nuevo tratamiento por mencionar algunos. Por regla general, mientras exista mayor distancia entre el propósito original y los propósitos para el tratamiento posterior, se requerirá de un análisis más comprensivo y detallado, y deberá de incluso considerarse un mayor número de criterios para esta evaluación de compatibilidad. Incluso puede que sea necesario que se incluyan garantías adicionales a fin de compensar por este cambio de propósito, como por ejemplo la de entregar información adicional y opciones explicitas al sujeto de datos.

Caso 3: La incompatibilidad es obvia

Si los datos fuesen procesados con un propósito adicional o posterior que cualquier persona razonable no solo consideraría como inesperada, sino que también como inapropiada o bien objetable, o bien que dicho procesamiento posterior no cumple con las expectativas de una persona razonable que se encuentre en la posición del sujeto de datos, es bastante probable que este se considera como incompatible. Sin embargo, puede que existan casos marginales que requerirán de un análisis posterior a fin de evaluar si hay o no compatibilidad.

Estos escenarios previos nos permiten indicar que hay un número limitado de factores clave que pueden ayudar a realizar un examen de compatibilidad, además de la necesidad de una

aproximación pragmática que permita el uso de supuestos prácticos basados en lo que una persona razonable consideraría como aceptable en cualquier circunstancia.

2.5.3 Factores clave a considerar a la hora de realizar un examen de compatibilidad

El Artículo 6 (4) y el considerando 50 RDGP indican los factores clave que deben de considerarse a la hora de realizar este examen de compatibilidad. A continuación, se mencionarán estos de forma breve.

2.5.3.1 Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto (art. 6 (4) (a) RGDP)

El factor que podría resultar más obvio a la hora de realizar un examen de compatibilidad entre dos propósitos vendría a ser la relación entre el propósito inicial y el propósito que justifique un posterior tratamiento de datos personales. Lo importante de este factor es que no solo debe de limitarse a lo indicado de forma textual, sino que debe de considerar también la sustancia de la relación entre ambos propósitos. De esta forma, es posible abarcar las situaciones en las que un procesamiento posterior haya sido implicado de alguna forma o asumido como siguiente paso por lógica, pero también abarca las situaciones en donde la conexión con el propósito inicial es parcial o inexistente. Lo que se debe tener claro es que mientras mayor sea la distancia entre el propósito de recolección o inicial y los propósitos de tratamiento posterior, más problemático será realizar esta prueba de compatibilidad, y este variará de caso a caso.

Un último punto a tener en cuenta a la hora de realizar dicho examen es que, al igual que con la especificación del propósito, es siempre necesario tener en cuenta el contexto fáctico y la forma en que generalmente se entiende un propósito por los stakeholders pertinentes en distintas situaciones bajo análisis[42].

2.5.3.2 El contexto en el que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento (art. 6 (4) (b) RGDP)

El segundo factor se enfoca en el contexto en el cual se recopiló la data y en las expectativas razonables de los sujetos de data involucrados respecto a su uso posterior. Es decir, lo que se busca aclarar con este factor es que expectativas tendría una persona razonable en la posición

[42] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203 pág. 24

del sujeto de data o bien que uso esperaría que le dieran a su data basándose en el contexto de la recolección de esta.

Acá podemos ver la relevancia que tiene la naturaleza de la relación entre el controlador y el sujeto de data. No sólo se refiera a algo dicho legalmente, sino que también considera aspectos como lo que sería costumbre o la práctica esperada en dicho contexto o relación. Por regla general, mientras más inesperado o sorpresivo sea el uso posterior, lo más probable es que este se considerará como incompatible. Una evaluación respecto a la naturaleza de dicha relación también debiese de incluir el balance de poder entre el sujeto de data y el controlador. En particular, se debería de indicar si los sujetos de data o un tercero a nombre de ellos se vio obligado a entregar la data por ley. De forma alternativa, esta recolección pudo haber sido basada en una relación contractual, donde se deberá de analizar la naturaleza del contrato y el balance de poder entre las dos partes. Si el procesamiento posterior es basado en el consentimiento, una evaluación sobre hasta qué punto el consentimiento se dio de forma libre y la precisión de sus términos deberá de realizarse. Normalmente, esta evaluación de compatibilidad deberá de ser más restrictiva si no se le entregó la suficiente libertad de elección al sujeto de data, como por ejemplo si los términos de consentimiento no eran del todo claros o si los usos posteriores se pueden considerar como objetables.

Para todos estos casos también debemos de considerar el estatus del controlador de data, la naturaleza del servicio entregado o bien la obligación legales o contractuales, ya que estas pueden aumentar las expectativas razonables de una mayor confidencialidad y limitaciones más restrictivas para el uso posterior. Mientras más específico y restrictivo sea el contexto de la recolección, más probable que haya limitaciones a su uso posterior.

Finalmente, a la hora de evaluar este factor también se debe de prestar atención a la transparencia del procesamiento, como también a si el procesamiento posterior se basa en alguna disposición legal. En este último caso, la seguridad legal y la predictibilidad en general pueden indicar si el uso posterior es apropiado, incluso si los sujetos de data no lo consideraron completamente.

2.5.3.3 La naturaleza de los datos personales, en concreto cuando se traten de categorías de datos especiales o datos personales relativos a condenas e infracciones penales (art. 6 (4) (c) RGDP)

El tercer factor se refiere a la naturaleza de la data y el impacto que tendría su tratamiento posterior a los sujetos de data. Esta aproximación se ha designado a fin de proteger a los

individuos del impacto proveniente del uso excesivo o inapropiado de sus datos personales. Por ende, la naturaleza de los datos procesados tiene un rol critico en estas disposiciones, por lo que es importante evaluar si el procesamiento posterior de datos involucra data sensible, como las establecidas en el RDGP en el artículo 9 u otras como datos biométricos, información genética, localización u otras que requieran protección especial, como los señalados en el artículo 10 RGDP. Mientras más sensible sea la información involucrada, más reducido es el chance de compatibilidad.

2.5.3.4 Las posibles consecuencias para los interesados del tratamiento ulterior previsto (art. 6 (4) (d) RGDP)

Este factor se refiere principalmente al impacto que el tratamiento posterior puede causarle al sujeto de data. A la hora de evaluar el impacto de un procesamiento posterior, se deben de considerar tanto las consecuencias positivas como negativas. Aquí podemos incluir a las potenciales decisiones o acciones de terceros y situaciones en los que el procesamiento posterior pueda llevar a la exclusión o discriminación de individuos. Aparte de esto, también se debe de considerar el impacto emocional que se puede causar, como irritación, miedo y angustia que puede ser el resultado de la pérdida de información personal del sujeto de data o al darse cuenta de que estos han sido comprometidos.

Desde una perspectiva más amplia, la noción de impacto relevante también considera la forma en que la data se procesa posteriormente. Podemos nombrar situaciones como si esta es procesada por un controlador distinto en otro contexto y con consecuencias desconocidas, si esta es divulgada públicamente o si se hace accesible para un mayor número de personas o bien si grandes cantidades de data personal se procesan y combinan con otras datas.

Las consecuencias relevantes también pueden variar desde ser específicas y bien definidas a otras más generales e impredecibles con una escala y rango variable. Sin embargo, se mantiene la idea de que mientras más negativo o incierto sea el impacto del procesamiento posterior, es más improbable que se considere como uso compatible.

2.5.3.5 Garantías aplicables por el controlador a fin de asegurar un tratamiento justo y evitar cualquier impacto negativo en lo sujetos de data (art. 6 (4) (e) RGDP)

Una característica de las evaluaciones con múltiples factores es que las deficiencias de algunos puntos se suelen compensar por el mejor desempeño de otras. En base a esta idea, es que el

último factor a considerar a la hora de realizar un examen de compatibilidad se enfoca en las garantías que el controlador ha aplicado a fin de asegurar un procesamiento justo y prevenir cualquier impacto indebido en los sujetos de data

Por ende, podemos indicar que cualquier medida adicional apropiada podría servir como "compensación" por un cambio de propósito o por el hecho de que el propósito no se haya especificado claramente al inicio del tratamiento como debió de hacerse. En este caso, se podría de requerir de medidas técnicas u organizacionales para asegurar la separación funcional, pero también tomar pasos extras para el beneficio del sujeto de data, como por ejemplo aumentar la transparencia, a fin de dar la posibilidad de objetar o dar consentimiento específico.

Si el propósito ha sido cambiado o no ha sido especificado claramente, un primer paso necesario para asegurar la compatibilidad es re-especificar los propósitos. También es a veces necesario darles notificación adicional a los sujetos de datos -dependiendo de las circunstancias y base legal del tratamiento posterior- a fin de darles la oportunidad de optar por participar o no en dicho tratamiento.

En otros casos, solicitar el consentimiento específico para un nuevo procesamiento podría ayudar a compensar por el cambio de propósito. Sin embargo, como se optaría por una de las nuevas bases legales establecidas en el RDGP artículo 6, debemos de recordar que se deberá de aplicar en paralelo lo mencionado en dicho artículo en conjunto con el artículo 5 b), ya que solo una nueva base legal no puede legitimar un uso posterior incompatible. Con esto nos referimos a que, si se realiza esto, deberá de volver a cumplirse de forma cumulativa todos los requisitos ya mencionados anteriormente.

Adicionalmente, la implementación de medidas técnicas u organizacionales puede resultar importante. La identificación de las medidas relevantes se facilita si el objetivo básico central es la protección y seguridad de los datos. Estos objetivos son, clásicamente, la disponibilidad, integración y confidencialidad. También se debe de considerar la transparencia, aislamiento e intervenibilidad.

Finalmente, a la hora de tratar de identificar las medidas que califican como garantías apropiadas para compensar por un cambio de propósito, normalmente el foco se relaciona con la noción de aislamiento. Al hablar de aislamiento, nos referimos a gestionar de forma adecuada los derechos

y funciones para acceder a los datos personales, que son objeto de revisión regular. Así se evitaría establecer funciones con privilegios excesivos y, de forma más general, los administradores y usuarios solo deben poder acceder a la información que necesiten para sus fines legítimos. También se toman en cuenta las medias técnicas como el endurecimiento de los supervisore y la correcta gestión de los recursos comunes. Otras medidas son la seudonimización de datos, la anonimización completa o parcial de esto o bien el agregar data, usar tecnologías que aumenten la privacidad u otras que aseguren que la data no puede usarse para tomar decisiones o acciones respecto a ciertos individuos.

2.5.3.6 Conclusión Art. 6 (4) RGDP

Como podemos ver, estos son los 5 factores clave que han de considerarse a la hora de realizar un examen de compatibilidad señalados por el RGDP. Podemos destacar que la aproximación que ha de darse de forma general no debe de ser ni específica para caer en la excesiva rigurosidad ni muy general para no caer en lo inútil. Otra noción relevante es que cada uno de estos factores puede evolucionar en un criterio más detallado o específico, ya que mientras que la tecnología, la sociedad y las prácticas comerciales, es posible que algunos de estos factores tomen mayor relevancia y que requieren una atención más específica a la hora de examinar la compatibilidad.

Por último, debemos de indicar que el examen de compatibilidad siempre tendrá criterios múltiples. Puede que no siempre todos los mencionados previamente o bien no sean del todo relevantes para todos los casos, ya que estos dependerán de más factores aplicados de forma cumulativa. Por ende, el peso de cada uno tendrá impacto distinto en la evaluación final.

2.6. El procesamiento posterior con fines históricos, estadísticos o científicos

La última parte del artículo 5 (b) respecto a la limitación de la finalidad establece que “de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

De esto ya podemos entender que este reglamento, al igual que su predecesor, permite el procesamiento posterior de data con estos fines, siempre y cuando el controlador compense este

cambio al implementar las garantías apropiadas y al particularmente asegurar que la data no se usará para tomar acciones o medidas respecto a algún individuo particular[43].

2.6.1 Objetivo de esta disposición

El principal rol de esta disposición es la de entregar mayor certidumbre legal. Dentro del considerando 50 del RGDP se indica que la operación de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. Sin embargo, aunque se indique que el tratamiento de datos personales para estos fines de archivo en interés público, investigación científica, histórica o estadístico (de ahora en adelante propósitos privilegiados), el controlador debe de compensar este de propósito aplicando todas las garantías necesarias y asegurar que la data de los sujetos de data no se utilizará para tomar medidas o acciones en contra de un individuo en particular. Estas garantías han de ser como mínimo las suficientes para excluir o minimizar cualquier riesgo a los sujetos de data[44].

El considerando 156 del RDGP nos indica de manera clara cuales son los requisitos que se han de cumplir para el tratamiento de datos personales con propósitos privilegiados. Dicho considerando menciona que:

"El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que

[43] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág 28
[44] Considerando 50 inc. 2 RGDP

los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos."

De la lectura de este considerando podemos desprender que los requisitos para el tratamiento de datos personales con propósitos privilegiados son los siguientes: Primero, que dicho tratamiento ha de estar supeditado o debe de ser dependiente del cumplimiento de la condición de que haya garantías adecuadas para los derechos y libertades del interesado. Segundo, dichas garantías han de asegurar que se apliquen medidas técnicas u organizativas para que se cumpla con el principio de minimización de los datos[45]. Tercero, dicho tratamiento ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir estos fines mediante un tratamiento que no permita identificar a los interesados o que ya no lo permita. Cuarto, que los Estados Miembros de la Unión están autorizados a establecer especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, olvido, supresión, limitación del tratamiento, portabilidad de datos y oposición los interesados, siempre esto sea bajo condiciones específicas y a reserva de garantías adecuadas.

Como podemos ver, la idea del RDGP es bastante clara: se permite el tratamiento de datos personales para estos propósitos privilegiados, pero siempre se vela por los derechos de los interesados con la aplicación de garantías establecidas, buscando principalmente la minimización de datos de estos, por el mismo Reglamento o por los Estados Miembros, siempre que esto sea bajo condiciones específica para estos últimos.

[45] Considerando 156 RGDP

2.6.2 Artículo 89 RDGP sobre Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o fines estadísticos

El artículo 5 b) del RDGP indica en su parte final que el tratamiento de datos personales con fines estadísticos, científicos, históricos y con fines de interés públicos se deben de cumplir con las garantías del artículo 89 RGDP. En muchas instancias la recolección de largas cantidades de datos personales es un elemento clave, o incluso un prerrequisito, para cumplir estos propósitos.

Por otro lado, el sobrecargar al controlador con obligaciones legales puede incluso impedir esta investigación o incluso ir en contra del mismo propósito del procesamiento. Así, esta sobrecarga se podría transformar en un detrimento para la sociedad, ya que muchas de estas se basan en archivar sistemas, investigación científico e histórico, o estudios estadísticos. Por esta razón, el artículo 89 (2) y (3) también permite la derogación específica del RGDP para dichos propósitos.

2.6.3 Garantías adecuadas aplicables para el tratamiento con fines privilegiados

El artículo 89 (1) RGDP indica que, en el procesamiento de datos con fines históricos, científicos, estadísticos, o de archivo de interés público se deberán de aplicar las garantías necesarias para asegurar los derechos y libertades de los sujetos de data. A fin de entender que garantías debemos de aplicar, es necesario definir cada uno de estos propósitos.

2.6.3.1 Fines de archivo en interés público

El considerando 158 del RDGP indica que este mismo reglamento se aplica para este tipo de tratamiento, pero teniendo presente que no debe ser de aplicación a personas fallecidas. Se indica también en este recital se define al tratamiento de datos personales con fines de archivo en interés público como cualquier operación con fin de “adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos”. Como se habla de interés público general, entendemos que los archivos personales o familiares o de compañías generalmente no se ven cubiertos por el artículo 89 RGDP, excepto si estos también cumplen con el criterio de ser guardados en el “interés público”.

2.7.3.2 Fines de investigación histórica

El considerando 160 RGDP indica que este reglamento se debe de aplicar al tratamiento de datos personales con fines de investigación histórica, pero que no aplica a personas fallecidas. Indica también que este tratamiento puede ser con fines de investigación histórica o con fines de

investigación genealógicos. En este último caso cabe destacar que como la investigación genealógica puede incluir a relativos vivos, el RGDP será aplicable para proteger los derechos y libertades de esos individuos.

2.7.3.3 Fines de investigación científica

El considerando 159 RGDP indica que el procesamiento de datos personales con fines de investigación científica debe de interpretarse de manera amplia, incluyendo, por ejemplo, desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado.

Por otro lado, el considerando 157 habla principalmente sobre el porqué el tratamiento de datos personales con fines científicos es facilitado por el mismo reglamento. Menciona el rol que esta cumple y menciona principalmente a la investigación como forma de obtener nuevos conocimientos sobre condiciones médicas extendidas y, respecto a las ciencias sociales, que la investigación permite obtener nuevos conocimientos sobre la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales. Indica además que los resultados de estas investigaciones pueden proporcionar conocimientos sólidos y de alta calidad que pueden servir como base para la concepción y ejecución de políticas basadas en el conocimiento, mejorar la calidad de vida y la mejora de los servicios sociales. A modo de resumen, el considerando 157 indica la importancia y rol de la investigación científica y por qué esta tiene esta característica de propósito privilegiado.

Finalmente, el RDGP no distingue si la investigación científica tiene roles de interés público, privados o con fines meramente comerciales. Se indica que, si los requerimientos aplicables son alcanzados, los fines privados o comerciales pueden de buscarse a través del procesamiento de datos personales con fines científicos[46]. Podemos indicar a modo de ejemplo, que las pruebas clínicas hechas por farmacéuticas o investigación científica realizada por universidades caería dentro del ámbito de aplicación del RDGP.

[46] Considerando 159 RGDP

2.7.3.4 Fines estadísticos

El considerando 162 RGDP establece que se entiende por fines estadísticos cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos.

También se agrega en este mismo considerando que resultado del tratamiento con fines estadísticos no son datos personales, sino que datos agregados, y que este resultado o los datos personales no son utilizados para respaldar medidas o decisiones relativas a personas físicas concretas. Podemos entender que se sugiere que los datos agregados no son nunca, por definición, datos personales. De esto podemos desprender que, en particular, los datos agregados son realmente anónimos y que por ende no son retribuibles a ningún sujeto de data.

Sin embargo, en la práctica, y principalmente debido al alto umbral establecido por la WP para alcanzar la anonimización total, pareciese ser bastante improbable que todos los datos agregados caigan fuera del ámbito de aplicación del RGDP. El riesgo de la re-identificación es inherente al procesamiento de una gran cantidad de data. Por estas razones, diversos escolares consideran que la mejor lectura del considerando 162 viene a ser que solo se trata de dejar en claro que la data procesada con fines estadísticos se mantiene como datos personales (sujetos al RGDP) sólo hasta esta sean anonimizadas a través de la agregación de datos.

Como podemos ver, todos estos propósitos privilegiados tienen un distinto objetivo y son detallados de forma clara y completa en los considerandos del RGDP, buscando dejar en claro que, por su relevancia y utilidad, su tratamiento no se considerará como fin incompatible con el original. Sin embargo, se enfatiza claramente que, para la realización de su tratamiento, se requerirá de las siguientes garantías dependiendo del caso.

A fin de asegurar que estas garantías serán las apropiadas, los términos “medidas o decisiones” deben de interpretarse en su sentido más amplio. Con esto nos referimos a que las garantías han de cubrir cualquier medida o decisión desconsiderada que realice el controlador o cualquier otra persona, y que además estas medidas o decisiones no sólo se refieran a procesos formales. Es decir, se busca que cualquier impacto relevante en individuos particulares sea evitado, sea positivo o negativo. Esto se explicita de mejor manera en el considerando 156 del RDGP, el que indica que el procesamiento de propósitos privilegiados debe estar supeditados a garantías adecuadas para los derechos y libertades del interesado de conformidad al mismo reglamento.

Se habla además de que dichas garantías han de asegurar que se apliquen medidas técnicas y organizativas para que se observe el principio de minimización de datos.

2.6.4 Obligación de la implementación de garantías apropiadas

Acorde a lo establecido en el artículo 89 (1) del RGDP, los controladores y procesadores deben de implementar todas las garantías necesarias para proteger los derechos y libertades de los sujetos de data cuyos datos personales hayan sido recolectados y tratados posteriormente para estos fines ya mencionados. De forma más específica, se indica que se deberán de tomar todas las medidas técnicas y organizativas a fin de garantizar, en particular, el respeto del principio de minimización de los datos personales. Con esto se refiere a que estos datos han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, principio el cual se encuentra en el artículo 5 (1)(c) del mismo reglamento.

Dentro de estas medidas el artículo 89 (1) menciona a la seudonimizacion y anonimizacion de manera específica, pero esta lista no es exhaustiva ya que pueden existir otras medidas adecuadas para reducir el riesgo asociado al tratamiento en estas áreas.

2.6.4.1 Seudonimización

El artículo 4 (5) RGDP define a esta como el tratamiento de datos personales de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Por ende, la data seudonimizada sigue considerándose como datos personales, ya que los individuos siguen pudiendo ser identificados. En virtud de esto, también se entiende que los controladores no están exentos del cumplimiento del RGDP, sino que simplemente están reduciendo los riesgos ligados al tratamiento de datos personales.

2.7.4.2 Anonimización

En virtud del considerando 26 RGDP, entendemos a la anonimización como el proceso a través del cual los datos se convierten en anónimos de forma que el sujeto de data no sea identificable, o deje de serlo. El proceso de anonimización debe de ser lo suficientemente eficaz para prevenir cualquier riesgo de re-identificación, por lo tanto sus requerimientos técnicos variaran caso a

caso dependiendo de la data disponibles y podría tornarse difícil de cumplir si es que existen técnicas de re-identificacion que se apliquen en paralelo.

El artículo 89 (1) indica que *puede* que se utilice la seudonimizacion en ciertos casos, pero respecto a la anonimizacion menciona que esta será obligatoria siempre que el fin a buscar se pueda alcanzar con su aplicación.

2.7.4.3 Otras medidas

Como se mencionó previamente, las medidas establecidas en el artículo 89 (1) no son del todo taxativas y funcionan como ejemplo de medidas técnicas u organizativas que pueden de ser utilizadas al realizar tratamiento con estos fines ya mencionados. Por ende, han de mantenerse en consideración otras medias, incluso pudiendo los mismos Estados Miembros establecer algunas propias en sus legislaciones.

2.7.5 Excepciones aplicables en virtud del artículo 89 RGDP

Finalmente, el artículo 89 en sus numerales (2), (3) y (4) indica que en ciertos casos será posible establecer excepciones a ciertos derechos contemplados en el RGDP a fin de cumplir con fines de investigación científica, histórica, fines estadísticos o de archivo de interés público.

El artículo 89 (2) se refiera a excepciones con fines de investigación científica o histórica o estadísticos que pueden establecer los Estados a los derechos de los artículos 15 (derecho al acceso de data), 16 (derecho a la rectificación), 18 (derecho a la restricción del proceso) y 21 del RGDP (derecho a la objeción). Sin embargo, dichas excepciones han de estar sujetas a las condiciones y garantías del apartado 1 del mismo artículo, agregando además otros dos requerimientos que han de cumplirse de forma simultánea. Estos requerimientos son que, primero, los derechos enumerados imposibiliten u obstaculicen gravemente el logro de los fines científicos y, segundo, que estas excepciones sean necesarias para alcanzar estos fines. Por ende, sólo se permiten estas excepciones cuando son estrictamente necesarias para cumplir con el fin del tratamiento.

El artículo 83 (3) se refiere a las excepciones realizables referentes a los datos personales con fines de archivo público, indicando que los Estados Miembros podrán prever excepciones a los derechos de los artículos 15 (derecho al acceso), 16 (derecho a la rectificación), 18 (derecho a la restricción del proceso), 19 (notificación), 20 (derecho a la portabilidad de data) y 21 (derecho

a la objeción). Al igual que el numeral anterior, estas excepciones sólo serán posibles si se cumplen con las condiciones y garantías del artículo 89 (1) y siempre que estos derechos puedan imposibilitar u obstaculizar de forma grave el logro de estos fines y dichas excepciones sean necesarias para alcanzar los mismos.

Finalmente, el artículo 89 (4) indica de forma clara que dichas excepciones al RGDP sólo son posibles para los fines mencionados en los apartados (2) y (3). Es decir, estas excepciones no se extienden a otros propósitos que pueden ser perseguidos de forma paralela con la misma data.

2.7 Consecuencias de la incompatibilidad

Hemos hablado largamente sobre la noción de compatibilidad y de su necesidad para llevar a cabo tratamiento posterior de datos personales. Sin embargo, ahora nos referiremos a que ocurre si no se cumple con la compatibilidad.

El no lograr el requerimiento de compatibilidad del artículo 5 (1) (b) del RGDP tiene serias consecuencias: el procesamiento de datos personales que sea incompatible con los fines especificados en la recolección de estos se considera como ilegal y, por ende, no está permitido.

En otras palabras, el controlador de datos no puede simplemente considerar el tratamiento posterior de datos como un tratamiento nuevo y desconectado del primero y así evadir esta prohibición al usar alguna de las otras bases legales del artículo 6 RGDP para legitimar dicho proceso. Como mencionamos al hablar de legitimidad, ambos requerimientos son cumulativos, se debe cumplir con el artículo 5 y 6 de forma simultánea.

Al legalizar un tratamiento de datos que se consideraría incompatible a primera vista con tan solo cambiar los términos del contrato con el sujeto de data, o al identificar un interés legítimo adicional para el controlador iría en contra del espíritu del principio de finalidad limitada y se perdería su sustancia.

2.7.1 Incompatibilidad bajo el RGDP

En las primeras propuestas del RGDP se indicaba en el artículo 6 (4) de esta una proposición que daba una excepción bastante amplia al requerimiento de compatibilidad, la que si se hubiese aplicado restringiría de forma grave la aplicabilidad de este requerimiento[47]. Esta propuesta

[47] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág. 36

inicial indicaba que “cuando el fin del tratamiento posterior no sea compatible con el fin para el cual la data fue recolectada, el tratamiento debe de tener una base legal en al menos una de las bases referidas en los puntos (a) a (e) del párrafo 2. Esto se aplicará en particular a cualquier cambio de términos y condiciones generales del contrato”.

Si se hubiese mantenido esta disposición en el RGDP, se habría dado la opción de que siempre hubiese sido posible remediar la falta de compatibilidad con el simple hecho de identificar una nueva base legal para el tratamiento. En este caso, la única base legal que no habría sido suficiente por sí misma para compensar por la incompatibilidad habría sido el “interés legítimo” del controlador bajo el punto (f).

La WP creada artículo 29 de la Directiva 95 recomendó en su opinión 203/2013 sobre el principio de finalidad que se removiera este párrafo del propuesto RGDP. Se basó principalmente en que la prohibición de incompatibilidad y el requerimiento de una base legal bajo el artículo 7 de la Directiva son requerimientos cumulativos. Por ende, para un cambio de fin, cualquiera de las bases legales debe de aplicarse de todas formas. Por ende, la directiva que regía previo al RGDP no permitía en principio el cambio de propósito sin el resultado positivo de un examen de compatibilidad, y que dicho nivel de protección debería de mantenerse en el RGDP igualmente.

Actualmente, el RGDP en su artículo 6 respecto a la licitud del tratamiento, señala en su numeral 4 que en los casos en que para el tratamiento con un fin distinto a aquel para el que se recogieron los datos personales y no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento deberá tener en cuenta:

a) La relación entre los fines para los cuales se recogieron los datos personales y los fines del tratamiento ulterior previsto
b) Contexto en el que se hayan recogidos los datos personales, en particular la relación entre los interesados y el responsable del tratamiento
c) La naturaleza de los datos personales
d) Las posibles consecuencias para los interesados del tratamiento ulterior previsto
e) La existencia de garantías adecuadas

Es decir, en el actual artículo 6 (4) RGDP se señalan los factores para realizar un examen de compatibilidad y determinar si el tratamiento con otros fines es compatible con el fin inicial, manteniendo la necesidad de realizar este examen para justificar un cambio de propósito.

2.7.2 Excepciones al requerimiento de compatibilidad

Sin embargo, el mismo RGDP señala que existen tres casos en los que el requerimiento de compatibilidad no es necesario para el tratamiento posterior. Estos casos son la autorización del interesado o sujeto de data con su consentimiento artículo 6 (4) RGDP, si es basado en el Derecho de la Unión o de los Estados Miembros cuando constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos referidos en el artículo 23 RGDP[48] y cuando su tratamiento ulterior sea con fines de archivo en interés público, fines científicos e históricos o fines estadísticos (artículo 5 (1) (b) RGDP).

2.8 Conclusiones

Hemos vistos como el principio de finalidad limitada surge y como fue evolucionando hasta su acepción actual. En 1950 se menciona dentro del artículo 8 CEDH y como cumplía con un rol de legitimidad para que se pudiese intervenir en la privacidad de una persona, es decir, se necesitaba una justificación legal para dicha intervención. En la década de los 80' aparece este principio en el Convenio 108 y las directrices de la OCDE, en donde se agrega su segundo componente que corresponde a la idea de incompatibilidad, y que no se permitirá tratamiento posterior de los datos personales si estos son incompatibles, salvo que la ley disponga claramente de excepciones a esto.

En 1995 en la Directiva 95/45/EU se establece ya de forma clara que este principio consta de dos partes: la especificación del propósito, es decir, que el fin para el cual se recolectan los datos debe de ser determinado, específico y legítimo, siendo este último requerimiento añadido en esta directiva, y que no serán tratados de maneta posterior si el nuevo fin es incompatible. Se añade, además, que se no se consideraran como fines incompatibles los relacionaos con la investigación histórica o científica, con fines estadísticos y siempre que se den las garantías correspondientes. Esta Directiva se mantuvo en vigencia hasta el 2018, año en donde comenzó a regir el RGDP sobre toda la Unión Europea.

[48] Artículo sobre limitaciones.

En el año 2000 se proclama la Carta de los Derechos Fundamentales de la UE, en donde por primera vez se separa la protección de datos personales (art. 8) respecto a la protección de la privacidad (art. 7). También queda establecido el principio de finalidad de manera textual, ya que en el artículo 8 (2) se menciona que los datos serán tratados de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legitimo previsto por la ley. La noción de "fines concretos", es una clara referencia a la necesidad de especificar el propósito, es decir, cumplir con la primera parte del principio de finalidad.

Finalmente, en el año 2018 comienza a regir el RGDP, reglamento en el cual se establece en su artículo 5 (1) (b) el principio de finalidad limitada, indicando que los datos personales han de ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. Se añade igualmente que el tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerarán como incompatibles con los fines iniciales, esto en virtud de lo indicado en el artículo 89 (1) del mismo reglamento.

Como podemos ver, desde los inicios de la protección de datos se ha tenido claro que, se debe de proteger a los sujetos de data a toda costa. Por ende, surgen estos distintos principios, entre los cuales aparece el principio de finalidad limitada, cuyo rol era principalmente que los datos recopilados han de ser determinados y especificados, a fin de que no se recopilen datos no relevantes para el tratamiento y que el sujeto de data sepa el fin para el que se recopilan sus datos. Posterior a esto, se añade el requisito de compatibilidad para el tratamiento posterior de datos y el requisito de legitimidad para la recopilación de datos. Finalmente, a través de toda esta evolución histórica del principio de finalidad se logra establecer su componente, la especificación del propósito y la compatibilidad para el tratamiento posterior de estos datos.

2.8.1 La especificación del propósito

El primer componente de este principio consiste en la especificación del propósito o fin. Dentro de esta noción hay tres requerimientos que hay que cumplir para la recopilación de los datos personales, siendo estos requerimientos que los fines deben de ser determinados, explícitos y legítimos.

Fines determinados

Con esto nos enfocamos principalmente en el controlador, quien trata los datos, quien debe de determinar de forma clara los fines para los que recopilará la data, a fin de no recolectar data no necesaria o irrelevante para dicho fin buscado, además de así establecer las garantías correspondientes. Por ende, podemos decir que este requerimiento limita el marco de trabajo del controlador, al obligarle a detallar los fines para los que los requiere la data.

Respecto al momento en el cual debe de detallarse los fines para la recopilación de datos, siendo este momento, a más tardar al momento en el que se recopilan los datos, pero no posterior a este hecho (recital 56).

Respecto al detalle y precisión de esta determinación, debe de ser lo suficientemente clara para el fin para el cual se recopilo la data. Por ende, los fines amplios o vago como "mejorar servicios, o fines de mercado" normalmente no son lo suficientemente detallados y por ende no cumplen con este fin. Además, el lenguaje que debe de usarse debe de ser el adecuado.

En el caso de existir diversos propósitos, deben de detallarse cada uno de manera clara a fin de cumplir con este requerimiento.

Fines explícitos

Con este requerimiento nos referimos a que debe de explicarse de forma clara no solo para el controlador, sino que para los terceros intervinientes en el proceso, como las autoridades relevantes, terceros y los mismos sujetos de data. Al indicar de forma clara o explícita los fines para los cuales se recopilará la data, los sujetos de data generan lo que se denomina como expectativas razonables, es decir, se harán una idea general sobre el para que se usaran sus datos recopilados.

También el indicar de forma explícita los fines para los que se recopilan los datos ayuda a la transparencia y predictibilidad, ya que se deja en claro el para que se usará la data, tanto para el controlador como para el sujeto de data, además de que al explicitar los fines se reduce el riesgo de que dicha data se use con otros fines. El RGDP indica de que formas ha de notificarse al sujeto de data sobre los fines para los que se usarán sus datos.

Fines legítimos

La idea de legitimidad se refiere no solo a las bases legales establecidas en el artículo 6 (1) del mismo reglamento, sino que también se deben de cumplir con todas las demás leyes existentes. Es decir, es un requisito cumulativo, tanto de las bases del artículo 6 y de todas las demás leyes vigentes, por lo que podemos decir que la legitimidad busca el fin para el que se recopilan los datos no sea en contra del estándar legal de la comunidad o en contra de las "buenas costumbres".

2.8.2 La incompatibilidad

Se habla de incompatibilidad ya que el RGDP habla que el tratamiento posterior de datos no se podrá realizar si el fin de este es incompatible con el original. Es decir, la regla general es que no podrá realizarse tratamiento posterior si es que el fin de este es incompatible con el original.

A fin de ver si existe compatibilidad para realizar un tratamiento posterior de datos, se debe de realizar un realizar un examen de compatibilidad, el cual basándose en distintos factores nos ayudará a resolver caso a caso si existe compatibilidad entre un propósito y otro. Estos factores se encuentran en el artículo 6 (4) RGDP, y entre estos destacan: relación entre ambos fines, contexto en el que se recogieron los datos, naturaleza de los datos personales, posibles consecuencias para los interesados del tratamiento ulterior y la existencia de garantías adecuadas.

La aplicación de estos factores se hará caso a caso y estos tendrán menor o mayor peso dependiendo del caso concreto. En caso de que este examen de un resultado positivo, entenderemos que el tratamiento posterior de datos si estará permitido, y si el resultado es negativo, entenderemos que el tratamiento ulterior no es permitido.

Tratamiento posterior con Fines de archivo público, fines científicos o históricos y fines estadísticos

El RGDP en diversos considerandos y en el artículo 5 (1) (b) y artículo 89 RGDP indica que los tratamientos posteriores con estos fines si están permitidos, siempre y cuando se cumpla con diversas condiciones.

Estos fines están permitidos porque en esencia estos tienen un impacto positivo y relevante en la sociedad, como por ejemplo la investigación científica en materias de salud o ciencias

sociales, fines estadísticos del país y otros. Como vemos, el RGDP busca facilitar estos fines por el rol que cumple, pero de todas formas otorga garantías y medidas técnicas y organizativas, a fin de que los datos de los interesados se vean protegidos en todo momento. El artículo 89 (1) indica por ejemplo medidas como la seudonimización y la anonimización, pero existen otras como encriptación, agregación de data, etc.

Los numerales 2 y 3 del artículo 89 indican las excepciones que pueden realizarse a ciertos derechos de los sujetos de data, pero estos sólo se aplicaran cuando dichos derechos imposibiliten u obstaculicen la obtención de dichos fines privilegiados y que esta excepción sea necesaria para alcanzar dichos fines. Finalmente, el numeral 4 indica claramente que estas excepciones a estos derechos solo se aplicarán para los fines del artículo 89, y no a otros fines que se busquen de forma paralela.

Capítulo 3: El rol del principio de finalidad limitada en la protección de datos personales

En el capítulo anterior analizamos largamente los elementos del principio de finalidad limitada que se señalan en el RGDP. Indicamos que este se puede desprender en dos componentes que son la especificación del propósito (purpose specification) y en la no incompatibilidad. Respectivamente, hablamos de que la especificación del propósito indica que los datos han de ser determinados, explícitos y legítimos; y que para ver si existe la compatibilidad, es decir, la posibilidad de seguir tratando de forma ulterior datos personales, ha de realizarse un examen de compatibilidad, el cual está explicitado en el artículo 6 (4) RGDP y que tiene una naturaleza sustantiva.

Sin embargo, ahora con todo este análisis de los componentes hecho hablaremos de algo más amplio, pero manteniéndonos dentro de la protección de datos personales. En este capítulo hablaremos nuevamente de los componentes del principio de la finalidad, pero ahora hablaremos del rol que estos cumplen dentro de la misma ley de protección de datos personales, esto para que podamos entender el peso que tiene este propósito dentro de la misma regulación, y poder compararlo con los otros principios de la protección de datos, a fin de ver si todos tienen la misma relevancia o si algunos tienen más peso que otros.

3.2 La función del principio de finalidad

Respecto del principio de finalidad limitada podemos indicar que este tiene una doble función relacionada directamente con el controlador de datos o responsable. Esta función consiste en (1) que se especifique de forma clara el o los propósitos para los que usará la data personal que busca recolectar y (2) que el mismo se ate a estas condiciones que el mismo predeterminó, limitando así el uso de datos personales al propósito específico. Aquí directamente vemos la aparición de los dos elementos clave del principio de finalidad, que son la especificación del propósito y la compatibilidad.

En base a esto podemos entonces decir que el principio de finalidad prohíbe la recogida de datos personales con fines no especificados o fines muy ambiguos o amplios. Es decir, este principio se opone a que el responsable del tratamiento recolecte datos personales con un propósito general. Al hacer esto, el principio de finalidad contribuye a genera un cierto balance entre los intereses del responsable o de la sociedad con los intereses, derechos y libertades de las personas.

Como podemos ver, el rol del principio de finalidad es establecer un balance tanto entre el responsable del tratamiento, sea un ente privado o público, con el sujeto de data, a fin de que el primero no pase a llevar los derechos del segundo.

3.3 El otro rol del principio de finalidad Limitada

Ya mencionamos la función del principio de finalidad, pero esto no abarca todo lo que busca este mismo. Este principio también se encuentra intrínsecamente unido con otras nociones sustantivas que le otorgan un mayor peso del que ya tiene. Estos otros conceptos son la transparencia, autodeterminación, certidumbre legal y predictibilidad de esta. Todas estas ideas buscan proteger el sujeto de data al establecer límites a los responsables del tratamiento al establecer el cómo deben de usar los datos de estos y ayudan además a asegurar lealtad del proceso.

3.3.1 Transparencia

Existe una fuerte conexión entre la transparencia y la especificación del propósito. Cuando el propósito especificado es claro y es compartido con stakeholders como la autoridad de protección de datos y los mismos sujetos de data, las garantías para esto pueden aplicarse de manera efectiva y completa. La transparencia también asegura la predictibilidad y permite el control de usuarios, conceptos nuevamente relacionados.

3.3.2 Predictibilidad

Si el propósito es lo suficientemente claro y específico, los sujetos de data sabrán que esperar, haciendo así que el procesamiento de datos sea predecible. Esto trae consigo también cierta certidumbre legal para los sujetos de data y para aquellos que procesan la data en nombre del controlador.

La predictibilidad es también una variante relevante para la evaluación de la compatibilidad y la posibilidad de un procesamiento posterior de datos. Por lo general, el procesamiento posterior no puede considerarse como predecible si es que no existe una relación suficiente con el propósito general y no entra en lo que se conoce como “expectativas razonables” de los sujetos de data al tiempo de su recopilación, esta misma basada en el contexto de la recolección.

3.3.4 Control de usuario(s)

El control de usuario es solamente posible cuando el propósito del procesamiento de datos es lo suficientemente claro y predecible. Si los sujetos de data entienden el propósito de dicho procesamiento, podrán ejercer sus derechos de la manera más eficiente, como, por ejemplo, objetar el procesamiento o solicitar la corrección o eliminación de su data[49].

Sin embargo, esto no significa que el propósito presentado sea siempre identificable como el actual o efectivo, ya que podrían ocurrir discrepancias entre que se pretende y lo que realmente busca el controlador de data. Por último, el cumplimiento de otros requisitos de protección de datos como por ejemplo la necesidad y relevancia de estos, siempre deberá de evaluarse con el propósito actual.

Como podemos ver, estas ideas buscan hablan de transparencia, predictibilidad y la autodeterminación del usuario. Todas estas están ligadas al principio de finalidad, ya que se relacionan fuertemente a la recogida de datos y buscan que el tratamiento que se vaya a realizar de sus datos sea de cierta forma lo más claro posibles, a fin de que el sujeto de data tenga claridad del cómo se usarán sus datos y pueda generarse las expectativas razonables respecto a este tratamiento. Estas ideas se ligan directamente con el artículo 5 (1) (a) del RGDP, que habla que los datos serán tratados de manera leal, lícita y transparente en relación con el interesado, que es otro de los principios de protección de datos personales.

3.3.5 El principio de finalidad y el imperio de la ley

Hildebrant[50] indica que el principio de finalidad está estrechamente relacionado con la idea del imperio de la ley y la del principio de legalidad. Como sabemos, el imperio de la ley se refiere a aquella situación en la que un gobernante solo obtiene poder cuando este acepta un sistema de chequeos y balances que permiten el ejercicio del poder de una forma no arbitraria. Es decir, el ejercicio de la autoridad debe de ser razonable, debe de usarse para el fin para el cual se otorgó dicho poder y no debe de abusarse del mismo al exceder los límites de dicho poder.

Como podemos ver, el principio de finalidad tiene características similares a las que describimos recién. Este principio busca que el responsable solo pueda procesar datas en un sistema de chequeos y balances y de forma no arbitraria al formular de manera previa un propósito o fin

[49] Article 29 Working Party Opinion 03/2013 on Purpose limitation, 2013, WP 203, pág. 14
[50] (Hildebrandt, 2014)

para la recolección de datos y abstenerse de tratar ulteriormente esta data con fines incompatibles a los previamente establecidos. Los requisitos de determinación, explicitud y legitimidad ayudan a que el tratamiento de datos sea digno, igual, racional y acorde a la ley, y ayuda además a hace efectiva la responsabilidad proactiva del responsable del tratamiento.

3.4 El principio de finalidad en la protección de datos personales

Finalmente, para que veamos que rol tiene el principio de finalidad en la protección de datos personales analizaremos el cómo se posiciona este principio dentro del marco legal del RGDP, y veremos como este principio se posiciona respecto a los otros principios del artículo 5 RGDP, a fin de que quede claro la importancia de este mismo.

De manera general, el procesamiento de datos personales tiene que cumplir con cuatro requisitos cumulativos para considerarse como legítimo bajo la regulación de la UE. Primero, el procesamiento ha de cumplir con todos los principios de protección de datos, debe de basarse en al menos una de las condiciones legales establecidas en el artículo 6 RGDP, que el controlador cumpla con las obligaciones impuestas al mismo y finalmente que los interesados sean capaces de ejercer sus derechos como sujetos de datos de forma efectiva. Respecto al principio de finalidad, es importante mencionar que una nueva base legal de procesamiento no puede permitir al responsable del tratamiento incumplir con sus obligaciones de procesar la data acorde a las condiciones predeterminadas que se fijaron al momento de la recogida de datos. Por ende, en el caso de que se establezca una nueva base legal de tratamiento, el responsable del tratamiento deberá de seguir cumpliendo con sus obligaciones previas respecto al tratamiento, e incluso puede que sea posible que se agreguen aún más obligaciones a cumplir en virtud de la nueva base de procesamiento.

Como podemos ver, estos 4 requisitos son necesarios y cumulativos para que un procesamiento se considere legítimo. Sin embargo, para efectos de este trabajó solo me centraré en el primer requisito, que indica que se han de cumplir todos los principios de protección de datos, que a mi parecer es el requisito que mejor nos permite entender el rol del principio de finalidad limitada en la protección de datos personales.

3.4.1 Los principios de protección de datos y su relación con el principio de finalidad

En el capítulo 1 mencioné de manera breve los seis principios de protección de datos recogidos en el actual RGDP de la UE. En este capítulo los mencionaré nuevamente, pero esta vez

entablaré una relación entre dichos principios y el principio de finalidad limitada, específicamente con su primer componente, el que se señaló en el capítulo 2 de este trabajo y se refiere a la especificación del propósito.

Este enfoque en la especificación del propósito es esencial para que entendamos el rol del principio de finalidad respecto a los demás principios de tratamiento de datos, ya que estos últimos depende del primero para ser aplicados y para poder defender tanto los derechos de los interesados como para tener un valor instructivo respecto a las obligaciones del responsable del tratamiento.

3.4.1.1 Licitud, lealtad y transparencia

El artículo 5 (1) (a) indica que los datos personales serán tratados de manera lícita, leal y transparente. Los dos primeros conceptos han sido de uno de los principios originales de toda la protección de datos personales, pero la idea de transparencia se agregó recién en el RGDP.

La idea de licitud hace referencia a lo ya mencionado respecto a la idea de legitimidad del principio de finalidad, que se refiere tanto a la necesidad de una base legitima para la realización del tratamiento de datos, pero que también dicho tratamiento sea acorde a la ley y no vaya en contra de lo que podemos denominar las buenas costumbres.

Cuando se habla de lealtad nos referimos a la idea omnipresente de la demanda de proporcionalidad dentro del tratamiento, es decir, que este no se exceda del propósito especificado previamente y no vaya en contra de los derechos fundamentales de los interesados afectados. La proporcionalidad variará de caso en caso. También cuando se habla de que el proceso sea leal nos referimos a que los interesados se les debe de notificar los posibles riesgos, reglas, garantías y derechos en relación con el procesamiento de sus datos y como ejercer estos mismos derechos. Es decir, el responsable ha de indicarle a los interesados toda la información respecto al tratamiento que realizará de sus datos.

Por último, tenemos al principio de transparencia. Ya mencionamos esta previamente, pero al hablar de este principio nos referimos principalmente a que se debe de proveer la información respecto al procesamiento existente, la identidad del responsable y el propósito del procesamiento y cualquier otra información que asegure un proceso leal y transparente. Como

vemos, la transparencia está fuertemente ligada a la lealtad del proceso, ya que es a través de la primera que podemos asegurar que un procesamiento será leal.

¿Pero cómo se relaciona esto a la idea de especificación del propósito? Esto queda claro al entender que para poder aplicar todos estos principios es necesario que el controlador ya tenga un propósito determinado a fin de recolectar los datos. Como sabemos, el principio de finalidad es opuesto a la recogida de datos con fines generales, ya que requiere que haya un fin determinado, explicito y legitimo para realizar la recolección de datos. Esto es lo importante, ya que previo a la recolección de datos ya se deberá de tener señalado todo esto, es decir, ya deberá de esta especificado el propósito, y una vez este se haya indicado, recién podremos empezar a considerar otros principios o preguntas, como por ejemplo si este es lícito, si es lo suficientemente transparente o si este es leal con el interesado. Como podemos ver, la aplicación de estos principios es condicional a la especificación del propósito[51].

3.4.4.2 La no incompatibilidad

Hemos hablado largamente de este principio, pero hay un elemento que debemos de señalar en este capítulo. Indicamos que el principio de finalidad limitada tiene dos componentes, la especificación del propósito y la compatibilidad. Ambas van juntas, pero el requisito de no incompatibilidad es totalmente dependiente de la especificación del propósito, ya que solo podremos realizar este examen de compatibilidad cuando tengamos un propósito inicial y queramos seguir tratando ulteriormente la data, y este propósito inicial será el indicado en la especificación del propósito.

3.4.4.3 minimización de la data y limitación del plazo de conservación

El artículo 5 (1) (c) indica que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Por otro lado, el artículo 5(1) (e) se refiere a la limitación del plazo de conservación de los datos, cuyo objetivo central es que la data debe mantenerse de forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de datos personales.

Estos principios se tienen a leerse en conjunción con el principio de finalidad limitada, ya que ambos tienen una directa dependencia con la especificación del propósito, ya que una vez

[51] Koning M. E. 2020. The purpose and limitations of purpose limitation pág. 132

especificado el mismo, podremos saber que datos serán los pertinentes a recoger y sabremos por cuanto tiempo estos se deberán de conservar para su análisis. La especificación del propósito permite que se realice un examen de proporcionalidad, en el cual debe de responder la pregunta si debe de procesarse x data. Al responder de forma positiva a dicha pregunta no solo se procesará dicha data, sino que se establecerá cual es la data relevante para dicho tratamiento y el periodo por el cual se conservará la misma. Por ende, la especificación del propósito es condicional para la implementación de la minimización de data y la limitación del plazo de conservación en el tratamiento de datos personales

3.4.4.4 exactitud

El articulo 5 (1) (d) indica que los datos personales serán exactos y, si fuera necesario, actualizados. Por otro lado, este principio también establece que el responsable ha de tomar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. Finalmente, también podemos vincular este principio a algunos derechos de la protección de datos, como por ejemplo la rectificación o el derecho al olvido.

La relación entre el principio de exactitud y el principio de finalidad limitada es clara, el mismo artículo indica que los fines para los que se traten los datos se tomarán en cuenta a la hora de suprimir o rectificar cualquier caso de imprecisión.

3.4.4.5 integridad y confidencialidad

El artículo 5 (1) (f) indica que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada a los datos personales, incluida la protección en contra el tratamiento no autorizado o ilícito y contra su perdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Este principio se refiere a principalmente a la seguridad del procesamiento y recae en el responsable del tratamiento, quien considerará los costos, medidas actuales, alcance, contexto y otros factores a fin de garantizar un nivel de seguridad adecuado, tal como se indica en el artículo 32 (1) del RGDP.

Por ende, la especificación del propósito es un factor determinante a la hora de realizar un análisis de riesgo del tratamiento, y será central a la hora de tomar una decisión respecto a las medidas de seguridad apropiadas para dicho tratamiento.

Como podemos ver, todos estos principios dependen de la aplicación del principio de finalidad limitada. La especificación del propósito que es la primera parte de este principio es un requerimiento condicional para la posterior aplicación de todos los demás principios, que como sabemos han de cumplirse todos de manera conjunta para cumplir con el primer pilar de legitimidad del tratamiento. Pero creo que con esto he dejado claro mi idea central, ha quedado claro que dentro de todos los principios de tratamiento de datos personales el principio de finalidad tiene un rol central, esencial y condicional para la aplicación de todos los demás principios de protección de datos.

3.5 Conclusiones

En este capítulo nos hemos enfocado principalmente en el rol del principio de finalidad dentro de la protección de datos personales y del rol que tiene dentro de uno de los pilares de legitimidad del tratamiento, siendo este pilar la necesidad de cumplir con todos los principios de protección de datos personales.

Indicamos que el principio de finalidad tiene una doble función, la de primero obligar al responsable a definir un propósito previo a al procesamiento y a anclarse al mismo a la hora de tratar los datos. De esta forma, protege los derechos fundamentales de los interesados al establecer un propósito previo a la recolección de datos, pero también permite la libre circulación de los datos personales al permitir el tratamiento ulterior de estos con fines compatibles.

Por otro lado, este principio prohíbe además la recogida de datos sin fines específicos, ya que la especificación del propósito debe de realizarse antes de la recogida. La especificación del propósito además nos permite responder la pregunta de ¿por qué se está procesando la data?, pregunta que debe de establecerse de forma clara para realizar preguntas posteriores de proporcionalidad de este. Debe de además tener una base legal sustantiva para su realización y debe de ser lo suficientemente clara para que una persona no experta pueda entender que es el procesamiento de data y que data será procesada y cual no. Por ende, la especificación del propósito obliga al responsable a ponderar sobre el procesamiento de datos.

Por otro lado, tenemos el requerimiento de no incompatibilidad, el cual obliga a que el tratamiento de datos se limite a los fines para los cual la data fue recogida. Este requerimiento

también limita el uso de data en base a un examen de compatibilidad entre el nuevo propósito y el propósito inicial, a fin de ver si es posible el tratamiento ulterior de datos.

También podemos indicar que el principio de finalidad se relaciona con la idea del Imperio de la Ley, ya que este principio busca generar un sistema de chequeos y balances para que el responsable del tratamiento no caiga en un abuso de poder al procesar los datos personales.

Finalmente, podemos encasillar al principio de finalidad dentro del requisito de cumplimiento de todos los principios de protección de datos para la legitimidad de un tratamiento de datos, pero dentro de este mismo requisito podemos indicar que el principio de finalidad tiene un rol clave y central, ya que sólo se podrán aplicar todos los demás principios si se realiza previamente la especificación del propósito, es decir, la aplicación de los demás principios es condicional a la determinación de un fin previo, el cual debe de ser determinado, explícito y legitimo.

Capítulo 4: El principio de finalidad limitada en Chile

Ya hemos hablado largamente del principio de finalidad, su historia, características, elementos y rol que cumple. Con todo esto ya claro, es relevante ver el cómo podemos aplicar este principio a Chile, ya que como se detallará a continuación Chile se encuentra bastante atrasado en materia de protección de datos personales. En este último capítulo, se hablará sobre el cómo se regulan los datos personales en Latinoamérica, como estos están regulados en Chile y criticar su situación actual y finalmente se efectuará una recomendación de sobre cómo podríamos construir este principio en específico en el nuevo proyecto de ley de datos personales, a fin de que este se integre de la forma más completa y entendible posible a nuestra legislación.

4.1 protección de datos personales en Latinoamérica

El foco central de este análisis a la protección de datos personales y al principio de finalidad limitada se ha hecho en su totalidad desde la perspectiva europea. Me he enfocado en como esta se ha desarrollado y evolucionado en el viejo continente y sobre cómo se entiende el principio actualmente en dicho lugar. Sin embargo, es necesario que hablemos de igual forma de como se ve este tema de la protección de datos personales en nuestro continente, para que nos hagamos una idea de cómo este se aplica y desarrolla aquí.

De forma sencilla, podemos decir que Latinoamérica está bastante atrasada en lo que respecta a protección de datos personales. Si bien la gran parte de los países de este poseen su regulación propia para esta materia, está a diferencia de lo que ocurre en Europa no está unificada de forma alguna bajo algún tipo de reglamento como el RGDP, por lo que cada país ha tomado distintas rutas para abarcar esta materia. Sin embargo, con la entrada en vigor del RGDP en la UE en el año 2018, muchos países de Latinoamérica han optado por reformar sus legislaciones locales en esta materia, a fin de elevar sus estándares de protección, esto debido a la aplicación extraterritorial del RGDP, ya que puede obligar tanto a empresas ubicadas en la UE que traten datos personales, como a empresas ubicadas en otros países que traten informaciones personales de ciudadanos europeos[52].

Dentro de Latinoamérica podemos encontrar al menos 2 grandes categorías en lo que respecta a protección de datos: 1) países que poseen leyes de protección de datos personales y 2) países que no poseen leyes de protección de datos personales. Chile se encuentra en la primera

[52] Art. 3 RGDP

categoría, pero dentro de esta este es un caso excepcional por razones que hablaremos más adelante.

Dentro de la primera categoría podemos hablar de países como México, Brasil, Perú, Costa Rica y Uruguay, entre otros. Cuando hablamos de países que tienen regulación en materia de datos personales, nos referimos a que estos países tienen una ley para esta materia emitida y en vigencia. Podemos mencionar que gran cantidad de los países en esta categoría proclamaron leyes en esta materia lo hicieron fuertemente influenciados por la Carta de Derechos Fundamentales de la Unión Europea, la Directiva 95/46/EU y por el RGDP[53]. También, gran parte de estos países elevó a norma constitucional la protección de datos personales.

Uno de los casos más destacables en esta categoría es el de Brasil, país que, a pesar de nunca haber tenido alguna regulación previa en la materia, aprobó en el año 2018 y entró en vigor el año 2020 la Lei Geral de Proteção de Dados fuertemente influenciada por la entrada en vigor del RGDP de la UE.

Por otro lado, también podemos destacar el caso de Argentina, país cuya ley de protección de datos Personales data al año 2000, pero que se basó fuertemente en las legislaciones europeas, especialmente la Directiva 95/46/EU, por lo que la Comisión Europea ha declarado que esta legislación garantiza un nivel adecuado de protección de datos, al igual que el caso de Uruguay.

Los otros países dentro de esta categoría como Costa Rica, México, Uruguay, Colombia, Perú tienen leyes de protección de datos que datan del año 2008 en adelante, por lo que podemos entender que este tema se ha desarrollado de forma tardía en gran parte de estos países.

Respecto al principio de finalidad, es interesante indicar que en todas las leyes respecto a esta materia se indica en alguno de sus títulos los principios rectores o generales sobre esta materia, y que en cada uno de ellos se encuentra de forma explícita.

La segunda categoría corresponde a países que aún no tienen leyes de protección de datos, como es el caso de Bolivia, Venezuela y Ecuador. Si bien ninguno de estos países consta con alguna ley es importante indicar que en estos tres países se habla a nivel constitucional de protección de datos. Debido a esto, de diversas organizaciones internas han manifestado su preocupación

[53] Respecto a la entrada en vigor de este último, diversos países como Chile, Argentina y México han tomado medidas para aumentar su protección de la privacidad y la seguridad de los datos personales de sus ciudadanos.

por no tener una legislación o marco regulatorio conciso para esta materia, por lo que apremian la creación de uno.

Como podemos ver con esta breve indicación sobre la protección de datos en Latinoamérica podemos entender que nuestro continente recién comenzó a emitir regulación sobre la misma en el siglo XXI, décadas más tarde que en Europa, la cual podemos indicar que comenzó en 1980 e incluso antes a hablar sobre esta materia. Podemos señalar además que varios países de nuestro continente optaron por guiarse por los instrumentos creados en Europa, pero que de cierta forma trataron de adaptar a sus realidades sociales, culturales y económicas. Por último, podemos destacar que gran parte de los países latinoamericanos habla de forma directa sobre la protección de datos en sus constituciones, excepto por Chile, el cual se remite a la ley 19.628, que data al año 1999 y sigue vigente a la fecha.

4.2 La Protección de Datos Personales en Chile actualmente

Actualmente, en Chile existe sólo una legislación respecto a la protección de datos personales, la cual es la Ley 19.628 sobre Protección de datos personales, pero para analizar esta es necesario primero hablar sobre el artículo 19 n°4 de la CPR, ya que es en esta en que se basó la creación de dicha ley.

Cabe destacar, que, para realizar un análisis de nuestra legislación en esta materia, me basaré fuertemente en lo indicado en los capítulos 1, 2 y 3 de esta memoria, a fin de comparar nuestra legislación con la europea respecto al principio de finalidad y su rol dentro de la protección de datos y ver cómo podemos traer esta última a nuestro país, a fin de mejorar el estándar de protección de datos que tenemos actualmente respecto a este principio específico.

4.2.1 Artículo 19 n°4 de la Constitución Política de la República

La CPR entró en vigor el año 1980 y trajo consigo grandes cambios para al país. Sin embargo, desde su entrada en vigor esta ha tenido cambios mínimos, por lo que es posible decir que esta se encuentra desactualizada respecto a ciertas cosas, como es el caso de la materia de protección de datos personales.

El artículo 19 N°4 de la CPR indicaba inicialmente que “La Constitución asegura a todas las personas: el respeto y protección a la vida privada y a la honra de la persona y su familia”. Esto se mantuvo por años hasta el 2018, en donde entró en vigor la ley 21.096, la cual elevó al derecho

a protección de datos personales a nivel constitucional, pero todavía ligado al derecho de la privacidad. Actualmente, el artículo 19 N°4 establece que: “se asegura a todas las personas el respeto y protección a la vida y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley”.

4.2.1.1 Datos personales a nivel constitucional

Como podemos ver, si bien Chile adoptó hace poco la protección de datos personales como un derecho fundamental, este lo sigue ligando al derecho de la privacidad, lo cual a mis ojos no es suficiente. Bajo nuestra perspectiva, este derecho de protección de datos debería de considerarse como un derecho aparte del de privacidad, tal como ocurre en la UE y en otros países latinos. El mantener ambos derechos ligados implica que uno depende del otro, cosa que es absurda, ya que, si bien ambos buscan la protección de la esfera más íntima de las personas, la protección de datos personales se ha desarrollado como una disciplina individual y con sus propias características.

A la fecha de redacción de esta memoria, Chile se encuentra ad-portas de un gran proceso de cambio normativo. El año 2019 ocurrió el denominado “estallido social” en el cual se exigieron cambios a nivel país para mejorar las condiciones de vida de todos los chilenos y chilenas, proceso que culminó en el acuerdo por una Nueva Constitución, la cual busca crear una nueva constitución y reemplazar la impuesta en el año 1980 por la dictadura militar.

Debido a este proceso de creación de una nueva constitución, que busca cumplir con las demandas sociales del país, considero relevante que se plantee y discuta la idea de la protección de datos personales. En otras palabras, consideramos necesario elevar a rango constitucional la protección de datos personales separado del derecho a la privacidad, a fin de que quede claro que su protección va más allá que una ley; sino que la protección de estos, debido a nuestra realidad actual donde la tecnología es rampante, su historia y rol, es un derecho fundamental individual de las personas.

Además, el elevar esta materia a rango constitucional propia nos permitiría elevar de forma directa nuestros estándares de protección de datos personales, ya que de forma directa tomaría mayor relevancia la ley que regule esta materia, ya que su base sería una regla constitucional.

Desde una perspectiva económica, la protección de datos resulta indispensable para el desarrollo de una estrategia digital y para atraer inversión extranjera.

4.2.2 Ley 19.628 sobre protección de datos personales

4.2.2.1 Rol, historia y estado actual de la de la ley 19.628

Actualmente en Chile se encuentra vigente la Ley 19.628 sobre protección de datos personales del año 1999. Esta ley tuvo su origen en la moción del Senador Eugenio Cantuarias en enero de 1993 y estuvo 6 años en tramitación, para luego ser publicada el 28 de agosto de 1999. Posteriormente, fue modificada por las Leyes N°19.812, 20.463, 20.521 y 20.575.

Lo que buscaba esta ley era llenar el vacío manifiesto que existía en nuestro ordenamiento jurídico, de modo de otorgar protección al derecho a la privacidad de las personas, en el ámbito del derecho Civil, ante eventuales intromisiones legítimas.

Sin embargo, si bien Chile fue pionero en Latinoamérica al de momento al promulgar una ley sobre protección de datos, en la actualidad esta se encuentra bastante desactualizada, ya que comparando la época en la que esta fue promulgada con la actual, ha habido un salto tecnológico gigante, respecto a velocidad, comunicación, tratamiento y demases. Es por esto que desde el año 2010 se ha apremiado la confección de una nueva ley y han ingresado diversos proyectos a la cámara, pero ninguno ha tenido éxito y se han paralizado en su mayoría. Sin embargo, con la entrada en vigor del RGDP y por el carácter comercial de nuestro país, se ha hecho más fuerte la necesidad de actualizar nuestra ley en esta materia, a fin de cumplir con los estándares actuales en esta.

4.2.2.2 Criticas a la Ley 19.628

Como podemos ver, existen diversas críticas a la ley de protección de datos personales actualmente vigente. Muchas de estas se deben principalmente al hecho de que esta ley está sumamente desactualizada en lo pertinente a tratamiento de protección de datos dado que en la época que se promulgó la tecnología era muy distinta a la que es actualmente. Acorde a la consulta experta sobre la ley 19.628 realizada por la Biblioteca del Congreso Nacional de Chile, las mayores críticas a la ley actual son que esta no considera un sistema de fiscalización adecuado, que ha sido sobrepasada por los avances tecnológicos, que el procedimiento de “Habeas Data” no es eficaz para la protección de derechos contemplados en la ley, falta de autoridad de control, entre otros. En esta consulta experta se preguntó a 7 expertos sobre su

opinión sobre esta ley y todos estos acordaron que la ley actual no cumple con su rol de proteger los datos personales.

Finalmente, otra fuerte razón por la cual se busca actualizar nuestra ley en esta materia es por el compromiso hecho con la OCDE en 2010. En el año 2010, Chile ingresó a la OCDE bajo la promesa de realizar adecuaciones normativas y modificaciones de marcos legales, entre los que destacaba la protección de datos y privacidad. El ICCCP señalo que, si bien Chile fue pionero en ley de datos en Latinoamérica, actualmente esta no tiene mecanismos de cumplimiento.

Respecto a la tramitación del proyecto de Protección de Datos, esta ingreso el año 2010 pero se estancó. Posteriormente, en 2012 se presentó otro proyecto, el que también se estancó en 2013. Finalmente, en 2014 el ministerio de economía convocó a la sociedad civil, academia y sector privada para hablar de datos y se logró un consenso sobre la necesidad de esta nueva ley, pero esta nuevamente no prosperó y se dejó de hablar. Por otro lado, la OCDE le pidió a Chile el 2015 a actualizar su legislación en esta materia, a fin de que se adecuase esta a las normas de la OCDE, es decir, a que aumentará su estándar de protección de datos.

Como se indicó la iniciativa de modificación a la ley 19.628 protección de Datos personales, el tratamiento de datos en Chile pugna con cualquier norma internacional y con las buenas prácticas promovidas por la OCDE. Ejemplos de esto es que no existe control sobre la información personal, ni la posibilidad de impugnar los tratamientos indebidos no consentidos y desinformados. Es importante una adecuada protección de los datos personales para el ejercicio de los derechos fundamentales en la red y fuera de ella, ya sea en entornos en línea y en entornos físicos.

4.2.2.3 El principio de finalidad en la ley 19.628

Como mencionamos anteriormente, existen variadas críticas a la ley vigente actual, pero en este trabajo nos referiremos solamente a como se encuentra establecido el principio de finalidad en nuestra ley, y que críticas y comentario podemos hacer a este.

Nuestra ley menciona al principio de finalidad limitada en su artículo 9 de la siguiente manera:

“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.

En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de datos.

Prohibiese la realización de todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda."

Como podemos ver, la ley actual menciona de forma cierta forma al principio de finalidad. Menciona que los datos deben usarse solo para los fines para los que fueron recolectados, salvo si provienen de una fuente de acceso al público. Por otro lado, este articulo mezcla también la noción de principio de finalidad con el principio de exactitud, ya que uno de los aportes centrales de esta ley fue la inclusión de lo que se conoce como derechos ARCO[54].

La ley actual también habla de la noción de fuente accesible al público, idea que se refiere a aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativo o sin más exigencia que, en su caso, el abono de una contraprestación. Esta es otra noción que ha sido duramente criticada, específicamente por su amplia definición y aplicación en la ley actual, pero este es un tema que se aparta del foco de este trabajo, que es específicamente el principio de finalidad.

En palabras breves, el principio de finalidad toma una forma bastante sencilla en la ley 19.628. Se establece que los datos no se utilizarán para fines distintos al fin para que se recolectaron, por lo que a primera vista podemos identificar que cumple con la función del mismo principio, es decir, limitar al responsable del tratamiento a sólo tratar los datos para los que se recolectaron, pero no habla de la segunda función del principio, que es la idea de no incompatibilidad, que permite que se trate de forma ulterior aquellos datos si es que los fines son compatibles. A mis ojos, el omitir esta segunda función del principio de finalidad es romper el equilibrio que busca, ya que, si bien se mantiene la idea de controlar al responsable del tratamiento, se le quita la posibilidad de seguir tratando la data, cortando de cierta forma así el libre flujo de esta.

[54] Derechos de acceso, rectificación, cancelación y oposición

Este libre flujo de data que menciono no debe de entenderse como que el controlador puede tratar los datos personales como plazca, sino que como sabemos este mismo ha de cumplir con diversas otras normas y principios que permiten que si bien siga tratando los datos personales bajo una idea de fines compatibles, este tratamiento nunca exceda sus capacidades o que este pase a llevar los derechos fundamentales de los interesados.

Finalmente, respecto a los propósitos privilegiados, esta ley sólo hace mención de los fines estadísticos en su artículo 4, pero este debido a su complejidad interpretativa y su falta de contenido ha sido criticado duramente. A mi parecer, este artículo buscaba añadir la idea de tratamiento de datos con fines privilegiados, pero termino obscureciendo esta idea debido a su redacción y contenido.

4.2.3 Ley 20575 Establece el principio de finalidad en el Tratamiento de datos Personales

Por último, tenemos la ley 20.575 que establece el principio de finalidad en el tratamiento de datos personales del año 2012.

Si bien esta ley busca añadir el principio de finalidad en el tratamiento de datos personales, esta queda, a mi parecer, corta en su alcance. Esto porque esta ley se enfoca meramente en la consagración de este principio en datos personales de carácter económico, financiero, bancario o comercial, que sólo deba referirse a la evaluación de riesgo para el proceso de crédito.

Es el mismo fundamente el que nos indica esto, ya que se señala que, si bien en Chile se encuentra cuestionada la protección de datos personales y protección a la vida privada, es necesaria de forma imperante resolver los problemas que yacen a la hora de evaluar el riesgo en el proceso de crédito. Esto debido a que los registros del DICOM sobre personas en situación de atrasos, moras o incumplimientos comerciales se estaban usando no simplemente para el otorgamiento de crédito, sino que se había transformado en práctica generalizada que los empleadores consultaran el DICOM del postulante y que ello influyera en la contratación de este. Como podemos ver, se estaba incumpliendo con el principio de finalidad, ya que se estaban usando los datos recogidos con fines determinados para otros fines, sin cumplir con el requisito de incompatibilidad, por lo que esto era totalmente ilegal.

Es importante mencionar esta ley, ya que, si bien esta buscó resolver un tema apremiante de la protección de datos personales, se enfocó solamente en dicho problema específico, es decir,

buscó parchar la ley actual para dicho problema en vez de reformarla completamente. Sin embargo, este parche cumplió con su fin de establecer el principio de finalidad dentro del título II de la ley 19.628, por lo que su introducción no es del todo criticable.

4.3 El principio de finalidad limitada en el nuevo proyecto de ley

Como se mencionó previamente, la actual Ley 19.628 ha sido objeto de diversas críticas y, sumado al apremio de diversos organismos internacionales como la OCDE y la entrada en vigor del RGDP en la UE, se ha impulsado fuertemente la redacción de una nueva ley de protección de datos personales. Han entrado más de 60 proyectos a la cámara de diputados, pero a la fecha, el proyecto que mayor peso ha tomado ha sido el proyecto sobre la protección de datos personales (boletín 11.092-07), el cual se refundió junto al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de datos personales (boletín N°11.144-07), ambos disponibles en línea[55].

Al estar refundidos, se entiende que se mezclaron ambos proyectos, y que por ende algunos artículos que trataban la misma materia se mezclaron o bien se impuso el precepto de un proyecto ante el del otro, caso que ocurrió con el principio de finalidad en este proyecto. Sin embargo, nos parece importante mencionar el origen de este principio en ambos proyectos, para luego dar una opinión del precepto actual y de las modificaciones realizadas en los trámites constitucionales posteriores.

4.3.1 Boletín 11.092-07

En el boletín 11.092-07 se establece al principio de finalidad de la siguiente forma: "los datos sólo serán tratados con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento posterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales[56]".

Como podemos ver, en este boletín se optó por usar la definición del principio de finalidad al igual que en el RGDP, casi siendo una copia exacta del mismo. También en este proyecto se indica en su artículo 6 el cómo realizar el examen de compatibilidad, tomando los factores que el artículo 6 (4) del RGDP aplica. Respecto a los fines privilegiados, se señala que estos no se

[55] https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07
[56] Artículo 8 (b) boletín 11.092-07

considerarán como incompatibles (art. 8 b)), que no se requiere el consentimiento erigido para su cesión (art. 7 c)) y que podrán conservarse por un periodo más largo (art. 8 i)) y la no obligación del responsable de proporcionar información cuando los datos personales no hayan sido obtenido de los titulares si se usan para estos fines (art. 12).

A mi parecer, la acepción del principio de finalidad en este boletín es la más amplia, esto puede entenderse en base a que el análisis realizado se centró en el RGDP y la historia europea, pero creo que a través de lo analizado y explicado en los capítulos anteriores podemos ver que esta acepción engloba todas las ideas centrales de la protección de datos, y a diferencia de la ley 19.628, se consideran ambos componentes de esta en este boletín, la especificación del propósito y la no incompatibilidad, permitiéndonos ver que si bien se limita al responsable, este igual puede tratar la data siempre y cuando los nuevos fines sean compatibles. Sin embargo, una pequeña crítica a esta adopción del RGDP es que no se incluye el factor de temporalidad de la especificación del propósito, ya que esta no se encuentra directamente en el art. 5 (1) (b) RGDP, pero si en su considerando 39 y al leerse en conjunto se entiende que el fin ha de determinarse a más tardar al momento de la recogida de datos. Agregar esto es fundamental para evitar posibles problemas respecto a cuando se debe de especificar el propósito.

4.3.2 Boletín 11.144-07

En este boletín se establece al principio de finalidad de la siguiente manera: “los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines. En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el titular otorgue nuevamente su consentimiento, los datos provengan de fuentes de acceso al público o así lo disponga la ley”. Respecto a los fines privilegiados, se hace un hincapié al artículo 89 del RGDP, respecto a las medidas que han de tomarse para realizar dichos tratamientos y se indican además los casos en los que estos fines son lícitos como tratamiento ulterior.

Como podemos ver, este boletín definió al principio de finalidad de manera muy similar a como este se encuentra en la Ley 19.628, pero la añade de manera explícita su primer componente, que es la especificación del propósito. Sin embargo, creemos que la crítica central a esta definición es que saca totalmente el segundo componente del principio, este viniendo a ser el de

no incompatibilidad para el tratamiento ulterior de los datos, sino que sólo permite este si se da el consentimiento nuevamente por parte del interesado. Como podemos ver, el enfoque de este proyecto va a darle más seguridad al interesado al darle un rol central a la idea de consentimiento al hacerla la fuente principal de legitimidad del tratamiento de datos.

Desde la perspectiva del principio de finalidad, este cambio de foco es inconveniente, ya que, al basar todo tratamiento posterior en el consentimiento, se le quita la facultad de al responsable de seguir tratando esta, afectando así el libre flujo de datos. Es interesante este cambio de foco, ya que a mis ojos tanto la no incompatibilidad como el consentimiento no debiesen de ser opuestos, sino podrían ser incluso complementarios. Recordemos que para probar la compatibilidad se ha de realizar todo un examen de factores para probarla, mientras que con el consentimiento sólo se requeriría la aprobación del interesado. Si ambos se aplicarán de forma complementaria, se permitiría el libre flujo de datos personales al permitirse el tratamiento ulterior siempre que exista compatibilidad, pero en los casos en que no exista compatibilidad o que bien el responsable considere que es necesario el consentimiento del interesado, podría de notificarle al mismo este nuevo propósito y ahí podría o bien obtener la aprobación del interesado para tratar los datos con este nuevo propósito o bien deberá de evitar realizar dicho tratamiento. Es decir, en el caso de que el examen de compatibilidad no sea del todo exitoso, el responsable podría de consultarle directamente al interesado si este nuevo procesamiento es, a sus ojos, realizable. Con esto se generaría una mayor flexibilidad a la hora de realizar tratamiento de datos.

Además, debemos de recordar que, al hablar de tratamiento de datos, no hablamos de sólo un proceso, sino que de diversos procesos que permiten recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma los datos personales. Esta es la definición dada de tratamiento de datos en este proyecto, de la cual está basada en la definición dada en la Directiva 95 y RGDP. Como señalamos en el punto 2.6.1.1, el primer acto de procesamiento es la recogida de estos, y que cualquier procesamiento posterior de estos, sea para el propósito especificado previamente o para cualquier otro propósito indicado posteriormente, se debe considerar como “tratamiento posterior” y que, por ende, este debe de cumplir con este requisito de compatibilidad. Como podemos ver, si se eliminamos el requisito de compatibilidad, entenderemos que cualquier tratamiento posterior a la recolección, sea el procesamiento,

almacenamiento, comunicación, etc, dependerá del consentimiento del interesado, lo que haría del tratamiento de datos un proceso interminable y exhaustivo, tanto para el responsable como para el interesado, ya que el primero deberá de preguntarle constantemente al segundo si este le permite realizar cualquier operación. Entiendo que cuando se habla de consentimiento se busca proteger este cambio de un fin específico, situación en donde es más que ideal solicitar el consentimiento del interesado, pero para realizar las operación de tratamiento de datos es recomendable sino ideal que se permita el tratamiento posterior bajo el requisito de compatibilidad, a fin de hacer el tratamiento más expedito y menos burocrático de lo que sería al andar constantemente solicitando al interesado su consentimiento para realizar distintos actos que se pueden entender que actúan en conjunto en el tratamiento de datos personales, pero que al fin y al cabo son distintos en esencia y por ende tratamientos distintos. Sin embargo, alguien podría indicar que esta idea es absurda y que, por ejemplo, es lógico que después de la recopilación de los datos el almacenamiento de estos será el siguiente paso a seguir y que no lo deberíamos de encasillar como un tratamiento posterior, sino que como parte inherente del mismo. La respuesta a esto es sencilla, en este ejemplo subyace de forma clara la idea de compatibilidad y si bien esta compatibilidad es obvia, indicamos también en el punto 2.6.1.4 que dependerá caso a caso la realización de un examen de compatibilidad, y que en estos casos donde haya una relación tan estrecha entre las ideas, no será necesario que se realice un examen de compatibilidad, pero que de todas formas ambas son partes distintas de un tratamiento.

Como hemos podido ver, en estos dos proyectos se ha presentado de forma diversa el principio de finalidad. En el boletín 11.092-07 se formuló a este al igual que en el RGDP, por lo que a mis ojos es el más adecuado, ya que incluye todos los componentes del principio, pero trayéndolos a la realidad chilena. El único problema de este proyecto es que no se menciona el requisito de temporalidad, que es clave para la especificación del propósito.

Por otro lado, el boletín 11.144-07 si bien añade el requerimiento de la especificación del propósito en su proyecto, omite el requerimiento de no incompatibilidad para tratamiento posterior, cambiándolo por el consentimiento explícito del titular para tratar los datos personales con un fin distinto. Como se explicó anteriormente, esto a mis ojos remueve una parte importante del principio de finalidad, que es tanto compatible con la idea de solicitud del consentimiento para el tratamiento ulterior de los datos personales pero que también permite

que el tratamiento se realice de forma fluida, ya que en virtud de la definición de tratamiento de datos personales podemos entender que el primer acto del procesamiento será la recogida, y que cualquier acto posterior tenga relación con el propósito original u otro distinto, se considerará como tratamiento posterior, por lo que deberá de cumplir con el requisito de compatibilidad. En este caso, el consultar por el consentimiento permanentemente podría retrasar altamente el proceso, ya que, si bien se busca darle mayor protección al interesado, con este cambio lo único que se hace molestarlo con distintas notificaciones.

4.3.3 Proyecto refundido

Finalmente, en este punto hablaremos sobre el cómo se encuentra el principio de finalidad en el proyecto de ley refundido que busca introducir modificaciones a la ley 19.628, sobre protección de los datos personales. Ya aquí podemos ver que se optó por una modificación muy sustantiva a ley actual más que cambiarla completamente, esto ya que dentro del mismo cuerpo legal está la regulación de datos económicos[57]. La discusión de este proyecto es amplia y abarca la gran mayoría de los elementos y componentes actuales de la regulación sobre protección de datos personales, ya que se busca actualizar fuertemente nuestra ley para elevarla a los estándares internacionales y defender de manera eficaz los datos personales en Chile.

Para el análisis del principio de finalidad, nos basaremos en el Primer trámite constitucional de este proyecto, específicamente en el Segundo informe de la Comisión realizado el 16 de marzo de 2020, ya que fue en esta en donde se discutió respecto al principio de finalidad y su redacción. Destaco además que, si bien existe un segundo informe de la Comisión realizado el 15 de diciembre de 2021, en este no se discutió sobre el principio de finalidad.

El proyecto refundido estableció el principio de finalidad de la siguiente manera.

Artículo 3.- Principios El tratamiento de los datos personales se rige por los siguientes principios:

b) Principio de finalidad. Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

[57] Proyecto Refundido;2020 pág. 7

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley"[58].

Como ya podemos ver, en el proyecto refundido el principio de finalidad se encuentra establecido de manera mucho más específica que en los boletines anteriores y que incluso en el RGDP, pero sigue la misma lógica que este último.

En el primer párrafo de este artículo vemos como la señala de manera clara el requerimiento de especificación del propósito, al indicar que los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. Añade además que el tratamiento de los datos personales debe limitarse al cumplimiento de estos fines, lo que nos indica que en este proyecto se le da especial importancia al principio de finalidad, ya que el tratamiento se limitará a sólo cumplir con los dichos fines.

El segundo párrafo es más amplio e incluye más elementos. Primero indica que, en aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, estableciendo el requerimiento de la temporalidad y reafirmando la esencia del principio de finalidad de no procesar datos con fines distintos al informado previamente. Directamente tras esto establece las excepciones a esto, es decir los casos en los que sí se permitirá un tratamiento con fines distintos a la inicial que son: (1) salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; (2) que exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento con fines distintos; (3) que el titular otorgue su consentimiento nuevamente; (4) que los datos provengan de fuentes de acceso al público, (5) y cuando lo disponga la ley.

Como podemos ver, a diferencia del RGDP que solo establece como excepción directa el tratamiento de datos con fines privilegiados, el artículo del proyecto refundido indica una mayor cantidad de excepciones. La primera corresponde al requerimiento de compatibilidad del

[58] Proyecto Refundido; 2020. pág. 80

principio de finalidad, que se incluye en esta disposición a fin de mantener el balance del principio de finalidad y para además permitir cierta flexibilidad dentro del procesamiento de datos, esto cuando se cumplan con el examen de compatibilidad, el cual si bien está establecido en el RGDP de forma general en el artículo 6 (4) y estaba incluido en el boletín 11.092-07, fue omitido en este. Las excepciones 2, 3 y 4 se refieren principalmente a bases de licitud del tratamiento, que previamente relacionamos con el elemento de legitimidad del principio de finalidad. Finalmente, el punto 5 se refiere a tratamiento con fines que la ley disponga, entre los que podemos encapsular los fines privilegiados. Respecto a esto últimos, dentro de este proyecto se encapsulan en el artículo 16 quinquies y se mencionan como una excepción a los derechos ARCO, esto de forma similar a como se regulan en el artículo 89 del RGDP.

Dentro de la discusión realizada en cámara respecto a este principio, se le decidió de añadir al párrafo segundo la siguiente frase: "En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; exista una relación contractual o pre contractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta **siempre que se enmarque dentro de los fines del contrato o, sea coherente con las tratativas o negociaciones previas a la celebración del mismo;** el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley"[59].

El establecimiento fue debido a que, como menciona el Senador Harboe, es que el principio de finalidad busca establecer que razones tuvo en vista el titular para otorgar su consentimiento al tratamiento que se mantenga no sólo al momento de la recolección, sino que también en la oportunidad de su utilización. Por ende, quien solicita un dato debe explicitar el tratamiento que se hará con él, buscando en definitiva que la entrega de un dato con una finalidad determinada no se pueda alterar, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente. A esto se añade la situación indicada en el párrafo segundo sobre la existencia de una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta. En resumen, con este añadido, se enfatizó aún más en la idea de compatibilidad para tratamiento posterior, específicamente señalando que,

[59] Proyecto Refundido; 2020. Pág. 490

aunque las partes se encuentren bajo un contrato, el propósito de un tratamiento respecto a este ha de enmarcarse en este mismo o ser coherente, es decir, no caer en la incompatibilidad.

Como hemos analizado, el principio de finalidad limitada se encuentra arduamente detallado y definido. Vemos que toma los elementos esenciales del principio de finalidad, la especificación del propósito y la noción de compatibilidad, pero también vemos que refuerza la idea de que no se puede realizar tratamiento a los datos personales si este no es acorde con los fines originales o es incompatible con aquellos. Sin embargo, también señala que existen excepciones, es decir, existen casos en los que se podrá tratar los datos personales con un fin distinto al fin inicial, pero que estos casos son taxativos.

Sin embargo, me gustaría realizar dos críticas a esta definición. La primera viene a ser respecto al elemento de temporalidad, ya que se indica que "no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección". A mis ojos esto podría llegar a ser mal interpretado bajo la idea de que sólo se deben de indicar los propósitos de la recolección *justo antes de la recolección",* lo que es un error, ya que estos se pueden señalar de forma previa a esta. Por otro lado, si bien este proyecto considera el requerimiento de compatibilidad, este no establece un criterio para realizar dicho examen como el que se encuentra en el RGDP. A mis ojos, el añadir un artículo que mencione estos factores permitiría que el examen de compatibilidad se realice bajo ciertos estándares o factores previamente determinados, dándole así un criterio de análisis.

4.4 Recomendaciones sobre cómo mejorar la protección de datos en Chile

Habiéndose realizado los análisis pertinentes, procederemos a efectuar nuestras recomendaciones sobre como perfeccionar el principio de finalidad en el nuevo proyecto de ley y sobre es posible elevar el actual o estándar de protección de datos personales.

Estas recomendaciones ya las he mencionado a lo largo de este capítulo, pero en esta última sección buscaré reafirmar estas mismas.

4.4.1 Establecimiento de la protección de datos personales como un derecho fundamental individual

Este punto ya fue indicado, pero creemos que es importante separar el derecho a la protección de datos personales del derecho a la privacidad Si bien ambos tienen un mismo origen, se han

desarrollado de manera individual cada uno, y que, si bien siguen estando fuertemente relacionados uno con el otro, el seguir hablando de ambos en forma conjunta es pasar a llevar los derechos de las personas. El subsumir la protección de datos personales en el derecho a la privacidad sólo generará inconvenientes y problemas doctrinales que pueden evitarse al separar ambos derechos.

Por otro lado, el rol de la ley es proteger a las personas y para hacer esto, la ley debe de adaptarse a las realidades de esta para protegerlas de la mejor manera posible. En la realidad actual las tecnologías se han vuelto una parte esencial de nuestra vida diaria y por lo tanto es necesario que la ley se adapte a esta realidad y nos proteja de los daños que estas pueden causar. Por ende, el establecimiento de un derecho individual y fundamental sobre la protección de datos personales nos permitirá proteger a los individuos de una manera más efectiva.

Finalmente, respecto a un derecho individual de la protección de datos personales, se debiese de considerar el establecer dentro de este mismo la idea del principio de finalidad limitada. Al establecer este principio, se establecería un elemento esencial de la protección de datos personales, la cual es que los datos sólo podrán ser tratados para fines concretos, el cual es uno de los pilares centrales del tratamiento de datos personales.

4.4.2 Recomendación respecto a la redacción del principio de finalidad en el nuevo proyecto de ley

Finalmente, creemos es necesario realizar una recomendación final respecto al principio de finalidad limitada. Esta recomendación de su redacción se efectúa sobre la base de todo lo analizado en forma previa. Finalmente, nos basaremos en el principio de finalidad limitada del proyecto actual, para buscar dar una definición más completa, acorde a la realidad de Chile.

Creemos que una mejor redacción del principio de finalidad es la siguiente:

Artículo 3 b): el tratamiento de los datos personales se rige por los siguientes principios: Principio de finalidad.

Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de los datos personales debe limitarse al cumplimiento de estos fines.

En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados **previamente o al momento de la recolección,** salvo que el tratamiento sea para

fines compatibles con los autorizados originalmente; exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distintas siempre que se enmarque dentro de los fines del contrato o, sea coherente con las tratativas o negociaciones privas a la celebración del mismo; el titular otorgue nuevamente su consentimiento; los datos provengan de fuentes de acceso público, y cuando lo disponga la ley.

Se agrega además un nuevo artículo al título II del tratamiento de los datos personales y de las categorías especiales de datos párrafo primero

Artículo 14. Sobre el tratamiento posterior de datos personales con fines distintos que aquel que se recogieron los datos personales

Cuando el tratamiento para un fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado, el responsable del tratamiento, a fin de determinar si el tratamiento con otro fin es compatible con el fin previamente establecido, tendrá en cuenta, entre otras cosas:

a) **Cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;**
b) **El contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;**
c) **La naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, o datos personales relativos a condenas e infracciones penales**
d) **Las posibles consecuencias para los interesados del tratamiento ulterior previsto**
e) **La existencia de garantías adecuadas, que podrán incluir el cifrado o la disociación de datos.**

A nuestro parecer, el redactar el principio de finalidad de esta forma, indicando de manera más clara el elemento de temporalidad y señalar en un artículo separado los factores a considerar para realizar un examen de compatibilidad es la mejor forma de establecer este principio en nuestra legislación. El proyecto refundido en sí ha tomado diversos elementos de diversos instrumentos internacionales, los ha estudiado y ha buscado implementar de la manera más

completa y correspondiente a nuestra realidad como país. Por ende, a diferencia de otros países, nuestro principio de finalidad se ve más robusto. Si bien este es más robusto, esto no lo hace más restrictivo o difícil de interpretar, sino que lo contrario. Lo que hace es indicar los diversos factores y elementos que influyen y se relacionan al principio de finalidad limitada. Establece la especificación del propósito, la compatibilidad, la temporalidad, el consentimiento, las relaciones contractuales, los datos de fuentes accesibles al público. Al hacer esto nos indica claramente en que situaciones se podrá tratar la data personal de forma excepcional, ya que la regla que establece es la limitarse al tratamiento de datos personales para los fines determinados previamente. La nueva ley busca ser clara y completa, y con esta redacción se alcanzará ese objetivo.

Capítulo 5: Conclusiones

A lo largo de este trabajo hemos desarrollado diversos conceptos y nociones referentes al tratamiento de datos personales y al principio de finalidad limitada. En el primer capítulo realizamos una introducción bastante concisa a esta materia. Primero hablamos sobre los orígenes de la privacidad y como esta fue tomando peso en el siglo XIX y como se consolido como derecho fundamental a mediados del siglo pasado. Vimos también que una de sus características es la dificultad de darle una definición universal a esta, por lo que su alcance y marco regulatorio depende de diversos factores, pero que de todas maneras es un derecho fundamental del hombre. También hablamos sobre la historia de la protección de datos personales, de cómo partió como una rama de la privacidad y como fue desarrollándose a lo largo de los años, hasta consolidarse a inicios del siglo XX como un derecho individual y que amerita su propio marco regulatorio. Vimos como los diversos instrumentos de esta materia fueron consolidándose y elaborar diversos principios, nociones y elementos, que actualmente se recogen en el RGDP. Todo esto sirvió como una introducción al principio de finalidad limitada, ya que hablamos de su origen y evolución hasta la actualidad.

Tras esto en el segundo capítulo nos enfocamos ya en el principio de finalidad limitada. Específicamente hablamos del desarrollo de este principio en diversos instrumentos y los elementos que se le fueron añadiendo con el tiempo hasta su consolidación actual en el RGDP. Tras esto, desmenuzamos este principio en dos componentes, la especificación del propósito y la no incompatibilidad, que analizamos arduamente a nivel elemental. Hablamos del sus elementos internos y el rol que cumplía cada uno respectivamente esto a fin de que tuviéramos una noción clara sobre que busca este objetivo.

Esta idea se consolido en el capítulo 3, ya que en este tomando todo lo analizado en el capítulo 2 buscamos definir el rol del principio de finalidad limitada dentro de la protección de datos, tanto de manera individual como su posición respecto a los demás principios de la protección de datos. Vimos que cumple con un doble rol, de obligar al responsable a definir previamente a la recolección de datos el propósito de esta misma y además lo obliga a ceñirse por dicho propósito definido a la hora de tratar de manera posterior los datos personales. Hablamos también de su similitud con la idea del Imperio de la Ley, ya que ambas buscan de cierta forma crear un sistema de chequeo y balances para limitar el poder de la autoridad y del responsable

del tratamiento, a fin de que este no abuse de su posición y poder. Luego de definir su rol individual, nos enfocamos en uno de los cuatro pilares principales para legitimar un tratamiento de datos; el cumplimiento de todos los principios de protección de datos personales de forma cumulativa. Vimos que, dentro de este requerimiento, el principio de finalidad limitada tiene una importancia mayor a los demás, ya que este es un requisito condicional para la aplicación de los demás principios, es decir, sin el principio de finalidad no sería aplicar los demás principios de protección de datos personales, por lo que aparte de cumplir con un rol de regulación cumple con un rol central a la hora de aplicar todo el marco legislativo de protección de datos personales.

Finalmente, buscamos traer todo los estudiado a Chile. Para esto se analizó la situación actual latinoamericana respecto a la protección de datos personales para luego enfocarse en la regulación actual chilena de esta materia, tanto en la vigente como en los proyectos de ley. Finalmente, hemos efectuado una recomendación final para una implementación adecuada, completa y clara del principio de finalidad para el nuevo proyecto de ley.

Glosario

RGDP	Reglamento General Datos Personales
DUDH	Declaración Universal de Derechos Humanos
CEdDH	Convención Europea de Derechos Humanos
CDFUE	Carta Derechos Fundamentales de la Unión Europea

Bibliografía

Bloustein, E. (1964). Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. *New York University Law Review*.

Friend, C. (1968). Privacy. *The Yale Journal*.

Gavison, R. (1980). Privacy and the limits of Law. *The Yale Journal*.

Gerety , T. (1977). Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review*.

Hildebrandt, M. (2014). Location data, pirpose bindinf and conextual integrity: What´s the message? En *Protection of Information and the Right to Privacy-a New Equilibrium?* (págs. 31-62).

López-Torres, j. (2014). Antecedentes Internacionales en mateira de privacidad y proteccion de datos personales. *Revista Académica Universidad EAFIT*, 103-117.

Lukács, A. (s.f.). What is Privacy? The history and definition of privacy. 256-265.

Posner, R. (1978). The Right of Privacy. *Gergia Law Review Vol. 12 No.3*.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review* , 1132-1140.

Warren, S. D., & Brandeis, L. (1890). The right to privacy. *Harvard Law review*, 193-220.

Westin, A. (2003). Social and political dimensions of privacy. *Journal of Social Issues Vol 59*, págs. 431-434.

WP Art. 29. (2013). *Opinion 03/2013 on purpose limitation.*

Koning M. E. 2020. The purpose and limitations of purpose limitation. Memoria para optar al título de doctor en derecho. Ultrecth, Radboud University Nijimegen. 297p.

Chile. Comisión Ortúzar, Consejo de Estado y Junta Militar de Gobierno. 1980. Constitución Política de la República de Chile.

Chile. Ministerio Secretaría General de la Presidencia. 1999. Ley 19.628: Sobre protección de la vida privada

Chile. Ministerio de Economía, Fomento y Turismo; Subsecretaría de Economía y Empresa Menor. 2012. Ley 20.575: Establece el principio de finalidad en el tratamiento de datos personales

Chile. Ministerio Secretaría General de la Presidencia. 2018. Ley 21.096: Consagra el derecho a protección de los datos personales.

Ministerio Secretaría General de la Presidencia, Ministerio de Economía, Fomento y Turismo y Ministerio de Hacienda. 2017. Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de datos personales. En: Cámara Senado: 15 de marzo de 2017. Valparaíso, Cámara de Diputados y Diputadas. 56pp.

Harboe, Araya, De Urresti, Espina y Larraín. 2017. Proyecto de Ley sobre protección de datos personales. En: Cámara Senado: 17 de enero de 2017. Valparaíso, Cámara de Diputados y Diputadas. 28pp.

Comisión de Constitución, Justicia y Reglamento. 2020. Segundo Informe recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la agencia de Datos Personales (Boletines N°11.092-07 y 11.144-07 refundidos). En: Cámara del Senado. 16 de marzo de 2020. Valparaíso, Cámara de Diputados y Diputadas. 563pp.

Roberts, R. 2018. Reporte: Consulta experta sobre la ley de Protección de la vida Privada de las Personas. Santiago. Biblioteca del Congreso Nacional de Chile 12pp.

UE. Parlamento Europeo y del Consejo. 2016. Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos)

UE. Parlamento Europeo, El Consejo y la Comisión. 2000. Carta de los derechos Fundamentales de la Unión Europea

OCDE. 1980. Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.